MANDIANT
AHORA PARTE DE Google Cloud

Informe de la Mirada a la Ventaja del Defensor, edición 3

El informe de la Mirada a la Ventaja del Defensor ofrece información sobre los temas de defensa cibernética de creciente importancia con base en las observaciones de primera línea de Mandiant y las experiencias del mundo real. En esta edición, se abordan temas como:

El camino hacia la autenticación sin contraseñas

Históricamente, la autenticación desafío-respuesta mediante una contraseña única ha sido uno de los principales mecanismos utilizados por las organizaciones para verificar una identidad con fines de autorización. Sin embargo, seguir el modelo de una transacción única para la autenticación, sin requisitos adicionales de verificación de la identidad, podría crear un riesgo sustancial para una organización.

A medida que los atacantes adoptan tácticas más sofisticadas para comprometer las identidades, se introducen nuevos controles y metodologías para ayudar a mitigar los riesgos. El control más común y que muchas organizaciones adoptaron es el requisito de autenticación multifactor (multi-factor authentication, MFA), un concepto que combina dos o más métodos independientes para verificar correctamente una identidad.

Gracias a diversas investigaciones de respuesta a incidentes, Mandiant pudo comprobar que mientras las organizaciones aumentaban la adopción de métodos tradicionales de MFA, los atacantes continuaban con tácticas de amenazas avanzadas para comprometer identidades utilizando técnicas como:

eludir la MFA obligatoria

abusar de métodos de MFA más débiles (por ejemplo, SMS, notificaciones push, llamadas telefónicas)

registrar dispositivos controlados por atacantes para la validación y autenticación de la MFA

Esta mayor amenaza hizo que la adopción de la MFA se centrara en nuevas herramientas con métodos de MFA más potentes, como la coincidencia de números, las notificaciones telemétricas contextuales y la introducción de contraseñas de un solo uso por tiempo (time-based one-time, TOTP). Además, los proveedores y organizaciones están mejorando aún más sus métodos de MFA mediante el uso de claves/tokens Fast Identity Online 2 (FIDO2), tokens de autenticación abierta de software/hardware (hardware Open Authentication, OATH) o autenticación basada en certificados.

Autenticadores

Para mejorar aún más la seguridad de la autenticación, el concepto de "autenticadores" empezó a integrarse en las prácticas de gestión de identidades y accesos de las organizaciones. Los autenticadores se alejan del contexto singular de una contraseña y requieren distintos componentes para poder verificar una identidad. Algunos ejemplos de autenticadores pueden incluir un multicontexto de nombre de usuario y contraseña combinado con métodos MFA fuertes, certificados, contexto de estado del dispositivo, cálculo de riesgo de identidad o métodos sin contraseña.

Al alinearse bajo el concepto de "autenticadores", el riesgo general que supone una contraseña comprometida se reduce enormemente, ya que la naturaleza singular de la contraseña deja de ser la primera y la última línea de defensa para la autenticación.

¿Qué significa "sin contraseña"?

Tomando como base sólidos métodos de MFA, la autenticación sin contraseña está empezando a formar parte de la ecuación del "autenticador" para muchas organizaciones. El método sin contraseña es básicamente un método para verificar una identidad sin que sea necesario un secreto basado en el conocimiento. Sin embargo, la identidad se autentica utilizando algo que se posee (dispositivo) o algo que se es (biometría). Bajo la premisa de la ausencia de contraseñas, el requisito de factores basados en la posesión o en la inherencia aumenta la seguridad, ya que elimina el requisito de que "algo que uno sabe" (contraseña) forme parte de la ecuación de autenticación.

Los métodos prácticos y escalables para sacar partido de la autenticación sin contraseña pueden incluir:

- **Aplicaciones de autenticación para dispositivos móviles:** pueden generar un código de un solo uso (one-time passcode, OTP) (basado en un algoritmo sincronizado) o se pueden usar para aprobar o hacer coincidir una secuencia de números que se muestra al usuario.
- **Tokens y claves de hardware FIDO2:** pueden interactuar con un dispositivo mediante una conexión física, Bluetooth o tecnología NFC (Near Field Communication). En particular, con el método WebAuthn de FIDO2, el token de hardware vinculado al dispositivo puede servir para autenticarse en la aplicación de destino utilizando un par de claves criptográficas único (almacenado en el dispositivo autenticador itinerante) y que se intercambia mediante criptografía de clave pública. FIDO2 Webauthn es un método eficaz que permite aprovechar la autenticación sin contraseña para combatir los ataques de suplantación de identidad (phishing), falsificación informática (spoofing) y adversarios en el medio (adversary-in-the-middle, AitM).
- **Claves de acceso:** funcionan como un token FIDO2, en el que se genera un par de claves criptográficas que se almacenan localmente en un dispositivo móvil y se intercambian mediante criptografía de clave pública con una aplicación que es el objetivo de la autenticación (que posee la clave pública). Para acceder a una clave de acceso configurada, el dispositivo móvil requerirá una identificación biométrica o un patrón de PIN o deslizamiento común en los dispositivos móviles más populares.
- **Certificados digitales:** permiten generar una firma digital de "identidad" válida como respuesta a una solicitud de autenticación mediante el uso de pares de claves públicas y privadas. En los dispositivos modernos, el módulo de plataforma de confianza (trusted platform module, TPM) puede ser utilizado como autenticador interno para almacenar la clave criptográfica privada, que se utiliza para firmar el certificado que será validado para la autenticación "sin contraseña" utilizando la clave pública correspondiente.

- **Biometría:** permite aprovechar las características físicas únicas de una persona para validar su identidad. Por lo general, la autenticación biométrica incluye métodos de reconocimiento de huellas dactilares (Touch ID y Fingerprint Unlock, por ejemplo) y faciales (Face ID y Face Unlock, por ejemplo), que son comunes en muchos teléfonos inteligentes, dispositivos móviles y computadoras portátiles modernas.

Planificar la autenticación sin contraseña

Las aplicaciones e infraestructuras heredadas que no admiten fácilmente métodos de autenticación mejorados pueden suponer un obstáculo para las organizaciones que intentan alinearse bajo el concepto de autenticadores. En lugar de centrarse en la integración de la ecuación del autenticador para cada aplicación individual, en la actualidad, es habitual que las organizaciones aprovechen una solución de inicio de sesión único (single sign-on, SSO) de terceros como puerta de entrada para la autenticación, que luego gestionará el acceso autenticado a las aplicaciones backend.

Planificar la tecnología sin contraseña como parte de la ecuación del autenticador puede llevar tiempo. Las consideraciones a tener en cuenta son las siguientes:

Identificar:

- Tecnologías y plataformas actuales que funcionan como almacenes y plataformas de identidades autorizadas (identity stores and platforms, IdP).
- Los almacenes de identidades existentes admiten de forma nativa métodos de autenticación sin contraseña, o bien requieren la integración de terceros y de intermediarios.
- Identidades que existen dentro de una organización, incluidos los tipos de identidad que podrían probar y verificar la experiencia sin contraseña.
- Controles de compensación y detecciones mejoradas para tipos de identidad que no admiten métodos de autenticación fuerte o sin contraseña (por ejemplo, cuentas programáticas o de servicio).
- El impacto para los usuarios invitados o terceros que no admitan la integración sin contraseña.
- Dispositivos que los usuarios utilizan habitualmente para la autenticación y el acceso, y verificación de si estos dispositivos admiten métodos sin contraseña.
- Aplicaciones que pueden integrarse directamente para utilizar métodos sin contraseña, o aplicaciones que admiten la integración de SSO con una plataforma de terceros que admite tales métodos.

Desarrollar un plan para:

- Adquirir e incorporar de forma segura dispositivos compatibles con la autenticación sin contraseña.
- Programa de capacitación para enseñar a los usuarios la experiencia sin contraseña.
- Modificaciones en el almacén de identidades y en la configuración de los dispositivos para incorporar la integración sin contraseña.
- Probar y validar la integración de la tecnología sin contraseña con usuarios piloto y aplicaciones de ámbito limitado.
- Implementación inicial e incorporación, así como ampliación del alcance de la tecnología sin contraseña en toda la organización.

Otro aspecto importante a tener en cuenta en el uso de la tecnología sin contraseña es la adecuación de los pasos de recuperación en caso de pérdida o robo de un dispositivo o una clave, ya que se trata de componentes esenciales del proceso de autenticación de una identidad. La planificación de medidas de recuperación seguras debe incluir la evaluación no solo del riesgo para la organización, sino también de los pros y los contras de la experiencia general de registro y autogestión de los usuarios.

Si bien los autenticadores internos (por ejemplo, dispositivos con un TPM integrado) ofrecen la posibilidad de exportar (almacenar) o sincronizar claves privadas entre dispositivos, esto también puede suponer un riesgo si las claves no cuentan con las medidas de seguridad y almacenamiento adecuadas. Al utilizar proveedores de identidad externos, las claves y frases de recuperación también sirven como método de recuperación de una identidad sin contraseña para su restablecimiento en un nuevo dispositivo. En el caso de los autenticadores itinerantes que permiten la autenticación sin contraseña, las opciones de recuperación de identidad pueden incluir validar los mensajes enviados a un dispositivo móvil o a una dirección de correo electrónico.

Pasar del concepto de contraseña única al de autenticación sin contraseña es un proceso largo. Muchas organizaciones que adoptan el concepto de autenticadores han descubierto que una MFA sólida es un pilar fundamental para lograr un plan de acción sin contraseñas. Aunque este proceso requiere de una planificación, ejecución y validación adecuadas, los beneficios para la seguridad y mitigación de riesgos son incalculables, sobre todo teniendo en cuenta que la identidad representa la nueva frontera de la seguridad en el modelo operativo híbrido actual.

Minimizar riesgos para obtener un ciberseguro

Los bancos de los Estados Unidos registraron USD 1200 millones en transacciones de ransomware según los 1489 informes enviados a los entes reguladores en 2021, lo que supone un fuerte aumento con respecto a los USD 416 millones registrados en 487 informes el año anterior[4].

Los pagos por ransomware se incrementaron en más del doble entre los años 2020 y 2021[1], lo que obligó a las aseguradoras a asumir más pérdidas y encaminó el mercado de los seguros de ciberseguridad por un camino volátil que apenas ha comenzado a estabilizarse. Y, si bien a finales de 2022 se produjo una desaceleración del 80 % en los aumentos de las tarifas de los seguros cibernéticos, lo que implica una mejora de las perspectivas del mercado para 2023[2], la mayoría de las aseguradoras creen que el riesgo cibernético seguirá en aumento, ya que el ransomware continúa siendo una de las principales amenazas[3]. Como resultado, las organizaciones pueden esperar un mayor escrutinio durante el proceso de suscripción sobre sus controles de seguridad y sus procesos y procedimientos internos con respecto al riesgo cibernético. Además, todavía quedan exclusiones preocupantes para eventos generalizados (por ejemplo, Log4j) e incidentes que pueden vincularse al conflicto en Ucrania o a grupos de ataque patrocinados por Estados nación. De hecho, las aseguradoras siguen reduciendo o incluso excluyendo la cobertura relacionada al ransomware si la organización no demuestra controles adecuados en la gestión de este riesgo.

En los últimos 12 meses, Mandiant registró un aumento en la participación de las aseguradoras cibernéticas durante las intervenciones de respuesta ante un incidente. Aunque no suele consultarse a los CISO sobre las decisiones de cobertura de las pólizas, recomendamos que trabajen codo a codo con el gerente de riesgos y el asesor jurídico de la organización para garantizar la precisión del proceso de solicitud y revisar las pólizas, de modo que no los tomen desprevenidos en caso de producirse una vulneración.

Seguros cibernéticos 101

A mediados de la década del 2000, las aseguradoras ampliaron la cobertura para reembolsar a las empresas por los costos derivados de ciberataques que afectaron directamente a su negocio[5]. Desde entonces, la ampliación de la cobertura se ha convertido en una herramienta útil para que los gerentes de riesgos financieros y los responsables de ciberseguridad mitiguen el riesgo y compensen los costos derivados de las vulneraciones de datos u otros incidentes de seguridad. Las pólizas suelen cubrir el riesgo cibernético sufrido por la empresa (riesgos sobre la propiedad o persona del asegurado) y la responsabilidad de consumidores o empresas (responsabilidad de terceros). Originalmente, la suscripción para seguros cibernéticos se centraba en los costos asociados con vulneraciones de datos y, como tal, se exigía a las organizaciones facilitar información sobre los tipos de registros, datos de clientes y datos regulados que procesaban para los suscriptores, así como certificar el cumplimiento de normas regulatorias, como HIPAA y PCI DSS. El ransomware y la extorsión multifacética suponen un riesgo adicional de interrupción de la actividad comercial que puede paralizar una empresa y generar costos significativos.

1. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, 4 de noviembre de 2022
2. Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, 7 de octubre de 2022
3. Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, 10 de enero de 2023
4. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, 4 de noviembre de 2022
5. The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019 The Growth and Challenges of Cyber Insurance, 2019

TABLA 1: Coberturas comunes de riesgos de seguridad cibernética.

Cobertura sobre la propiedad o persona del asegurado	**Responsabilidad de terceros**
Honorarios por respuesta ante incidentes e investigación forense	Responsabilidad en materia de seguridad y privacidad
Supervisión de notificaciones, crédito e identidad	Responsabilidad en materia de comunicación multimedia y medios de comunicación
Recuperación de datos	Defensa y sanciones reglamentarias
Interrupción de la actividad empresarial	Responsabilidad en materia de PCI DSS
Extorsión cibernética y ciberdelincuencia	Defensa de la Ley de protección del consumidor con respecto a las llamadas telefónicas
Daños a la reputación	

*Fuente: Honigman LLP Attorneys and Counselors, Cyber Insurance 101, 19 de mayo de 2021

Como resultado, las aseguradoras se han puesto manos a la obra para examinar más detenidamente los controles técnicos de una organización y las actividades de mitigación contra la interrupción y otras pérdidas comerciales asociadas. Esto se traduce en un riguroso proceso de suscripción para determinar los riesgos y el precio de las pólizas. Hoy en día, la suscripción implica preguntas adicionales, entrevistas y someterse a una exploración externa de su entorno.

La presidenta del Departamento de Ciberseguridad y Privacidad de Datos de Woods Rogers, Beth Burgin Waller, quien dedica mucho tiempo a analizar y negociar seguros cibernéticos para clientes, además de ofrecer asesoramiento de respuesta ante incidentes, recomienda trabajar con el equipo de gestión de riesgos y el departamento legal para prepararse para el proceso de suscripción.

Los cuestionarios de suscripción suelen incluir preguntas en blanco y negro que no se aplican a las complejas infraestructuras corporativas multinube y multirred de la actualidad. Por ejemplo, al responder a una pregunta sobre si dispone de autenticación multifactor (MFA) en toda la empresa, es posible que sus suscriptores le pidan pruebas de que la MFA está presente en todos los sectores de la empresa, desde copias de seguridad hasta aplicaciones comerciales en la nube y VPN. Su asesor jurídico y su equipo de gestión de riesgos pueden ayudarle a detectar las afirmaciones generalizadas incluidas en la solicitud y facilitar respuestas complementarias que aclaren los controles de producción actuales y los planes de mejora.

Comprender los matices de la cobertura de respuestas ante incidentes

Burgin Waller recomienda encarecidamente revisar la política de especímenes (muestras). "A medida que el mercado se estabiliza, el lenguaje de las pólizas cibernéticas se está estandarizando de forma similar a otros productos de pólizas de seguros", afirma Burgin Waller. La póliza de muestra puede indicar que usted tiene cobertura contra la interrupción del negocio hasta un cierto límite, pero sin un análisis minucioso de la póliza de muestra usted puede tener exclusiones incorporadas en la póliza para programas heredados, eventos generalizados como Log4j, o la última exclusión: actos de guerra, que cubre incidentes atribuidos a actores de amenazas de Estado nación. Burgin Waller sugiere prestar especial atención a los sublímites de las políticas. En un ejemplo, una póliza cibernética básica incluía un sublímite para incidentes iniciados a través del phishing y exigía a la organización una cobertura complementaria contra el ransomware. "Leer detenidamente su póliza de muestra desde el principio", afirma Burgin Waller, "puede ahorrarle importantes dolores de cabeza durante un incidente al aclarar lo que puede o no incluirse en la cobertura de su organización antes de que se produzca un incidente".

¿Puede esperar que el proveedor de respuesta ante incidentes y los costos relacionados estén cubiertos? Los equipos de respuesta ante incidentes de Mandiant suelen encontrarse con tres situaciones habituales:

1) El proveedor de respuestas ante incidentes (incident response, IR) es un proveedor autorizado con tarifas previamente negociadas. Esto agiliza la puesta en marcha de los contratos y puede facilitar a los clientes la presentación de sus reclamos.

2) El proveedor de IR no cuenta con autorización previa y la aseguradora cubrirá USD x/hora. El cliente deberá compensar la diferencia si la tasa de IR es superior al importe cubierto.

3) El proveedor de IR no cuenta con autorización previa y la aseguradora no proporcionará cobertura alguna si se recurre a ese proveedor de IR. Este caso es el que más problemas puede causar en caso de producirse una vulneración.

Es importante revisar los modelos de políticas para comprobar si cubren todo el proceso de respuesta ante incidentes. Algunas pólizas cubren únicamente la investigación y excluyen los pagos por ransomware, los costos del asesoramiento jurídico en general o los gastos relacionados con las tareas de recuperación y remediación a largo plazo. Además, es posible que las aseguradoras no cubran una investigación completa para determinar exactamente cómo se infiltró un atacante y verificar que no dejó ninguna puerta trasera que pudiera hacer que el cliente quedara vulnerable frente a una nueva infección. Es entonces que la decisión de seguir adelante con una investigación en profundidad destinada a reducir futuros riesgos se convierte en una decisión comercial.

Un nuevo enfoque

En general, el mercado de los seguros cibernéticos está evolucionando de tal manera que los proveedores se alían con sus clientes para mejorar la resistencia cibernética global. La industria de seguros cuenta con programas muy avanzados de modelización de riesgos que sirven para aumentar la seguridad de las organizaciones.

Muchos socios de seguros ofrecen un paquete de proveedores y soluciones que ya han investigado para ayudar a sus clientes a navegar por el mercado de la ciberseguridad y reducir riesgos empleando tecnologías que hayan demostrado su eficacia.

Los socios de seguros incluso identificaron controles de seguridad que pueden tener un impacto positivo tanto en los riesgos cibernéticos de una organización como en los costos de las pólizas relacionadas[6]. Mandiant adopta las recomendaciones de la industria de seguros y destaca las siguientes cinco prácticas que, aplicadas de forma correcta, pueden mitigar el impacto de los ataques típicos o evitarlos:

1. **Autenticación multifactor:** La MFA, o autenticación de dos factores, es una tecnología que combina dos o más credenciales independientes (por ejemplo, contraseñas, tokens de seguridad y huellas faciales o dactilares) para permitir el acceso del usuario. Gracias a diversas investigaciones de respuesta ante incidentes, Mandiant pudo comprobar que mientras las organizaciones han aumentado la adopción de métodos tradicionales de MFA, los atacantes continúan con tácticas de amenazas avanzadas para comprometer identidades. Implementar sólidas herramientas y métodos de MFA, como la coincidencia de números, las notificaciones telemétricas contextuales y la introducción de contraseñas de un solo uso por tiempo (TOTP), en todos los portales de inicio de sesión accesibles de manera externa y para cualquier aplicación interna sensible, puede reducir los riesgos asociados a las técnicas comunes de acceso inicial de los adversarios.
2. **Gestión de identidades y acceso privilegiado:** La identidad es la nueva barrera de seguridad en el modelo operativo híbrido actual. Mandiant constata que los sistemas de gestión de accesos y directorios se ven comprometidos en muchos casos de respuesta ante incidentes. Los actores suelen utilizar estos sistemas para escalar privilegios. Las organizaciones deben asegurarse de que tanto usuarios como sistemas cuentan con el acceso adecuado y de que los sistemas de gestión de directorios y accesos están correctamente configurados para evitar la escalada de accesos privilegiados no autorizados.
3. **Copias de seguridad seguras, cifradas y probadas:** Mandiant recomienda a las organizaciones contar con un plan probado para proteger y cifrar sus copias de seguridad a fin de facilitar la restauración de sistemas y datos en caso de sufrir

6. Marsh, Cyber Insurance Market Overview: Fourth Quarter 2021, 7 de diciembre de 2021

un ataque cibernético. Las soluciones de copia de seguridad y almacenamiento externo pueden ayudar a disminuir la probabilidad de pérdida de IP y garantizar que los registros más importantes estén protegidos frente a pérdidas. Las empresas utilizan cada vez más las soluciones de servicios en la nube como una manera de mantener una copia de sus redes en la nube o híbridas en caso de sufrir un ataque cibernético que, de otro modo, paralizaría las operaciones.

4. **Planificación y pruebas de respuesta ante incidentes cibernéticos:** Mandiant considera que planificar y probar la respuesta ante incidentes cibernéticos es una actividad crítica que implica examinar los controles técnicos existentes, las arquitecturas de red y las capacidades de primera respuesta. Mandiant sugiere desarrollar planes para posibles situaciones típicas de respuesta y validar continuamente las capacidades de ciberdefensa para permitir una rápida contención en caso de producirse un incidente.
5. **Contratar socios en el ámbito legal y de respuesta ante incidentes:** Una parte importante de la planificación de la respuesta ante incidentes cibernéticos es estar preparado para obtener soporte externo para proteger a la empresa de riesgos legales y obtener experiencia en respuestas ante incidentes. Los asesores legales, sobre todo los especializados en cuestiones cibernéticas, deben poder trabajar sin problemas con los forenses en caso de sufrir un ataque para evaluar la responsabilidad legal y los riesgos que puedan surgir del incidente. El soporte externo de respuesta ante incidentes puede reducir significativamente el tiempo de respuesta, lo que disminuye el impacto de una vulneración. Un contrato de servicio de respuesta ante incidentes (Incident Response Retainer, IRR) les permite a las empresas acordar los términos y condiciones de los servicios de respuesta ante incidentes antes de que se sospeche un incidente de ciberseguridad.

Los socios de seguros también ofrecen asesoramiento y servicios de seguridad para agilizar el proceso de solicitud. Muchos intermediarios y aseguradoras diferencian sus servicios ampliando su consultoría con evaluaciones, ciberhigiene y procesos necesarios para desarrollar capacidades defensivas eficaces.

Obtenga más ayuda para conocer los seguros cibernéticos de los socios de Mandiant, podcasts, seminarios web y ofertas de Google Cyber Risk.

Estudio de caso desde el punto de vista de un analista de seguridad: Identifique y detenga los ataques a la cadena de suministro de software

Qué aspectos positivos tiene activar las funciones de detección y respuesta

El año pasado, Mandiant informó un aumento significativo en el ataque a la cadena de suministro: el 17 % de las intrusiones en el transcurso del año 2021 se originó dentro de la cadena de suministro, frente a <1 % en 2020[7]. Este aumento se explica en parte por el hecho de que el 86 % de las intrusiones comprometidas rastreadas por Mandiant estaban relacionadas con la vulnerabilidad de SolarWinds y SUNBURST[8]. Sin embargo, también se correlaciona con el hecho de que las organizaciones mantienen relaciones tecnológicas con un promedio de 244 proveedores[9].

Los ataques a la cadena de suministro de software no son ninguna novedad. En 2017, el mundo sufrió un ataque conocido como NotPetya. El código malicioso, disfrazado de ransomware, se aprovechó de la vulnerabilidad EternalBlue filtrada de la NSA para infiltrarse en las redes y destruir datos sistemáticamente. Los atacantes detrás de NotPetya vulneraron una compañía de software de servicios financieros que era proveedora del Gobierno ucraniano.

Ese mismo año, la utilidad CCleaner[10] sufrió una vulneración y los piratas informáticos lograron sustituir la versión legítima del software por una maliciosa, lo que provocó que más de 2 millones de hosts se vieran comprometidos.

En 2020, el mencionado ataque generalizado que aprovechó un componente de SolarWinds fue perpetrado por APT29 (antes conocido como UNC2452), un actor de amenazas cuyo objetivo se considera coherente con los intereses estratégicos rusos[11]. Entre las víctimas afectadas por APT29 se incluyen organizaciones gubernamentales y empresas de la lista Fortune 500. Una vez más, los atacantes apuntaron a la cadena de suministro de software inyectando un código de puerta trasera en el componente de software Orion, lo que les permitió acceder a los entornos internos de las víctimas y desplegar el malware SUNBURST después de que el código actualizado se expandiera a través de un proceso legítimo.

Los atacantes encontraron la manera de afectar los componentes básicos de nuestra empresa digital. Al atacar y comprometer con éxito un paquete popular utilizado por los desarrolladores de software, es fácil amplificar la propagación del código malicioso directamente a las víctimas a gran escala. Este enfoque hace que los defensores se pregunten si confiamos en nuestra capacidad de defensa. Las organizaciones de todo el mundo se esfuerzan por mantener la visibilidad de su superficie de ataque y la confianza en sus funciones de detección y respuesta. Muy a menudo, las organizaciones no están seguras de su capacidad para detectar y detener rápidamente los ciberataques dentro de su cadena de suministro de software, en parte porque no cuentan con defensores debidamente capacitados y no se activan, ni responden, con la frecuencia necesaria para perfeccionar su capacitación y conocimientos.

7. Mandiant, M Trends 2022
8. Mandiant, M Trends 2022
9. Mandiant, The Defender's Advantage Cyber Snapshot Issue 2, 2022
10. Mandiant Threat Intelligence, "CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators:, septiembre de 2017
11. Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", diciembre de 2020

Los ataques a la cadena de suministro de software están diseñados para abusar de la confianza en proveedores externos con el fin de obtener acceso indirecto al entorno de la víctima y pueden ser difíciles de detectar. En definitiva, los ojos entrenados y el proceso de investigación del analista de seguridad son los factores decisivos para identificar y detener ataques avanzados.

> Los ataques a la cadena de suministro hacen que la confianza existente dificulte enormemente la detección directa del componente malicioso. Contar con una capacidad de detección y respuesta activada y eficaz resulta aún más crítico, ya que un evento sospechoso detectado en las fases posteriores del mismo ciclo de vida del ataque permite a los analistas descubrir el implante de forma indirecta, revirtiendo las acciones de los atacantes a través de la investigación.
>
> —Steve Ledzian VP, CTO-APAC, Mandiant

Detección e investigación desde el punto de vista de un analista sobre el ataque a la cadena de suministro de software

A mediados de octubre de 2021, los analistas de seguridad del servicio gestionado de detección y respuesta de Mandiant identificaron varios eventos que parecían ser un envenenamiento de repositorios de código abierto. El siguiente caso describe su proceso de detección e investigación, y las preguntas que intentaban responder, en relación con los paquetes alojados en Node Package Manager (NPM), el gestor de paquetes de la plataforma JavaScript Node.js.

Un pequeño equipo de analistas de seguridad de Mandiant detectó inicialmente varias alertas que indicaban que se estaba utilizando una utilidad nativa de Windows **CERTUTIL.EXE** para descargar cargas útiles desde una URL común **(hxxps://citationsherbe[.]at/sdd.dll)**. A medida que más analistas del Centro de operaciones de seguridad (Security Operations Center, SOC) comenzaron a detectar alertas similares, el equipo empezó a trabajar codo a codo en busca de respuestas a sus preguntas de investigación.

¿Qué es? ¿Cómo llegó a descargarse en el sistema?

Las primeras preguntas de investigación que hay que responder son: "¿Qué malware está presente y cuáles son sus capacidades?" y "¿Cómo llegó al sistema?". Los analistas adquirieron la carga útil de los hosts iniciales para determinar la funcionalidad y las capacidades del binario sospechoso. El análisis de triaje indicó que el binario era una variante del malware DANABOT, cuyo objetivo es robar credenciales mediante la comunicación con un servidor de control y comando (C2) controlado por el atacante. Utilizando la dirección C2 del malware, los analistas comenzaron a examinar más detenidamente el entorno e identificaron otros sistemas que se comunicaban con la infraestructura del atacante. Este proceso permite que los analistas puedan determinar si el mismo malware o uno similar puede haberse implementado en otros sistemas sin recibir la alerta correspondiente. Una vez confirmado que la carga útil es malware, el equipo de analistas procede a contener los hosts comprometidos de forma remota o iniciando la actuación del equipo de respuesta ante incidentes.

DANABOT es una puerta trasera escrita en Delphi que se comunica utilizando un protocolo binario personalizado a través de TCP. La puerta trasera implementa un marco de plugins que le permite agregar capacidades a través de plugins descargados. Las capacidades de DANABOT incluyen el control total del sistema utilizando un plugin VNC o RDP, captura de video y pantalla, keylogging, ejecución arbitraria de comandos shell y transferencia de archivos. El plugin proxy de DANABOT le permite redirigir o manipular el tráfico de red asociado a los sitios web objetivo. Esta capacidad suele utilizarse para captar credenciales o datos de pago. DANABOT también puede extraer credenciales almacenadas asociadas a navegadores web y clientes FTP.

"ua-parser-js" es un paquete liviano y pequeño que se implementa dentro de una aplicación web o del lado del servidor para extraer y filtrar los datos relevantes necesarios para analizar una cadena de Agente de usuario (es decir, Navegador, Motor, Sistema operativo, CPU y Dispositivo).

¿Cómo llegó hasta allí?

Para comprender cómo se implementó el malware, los analistas suelen basarse en los datos recopilados por las tecnologías de detección y respuesta en puntos finales (endpoint detection and response, EDR). Revisando la telemetría EDR, los analistas rastrearon la actividad hasta comandos legítimos ejecutados por los usuarios para actualizar paquetes NPM.

Una investigación minuciosa reveló que cada uno de los hosts afectados tenía un archivo similar guardado en el directorio **UA-PARSER-JS PACKAGE**, lo que llevó a los analistas a pensar que estaba comprometido y propagaba malware. La modificación maliciosa del directorio JS Package incluía un paso de instalación previa en el proceso de instalación del paquete, lo cual descargaba el malware. Al revisar el script comprometido, los analistas descubrieron que también descargaba e implementaba coinminers (también llamados mineros de criptomonedas) en el host. Los analistas comprobaron los problemas de GitHub correspondientes al repositorio del paquete y encontraron una pregunta que alguien había hecho acerca de si el paquete se había visto comprometido muy recientemente. Según una incidencia de GitHub registrada el 22 de octubre de 2021, aproximadamente a las 12:15 UTC, el paquete de NPM **"ua-parser-js"**, una popular biblioteca de Node.js que acumulaba más de 7 millones de descargas semanales, fue comprometido para propagar malware. El actor pudo publicar tres versiones maliciosas del paquete apropiándose de la cuenta NPM del autor. Según el registro Git del repositorio, el 22 de octubre, entre las 16:14 UTC y las 16:25 UTC, el autor del paquete envió una versión limpia de los paquetes maliciosos para evitar más ataques.

¿Qué otras actividades realizó este actor de amenazas?

Una vez que los hosts fueron contenidos, los analistas continuaron con la investigación para determinar la causa raíz del ataque. Revisando el registro git del repositorio de paquetes, los analistas encontraron marcas de tiempo de cuándo se introdujo el cambio malicioso y cuándo se aplicó la corrección unas horas más tarde. Un análisis más exhaustivo de las TTP del atacante permitió al equipo vincular otros paquetes de NPM, comprometidos por el mismo atacante, y determinar el alcance de la actividad realizada por el actor. El equipo logró atribuir la actividad a UNC3379 con una confianza razonable, analizar el malware, documentar el comportamiento del atacante y desarrollar técnicas de detección para impedir futuras actividades.

Para obtener más información sobre este ataque a la cadena de suministro de software, consulte el blog de investigación No Unaccompanied Miners: Compromisos de la cadena de suministro a través de los paquetes Node.js.

Confiar en el instinto, el pensamiento crítico y la experiencia de los analistas

Sin importar la escala de la investigación, el tiempo es esencial. Mandiant confía en el conocimiento, la capacitación y el pensamiento crítico de nuestros analistas para investigar y responder. Nuestro equipo actúa como un detective, aprovechando las pistas, pruebas y artefactos forenses para descubrir la historia que hay detrás de cada incidente. El objetivo del proceso de investigación es responder a preguntas fundamentales sobre el ataque para determinar:

- Alcance de la intrusión
- Si aún sigue en curso
- Fecha más temprana del ataque y causa de la intrusión
- Tipo y alcance de los datos expuestos
- Identidad y motivos del actor de amenazas

Comprender estos factores sobre la intrusión guiará su contención, erradicación y recuperación. Gracias a la experiencia en primera línea, simulacros y capacitación, Mandiant recomienda capacitar a sus analistas para que dirijan las investigaciones y tomen decisiones fundamentales sobre los plazos y la ejecución de la contención y la erradicación. "Es común que las organizaciones que se encargan de su propia investigación y respuesta ante incidentes se precipiten a la hora de solucionar el problema", afirma Eric Scales, vicepresidente de Mandiant. "Cuanto más se conozca sobre el ataque, mayor será el éxito para su erradicación y recuperación".

En el caso que aquí se presenta, la investigación dirigida por analistas de Mandiant MDR desarrolló indicadores atómicos clave relacionados con la actividad, realizó un triaje del malware implementado para determinar las medidas de corrección adecuadas y, utilizando nuestro amplio conocimiento e investigación sobre el grupo de amenazas, exploró con éxito los entornos de nuestros clientes para descubrir actividad maliciosa adicional relacionada con esta campaña que no fue detectada por sus productos de detección y respuesta de endpoints (EDR).

Activación de la ciberdefensa en torno a los objetivos de rendimiento de la ciberseguridad intersectorial de CISA

Los actores de amenazas de Estados nación continúan persiguiendo las tecnologías de infraestructuras críticas. El año pasado, Mandiant comunicó el descubrimiento de herramientas que permiten a los atacantes buscar, comprometer y controlar determinados sistemas de control industrial (industrial control systems, ICS) o dispositivos de control de supervisión y adquisición de datos (supervisory control and data acquisition, SCADA) una vez que han establecido el acceso en una red de tecnología operativa (operational technology, OT)[12]. A medida que las infraestructuras industriales y críticas se conectan cada vez más a la red, la mayor complejidad de las amenazas aumenta la necesidad de actualizar las directrices de ciberseguridad para las infraestructuras críticas. La Agencia de ciberseguridad e infraestructuras (Cybersecurity and Infrastructure Agency, CISA), los Institutos nacionales de normas y tecnología (National Institutes of Standards and Technology, NIST) y la comunidad interinstitucional desarrollaron objetivos de ciberseguridad coherentes en todos los sectores de infraestructuras críticas.

En octubre de 2022, CISA publicó los Objetivos de rendimiento de ciberseguridad intersectoriales (Cybersecurity Performance Goals, CPG)[13] como guía para ayudar a las organizaciones a identificar y priorizar las prácticas de ciberseguridad más importantes. Los CPG de CISA pretenden ser una línea de base para abordar los desafíos de ciberseguridad a los que se enfrentan las organizaciones día a día. Tienen la intención de avanzar hacia el objetivo compartido de reducir los riesgos cibernéticos para defender mejor las infraestructuras críticas de nuestro país, como hospitales, proveedores de energía, sistemas de transporte y grandes fábricas.

Mandiant adopta las directrices de los CPG de CISA para crear un punto de partida que minimice los riesgos. Los CPG constituyen una primera iteración de los objetivos del Memorando de seguridad nacional (National Security Memorandum, NSM-5): Mejora de la ciberseguridad de los sistemas de control de infraestructuras críticas. Son un paso importante, no un programa integral de ciberseguridad, para iniciar la trayectoria hacia una práctica de ciberseguridad más sólida.

12. Mandiant, INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, 13 de abril de 2022
13. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

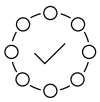
Los CPG sirven de base, no de límite, para mitigar los riesgos cibernéticos. Entre sus principales características destacan:

Subconjunto asignado de prácticas de ciberseguridad

Directrices pertinentes específicas para TI y OT

Prácticas prioritarias para mitigar los riesgos

Informado por las amenazas observadas por CISA y sus socios gubernamentales e industriales



Aplicable a todos los sectores de IC (infraestructuras críticas)

Los CPG señalan acciones y elementos específicos relacionados con OT e ICS como una manera de ayudar a estas organizaciones a defender mejor sus infraestructuras críticas.

Sin importar cuál sea el tamaño de la organización, proteger la infraestructura crítica requiere comprender las ciberamenazas relevantes, las pruebas rigurosas de la seguridad y la detección y respuesta ante amenazas realizadas en toda la empresa. Los CPG ayudan a las organizaciones a pensar en cómo dirigir la inversión hacia los resultados de seguridad que más las afectan, teniendo en cuenta al mismo tiempo el presupuesto, el personal y la experiencia. Invertir en prácticas para aplicar los CPG "ayudará a abordar de manera significativa los riesgos significativos para la seguridad, la salud y los medios de vida de los estadounidenses".[14]

14. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022.

Conocer las ciberamenazas relevantes

Los CPG guían a las organizaciones para mantenerse al tanto de las amenazas relevantes y aprovechar las tácticas, técnicas y procedimientos (tactics, techniques, and procedures, TTP) de los atacantes para detectar los ataques en curso. Comprender las ciberamenazas relevantes es primordial en el enfoque de Mandiant respecto a la seguridad de OT, en el que guiamos a los clientes para mejorar las capacidades de detección de amenazas tanto de las redes de TI como de OT, con total conocimiento de la situación[15]. Creemos que los defensores y los responsables de la respuesta ante incidentes deberían prestar mucha más atención a los métodos de intrusión, o TTP, a lo largo del ciclo de vida del ataque, la mayoría de los cuales están presentes en lo que llamamos "sistemas intermedios", en su mayoría sistemas que cruzan los límites de la red de TI y OT o aquellas estaciones de trabajo y servidores en red dentro de la red de OT que utilizan sistemas operativos y protocolos similares (o iguales) a los utilizados en TI. Centrarse en los métodos de intrusión es eficaz porque la mayoría de los ataques sofisticados contra la OT aprovechan estos sistemas intermediarios como trampolín hacia su objetivo final.

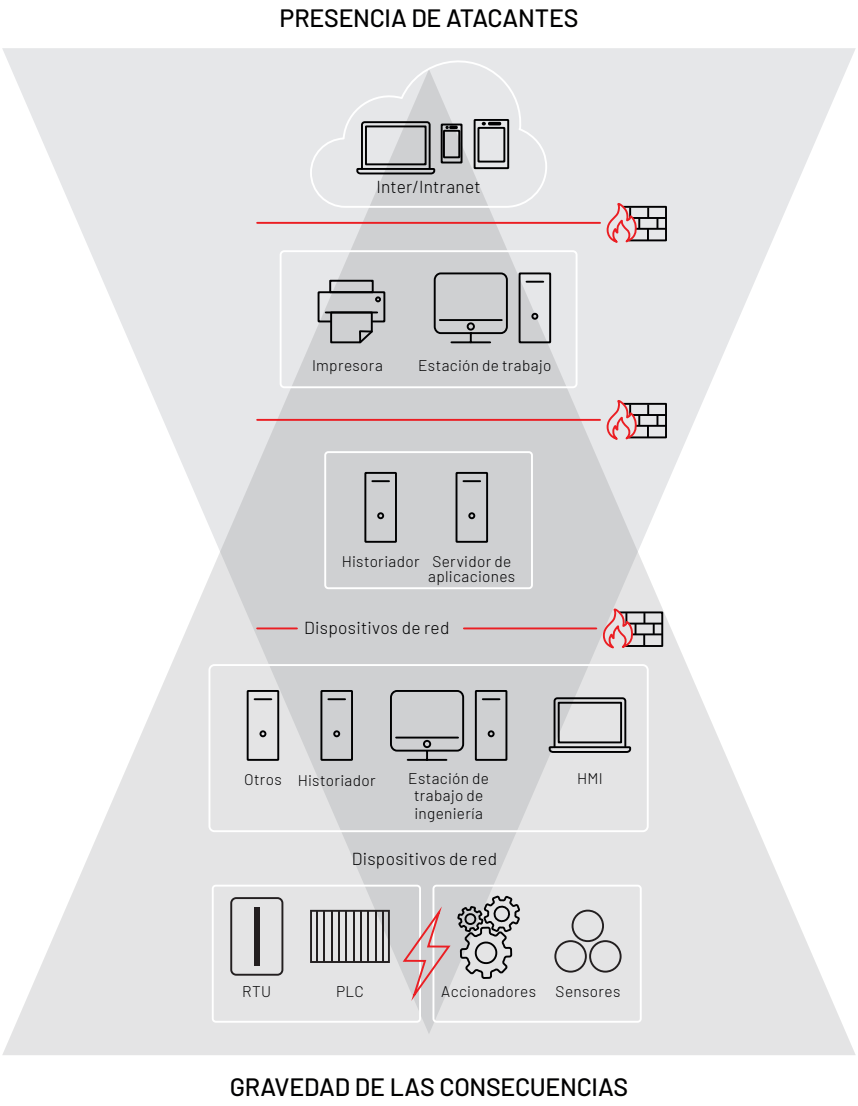


Figura 1. El embudo de oportunidades para detectar amenazas de OT.

15. Mandiant, The Mandiant Approach to Operational Technology Security, diciembre de 2019.

La mejor oportunidad para detectar a un atacante de OT se encuentra en la intersección entre los dos triángulos de la Figura 1[16]. Es aquí donde el equilibrio entre la presencia del atacante y la consecuencia operativa de una intrusión hace que sea más fácil y significativo para las organizaciones de seguridad identificar la actividad de las amenazas. Los defensores deben comprender los métodos de intrusión de los atacantes y aprovechar ese conocimiento para cazar y detectar amenazas avanzadas. La caza de amenazas cerca de la DMZ de OT y del Sistema de control distribuido (Distributed Control System, DCS) puede ser más eficiente, ya que las características detectables de la intrusión todavía están presentes y la gravedad de las posibles consecuencias de la intrusión es alta, pero todavía no es crítica.

16. Mandiant, The Mandiant Approach to Operational Technology Security, diciembre de 2019.

2022

En 2022, Mandiant detectó la exposición de documentación confidencial de OT y redes en ataques de extorsión mediante ransomware[17]. La exposición de datos confidenciales de OT a través de ransomware o cualquier tipo de filtración de datos permite a los actores sofisticados obtener información sobre los objetivos, específicamente sobre la infraestructura, activos, debilidades de seguridad y procesos de la víctima. Los actores de amenazas utilizan este tipo de datos de reconocimiento para crear ataques más significativos y precisos.

TABLA 2: Documentación expuesta en ataques de extorsión mediante ransomware

Víctima (nombres suprimidos)	Contenido de la filtración
Fabricante de trenes industriales y de pasajeros	Credenciales de administración de contraseñas de un fabricante de equipos originales, requisitos de la arquitectura de control y canales de comunicación para un vehículo tranviario europeo, copias de seguridad de los archivos de proyectos PLC de Siemens TIA Portal, etc.
Dos organizaciones petroleras y de gas	Documentación detallada de redes y procesos, incluidos diagramas, HMI, hojas de cálculo, etc.
Integrador de sistemas de control	Documentación de ingeniería de proyectos de clientes (algunos archivos estaban protegidos por contraseña, que no intentamos eludir).
Productor de energía hidroeléctrica	La mayoría de los datos estaban relacionados con las finanzas y la contabilidad, pero identificamos una lista de nombres, correos electrónicos, privilegios de usuario y algunas contraseñas de empleados de TI, mantenimiento de planta y operaciones.
Proveedor de servicios de rastreo de vehículos por satélite	Diagramas de productos, visualizaciones y código fuente de una plataforma propia utilizada para rastrear flotas de automóviles a través del Sistema de posicionamiento global (Global Positioning System, GPS).
Productor de energía renovable	Contratos legales entre la víctima y los clientes donde se establecen las condiciones de mantenimiento y suministro de la infraestructura de energía renovable. Los contratos establecían que el proveedor de servicios podía acceder libremente al sistema SCADA del tercero a través de direcciones IP públicas de Internet.

- Aplicar políticas sólidas de manipulación de datos a los empleados y subcontratistas que tengan contacto con datos de todos los segmentos de la red para garantizar la protección de la documentación interna.
- Evitar almacenar datos operativos muy sensibles en redes menos seguras.
- Prestar especial atención al seleccionar subcontratistas que apliquen programas de seguridad completos para proteger los datos operativos.
- Las víctimas de intrusiones de ransomware deben evaluar el valor de los datos filtrados para determinar qué controles compensatorios pueden ayudar a reducir los riesgos de nuevas intrusiones.
- Cambiar las credenciales y claves API que se hayan filtrado. Contemplar la posibilidad de cambiar las direcciones IP expuestas de los sistemas críticos y servidores de acceso directo de OT.
- Realizar periódicamente ejercicios de simulación de ataque para identificar la información interna expuesta externamente e insegura.

17. Mandiant, 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information, enero de 2022

Pruebas de seguridad rigurosas

Una de las principales medidas para mejorar con confianza la seguridad de las redes TO es probar los controles de seguridad en cada capa de la red TO de forma segura contra los ataques más frecuentes y las familias de malware dirigidas a activos críticos. Los CPG de CISA recomiendan la validación periódica de terceros respecto de la eficacia y cobertura de las ciberdefensas de una organización.

Mandiant recomienda un programa personalizado que se adapte a las necesidades de evaluación de la organización. Un programa integral de pruebas para OT es más eficaz si se realiza desde el punto de vista de los atacantes, aprovecha la simulación y emulación para mitigar el impacto en las operaciones en tiempo real, e incorpora una combinación adecuada de equipo de simulación de ataque, equipo de integración, pruebas de penetración y pruebas de seguridad de redes y componentes. En los casos en los que las pruebas proactivas no son admisibles, debido a los requisitos de tiempo de actividad operativa de los entornos de OT de producción, Mandiant recomienda realizar evaluaciones técnicas que valoren la eficacia de la segmentación de la red, controles de acceso, sistemas de supervisión de la red, políticas de dispositivos transitorios y capacidades de respuesta ante incidentes. Las pruebas continuas no se limitan a evaluar la eficacia de los controles de seguridad en un momento dado, sino que también ayudan a detectar problemas de seguridad complejos en redes integradas (de TI a OT) antes de que un atacante los aproveche. La validación continua también puede preparar al equipo de la organización para supervisar y detectar incidentes cibernéticos y responder a ellos. Las organizaciones deben esperar de estos programas recomendaciones tácticas para mitigar los hallazgos críticos, recomendaciones estratégicas para mejoras a largo plazo e identificación de deficiencias en la capacidad del personal para supervisar y responder ante incidentes de OT.

Los servidores de comunicaciones de plataforma abierta permiten intercambiar datos similares e independientes del fabricante entre máquinas, dispositivos y sistemas del entorno industrial.

Respuesta y recuperación

En la sección 7, los CPG de CISA destacan la necesidad de que las organizaciones mantengan, practiquen y actualicen planes de respuesta ante incidentes de ciberseguridad en casos de amenazas relevantes. La experiencia de Mandiant en la primera línea de respuesta ante incidentes de OT de gran repercusión, como TRITON e INCONTROLLER, permite comprender mejor la diferencia entre la respuesta ante incidentes de TI y de OT, así como las herramientas y procedimientos necesarios para dar una respuesta de OT.

Si bien los objetivos de remediación y contención (eliminar la amenaza del entorno y restablecer las condiciones normales de funcionamiento de los sistemas) son iguales en los entornos de TI y OT, las herramientas pueden ser muy diferentes. El personal de TI suele utilizar la tecnología de detección y respuesta de endpoints para ayudar en la investigación, contención y recuperación o remediación. Estas herramientas no suelen instalarse en servidores o componentes de redes de OT.

La contención en TI es relativamente sencilla y a menudo mucho menos perjudicial de lo que puede ser en entornos complejos de OT. Por ejemplo, detener e iniciar funciones específicas o incluso eliminar todo un sistema de la red de TI es una práctica común. Estas acciones pueden ser más potentes cuando se llevan a cabo en un componente de TO. Antes de iniciar o detener procesos o de desconectar un componente sin que ello afecte a las operaciones, debe contarse con un conocimiento exhaustivo de los procesos subyacentes, lo que puede acarrear un tiempo de inactividad significativo o un riesgo potencial para la seguridad de la vida personas. Los servidores de comunicación de plataforma abierta (Open Platform Communication, OPC), por ejemplo, pueden afectar a toda la línea de fabricación durante semanas si se desconectan al azar. La planificación detallada, al margen de la respuesta activa ante un incidente, ayuda a los propietarios de los sistemas a tomar decisiones basadas en el riesgo según el tiempo de inactividad potencial, la pérdida de producción o los riesgos para la seguridad de la vida. La capacidad de la organización para comprender los objetivos y metas de los posibles atacantes puede ayudar a guiar al propietario del sistema a la hora de tomar decisiones más seguras y menos arriesgadas.

Por último, las redes de TO constan de muchas subredes gestionadas por proveedores a las que la organización no tiene acceso directo. Mandiant recomienda desarrollar planes de respuesta y manuales para incorporar sistemas de terceros y probarlos junto con dichos proveedores. No cabe duda de la importancia de contar con un plan, y ponerlo en práctica, para resolver los incidentes de ciberseguridad de forma rápida, eficaz y a gran escala.

Mandiant asigna las ofertas de seguridad de OT a las Cinco funciones del marco de ciberseguridad de NIST[18], que los CPG de CISA pretenden complementar, adaptando los servicios al ciclo de vida de la gestión de riesgos de ciberseguridad de una organización.

18. NIST, Cybersecurity Framework, The Five Functions, mayo de 2021

		IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Inteligencia	Suscripción de inteligencia					
	Analista especializado en inteligencia					
	Servicio de evaluación de vulnerabilidades					
	Análisis personalizado y evaluación de la caja negra					
Asesoramiento	Diagnóstico de fallas					
	Evaluación del programa de seguridad					
	Pruebas de ataque y penetración					
	Planificación de respuesta ante incidentes					
	Respuesta ante incidentes					
	Capacitación sobre seguridad					
	Asesor especializado					
Defensa gestionada para OT	Inicio rápido					
	Supervisión continua					
Tecnología de terceros	Supervisión de protocolos de red de OT					

Figura 2. Ofertas de Mandiant específicas para OT

Mandiant ofrece perspectivas de ciberseguridad de primera línea con un amplio conocimiento funcional de los sistemas de control industrial adquirido a lo largo de décadas de trabajo práctico en entornos de ICS y OT. Los expertos en OT de Mandiant realizan pruebas de seguridad avanzadas para ayudar a las organizaciones industriales a mejorar sus capacidades de mitigación y detección en las redes de OT de extremo a extremo. Deje que ayudemos a su organización a planificar los CPG de CISA para crear un entorno de OT más seguro y aumentar su preparación cibernética.

Reflexiones finales

Esta edición de la Mirada a la Ventaja del Defensor enseña a las organizaciones que están empezando a pasar de las contraseñas tradicionales y la autenticación multifactor (multi-factor authentication, MFA) a la implementación de la autenticación sin contraseña a crear métodos de MFA sólidos y a contemplar el inicio de sesión único de terceros para ayudar a gestionar la autenticación back-end en todos sus dispositivos y aplicaciones. Aconsejamos a quienes exploran el mercado volátil de los seguros cibernéticos, y les recomendamos incluir asesoramiento y gestión de riesgos a la hora de elaborar las solicitudes de suscripción, revisar detenidamente el modelo de póliza y considerar a sus proveedores de seguros como un socio en la gestión global de riesgos.

También demostramos la manera en que las seis funciones críticas de la ciberdefensa descritas en La Ventaja del Defensor coinciden con las directrices proporcionadas por la Agencia de ciberseguridad e infraestructura de los Estados Unidos (U.S. Cybersecurity and Infrastructure Agency, CISA) en su reciente publicación de los Objetivos de rendimiento de la ciberseguridad intersectorial (Cross-Sector Cybersecurity Performance Goals, CPG). Se trata de prácticas de ciberseguridad que los propietarios y operadores de infraestructuras críticas pueden aplicar para reducir significativamente los riesgos. Asimismo, destacamos un caso práctico que ejemplifica las tácticas desplegadas por un SOC optimizado en el que los analistas investigan las alertas relevantes como una investigación unificada y se basan en la capacitación, experiencia y pensamiento crítico de los analistas para investigar un ataque a la cadena de suministro.

El conocimiento es una de nuestras mayores ventajas en la lucha contra los adversarios cibernéticos. La Mirada a la Ventaja del Defensor está diseñada para proporcionar precisamente eso: conocimiento e información capaz de orientar a los equipos de seguridad y permitir a los responsables tomar decisiones inteligentes. La industria de la ciberseguridad debe compartir información y trabajar de forma unida para ayudar a los agentes implicados en la lucha, la Mirada a la Ventaja del Defensor es solo una forma en la que Mandiant respalda la causa.

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

Mandiant es un líder reconocido en defensa cibernética dinámica, inteligencia de amenazas y servicios de respuesta ante incidentes. Gracias a décadas de experiencia en primera línea, Mandiant ayuda a las organizaciones a confiar en su preparación para defenderse y responder a las ciberamenazas. Mandiant ahora parte de Google Cloud.

MANDIANT
AHORA PARTE DE Google Cloud