FIREEYE | MANDIANT

M-TRENDS 2021

FIREEYE MANDIANT SERVICES | SONDERBERICHT

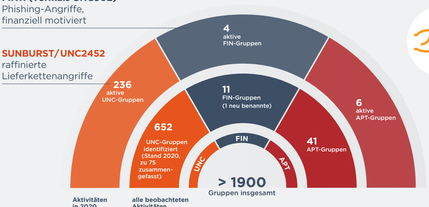
Cybersicherheits-Trends, die sich bei den Incident-Response-Untersuchungen und -Einsätzen von Mandiant zwischen dem 1. Oktober 2019 und dem 30. September 2020 abzeichneten

WER DIE ANGREIFER SIND

Aktuelle Hackergruppen

FIN11 (vormals UNC902)
Phishing-Angriffe, finanziell motiviert

SUNBURST/UNC2452
raffinierte Lieferkettenangriffe



UNC: *unkategorisierte Angreifer*
FIN: *finanziell motivierte Angreifer*
APT: *Angreifer hinter Advanced Persistent Threats*

Angreifer arbeiten heutzutage häufiger zusammen, um ihre Ziele zu erreichen.

Mehrere Hackergruppen in einer Umgebung identifiziert

2020 **29%**

2019 **15%**

WAS SIE IM VISIER HABEN

Die am häufigsten angegriffenen Branchen

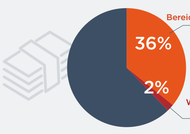
Unternehmens-dienstleistungen | Einzelhandel, Hotel- und Gaststättenge-werbe | Gesundheitswesen | Hightech | Finanzwesen

Gruppen, die gezielt pandemierelevante Branchen angreifen
APT32, APT41, UNC788, UNC2062

WORAUF SIE AUS SIND

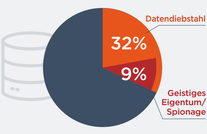
Gezielte Angriffe

Ziel: Bereicherung



Direkte *Bereicherung schließt Erpressung, Lösegeldforderungen, den Diebstahl von Zahlungskartendaten und illegale Überweisungen ein.*

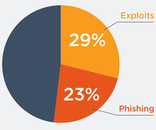
Ziel: Datendiebstahl



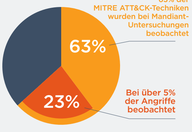
WIE SIE ANGREIFEN

Am häufigsten verwendete Techniken

Erster Angriffsvektor
(sofern identifiziert)



MITRE ATT&CK



MITRE ATT&CK® *ist eine weltweit verfügbare Wissensdatenbank mit Taktiken und Techniken, die bei realen Angriffen beobachtet wurden.*

Häufig angegriffene Technologien

88% Remote Desktop Protocol (T1021.001) bei Angriffen über **Fernzugriffsdienste (T1021)**
Bei 25% aller Angriffe betroffen

100% Windows-Dienste (T1569.002) bei Angriffen über **Systemdienste (T1569)**
Bei 31% aller Angriffe betroffen

80% PowerShell (T1059.001) bei Angriffen über **Befehls- oder Skriptinterpreter (T1059)**
Bei 41% aller Angriffe betroffen

Steiler Anstieg bei Ransomware

Bei jedem vierten Incident-Response-Einsatz von Mandiant spielte Ransomware eine Rolle.

2020 **25%**

2019 **14%**

Medianwert der Verweildauer (global)

Ransomware-Untersuchungen

2020
5 Tage

Sonstige Untersuchungen

2020
45 Tage

Alle Untersuchungen

2020
24 Tage

WANN WIR SIE FINDEN

Medianwert der Verweildauer (global)

2011	2012	2013	2014	2015	2016	2017	2018	2019
416	243	229	205	146	99	101	78	**56**

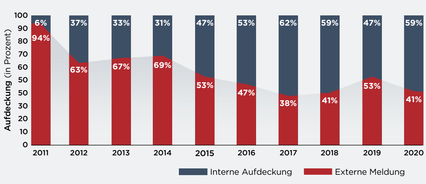
Als Verweildauer *wird der Zeitraum bezeichnet, während dessen ein Angreifer Zugang zu einer Umgebung hat, bevor er erkannt wird. Der Medianwert ist der Wert in der Mitte eines sortierten Datensatzes.*

WIE WIR SIE FINDEN

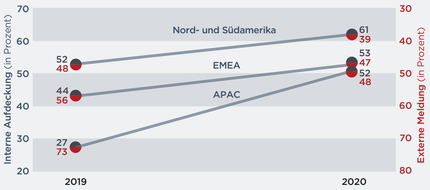
Aufdeckung weltweit nach Quelle: 2011–2020

Als interne Aufdeckung *bezeichnen wir Fälle, in denen ein Angriff im Unternehmen selbst erkannt wird.*

Externe Meldung *heißt, dass das Unternehmen von Dritten über den Angriff informiert wird.*



Aufdeckung nach Region und Quelle: 2019 und 2020



Weitere Einzelheiten, Schlussfolgerungen und Informationen über Abwehrstrategien finden Sie im vollständigen Bericht unter
www.fireeye.de/current-threats/annual-threat-report/mtrends.html

Offenlegung: Die Fallstudien und Beispiele stammen aus unseren Einsätzen bei diversen Kunden und repräsentieren nicht unsere Tätigkeit für einen bestimmten Kunden oder eine spezifische Kundengruppe. In vielen Fällen wurden die Fakten abgewandelt, um die Identität unserer Kunden und der mit diesen in Verbindung stehenden Einzelpersonen zu schützen.

FIREEYE | MANDIANT