# Allgemeine Lage der Schadsoftware im Jahr 2019

Präsentiert von

Malwarebytes LABS

# Inhalt

# Zusammenfassung

2018 began mit einem Paukenschlag und endete – nun ja, mit einem weiteren Paukenschlag. Man kann getrost behaupten, dass dieses Jahr – trotz eines eher ereignislosen zweiten Quartals (die berühmte Ruhe vor dem Sturm) – von Anfang bis Ende actiongeladen war. Unmittelbar nach einer wahren Cryptomining-Explosion im letzten Quartal 2017 begannen die Bedrohungsakteure Anfang 2018 damit, ihre Cryptomining-Taktiken zu diversifizieren, indem sie ihre Angriffe auf Android und Mac ausdehnten, Cryptomining-Schadsoftware in Umlauf brachten und mit Innovationen bei den browserbasierten Angriffen aufwarteten.

Zwar ebbte das Cryptomining im zweiten Quartal ab, aber dafür stand schon eine neue Bedrohungsart in den Startlöchern, um die Stelle des Cyptomining einzunehmen: die sogenannten Information-Stealer. Diese ehemaligen Banking-Trojaner – hier sind insbesondere Emotet und TrickBot zu nennen – haben sich zu Dropper-Trojanern mit zahlreichen Modulen zur Erzeugung von Spam und zur lateralen Verbreitung in Netzwerken sowie zu Daten-Skimmern und sogar Cryptowallet-Stealern weiterentwickelt. Diese Schadsoftware-Varianten zielten vor allem auf Unternehmen ab, da sich hier durch den Diebstahl hochsensibler Daten, die auf dem Schwarzmarkt für zukünftige Re-Targeting-Kampagnen verkauft werden können, die höchsten Profite erzielen lassen.

Und da wir gerade von Unternehmen als Opfern sprechen – andere Schadsoftware-Familien traten schon bald in die Fußstapfen von Emotet und TrickBot und nahmen ebenfalls Unternehmen aufs Korn, deren Netzwerke nicht gepatcht und unsicher waren. Tja, sie haben eine Unmenge an Zielen gefunden. Von massiven Verletzungen der Datensicherheit bis hin zu Ransomware-Angriffen, die kritische Infrastrukturen lahmlegten. Letztendlich erlebten Unternehmen 2018 all das, womit Privatanwender schon seit Jahren zu kämpfen haben – allerdings in einem wesentlich größeren und gefährlicheren Maßstab.

Und so endete 2018 damit, dass die verschiedenen Benutzergruppen mit ihren jeweils eigenen Problemen zu kämpfen hatten, und mit dem Versprechen, dass 2019 aller Wahrscheinlichkeit nach mindestens genauso dramatisch wird wie das Vorjahr.

## Methodik

Im Gegensatz zu unseren vierteljährlichen Berichten zu Taktiken und Methoden der Internetkriminalität, die detailliert auf die im Zeitraum von drei Monaten erfassten Metriken eingehen, vergleicht unser jährlicher Überblick über die Schadsoftware die Monate von Januar bis November 2018 mit dem gleichen Zeitraum im Jahr 2017. Wir kombinieren dabei die von unseren Forschern zusammengetragenen Informationen mit den Daten, die wir über Honeypots, virtuelle Sandkästen und unser Telemetriesystem für Unternehmens- und Privatanwenderprodukte erfasst haben. All diese Daten dienen uns dazu, die wichtigsten Bedrohungen des Jahres zu identifizieren und festzustellen, wohin der Trend geht, was Menge und Verbreitung anbelangt.

Außerdem geht unser jährlicher Bericht auf die Bedrohungen nach Regionen – Nordamerika/asiatisch-pazifischer Raum/Lateinamerika, Europa/Naher Osten und Afrika (EMEA) – sowie auf die wichtigsten vertikalen Branchen ein, die Ziel der produktivsten Formen von Schadsoftware sind.

Doch genug der einleitenden Worte – erfahren Sie nun, was wir über die allgemeine Lage der Schadsoftware im Jahr 2018 herausgefunden haben.

# Die 10 wichtigsten Erkenntnisse

## Cryptominer auf dem Vormarsch

In der ersten Jahreshälfte 2018 wurde Ransomware durch eine massive Flut von Cryptominern, zu der es nach dem kometenhaften Anstieg des Bitcoin-Wertes gegen Ende 2017 kam, von ihrem Thron gestoßen. Es schien, als hätten die Bedrohungsakteure alle anderen Arten von Angriffen aufgegeben, um mit dieser neuen Technik zu experimentieren. Dabei ließen sie nichts aus – gleichgültig, ob Desktops oder Mobilgeräte, Mac-, Windows- und Android-Betriebssysteme oder software- und browserbasierte Angriffe. Allerdings nahm die Zahl der Cryptomining-Erkennungen im Verlauf des Jahres nur um sieben Prozent zu – ein relativ bescheidener Anstieg, der darauf zurückzuführen war, dass die zweite Jahreshälfte eher ruhig verlief, was diese Bedrohungsart anbelangt.

## Das Jahr der Mega-Sicherheitsverletzungen

Im Gegensatz zu den Ransomware-Plagen, die 2017 kennzeichneten, kam es 2018 zu keinen größeren globalen Ausbrüchen. Stattdessen war es das Jahr der Mega-Sicherheitsverletzungen. Angreifer drangen in die Netze großer Unternehmen – wie u. a. Facebook, Marriott, Exactis, MyHeritage und Quora – ein, wodurch Millionen von Kunden betroffen waren. Die Anzahl der gehackten Datensätze nahm 2018 im Vergleich zum Vorjahr um sage und schreibe 133 Prozent zu.

## Ransomware wird immer raffinierter

2018 konnten wir bei den Angriffstechniken der Ransomware einen Wandel beobachten. Statt des Doppelangriffs mit Malvertising Exploits, durch die Ransomware Payloads eingeschleust wurden, verlegten sich die Bedrohungsakteure auf gezielte, manuelle Angriffe. Das Gießkannenprinzip wurde durch Brute-Force-Angriffe ersetzt, wie bei den erfolgreichsten SamSam-Kampagnen 2018 zu beobachten war.

## Unternehmen mussten Schläge einstecken

Die Autoren von Schadsoftware machten in der zweiten Hälfte 2018 eine Kehrtwende und zielten statt auf Privatanwender auf Unternehmen ab. Ihnen war klar geworden, dass Unternehmen weitaus lohnendere und gewinnträchtigere Opfer sind als Einzelpersonen. Die Gesamtzahl der Schadsoftware-Erkennungen bei Unternehmen stieg im letzten Jahr beträchtlich – satte 79 Prozent, um genau zu sein. Das war primär auf die Zunahme von Backdoor-Programmen, Minern, Spyware und Information-Stealern zurückzuführen.

## Erkennungen bei Privatanwendern sinken geringfügig

Obwohl Unternehmen als Angriffsziele in den Mittelpunkt gerückt sind, hat die Zahl der Schadsoftware-Erkennungen bei Privatanwendern im Verlauf des Jahres nur um drei Prozent abgenommen. Der Grund dafür ist auch hier die Zunahme von Schadsoftware wie Backdoor-Programmen, Trojanern und Spyware, zu der es 2018 gekommen ist. Während 2017 insgesamt 775.327.346 Erkennungen bei Privatanwendern zu verzeichnen waren, kam es 2018 zu rund 25 Millionen weniger Infektionen. Das ist ein zahlenmäßig beträchtlicher Rückgang, wenn man die Prozentsätze einmal beiseite lässt.

## SMB-Schwachstellen verbreiten Trojaner wie ein Lauffeuer

Von der NSA genutzte Exploits, die 2017 von der Gruppe „The Shadow Brokers“ als Angriffsmöglichkeit veröffentlicht wurden, machten auch 2018 von sich reden, da Internetkriminelle die SMB-Schwachstellen EternalBlue und EternalRomance nutzten, um gefährliche und raffinierte Trojaner wie Emotet und TrickBot zu verbreiten. Tatsächlich ging 2018 die größte Bedrohung für Privatanwender und Unternehmen von den Information-Stealern aus, die zudem die wichtigste regionale Bedrohung für Nordamerika, Lateinamerika und die EMEA-Region (Europa, Naher Osten und Afrika) darstellten.

## MalSpam nimmt die Stelle von Exploits als bevorzugter Angriffsvektor ein

Die Exploit-Landschaft verödete gegen Ende 2017 etwas, nachdem zahlreiche Kit-Erzeuger hinter Gittern gelandet waren. Das Ergebnis war, dass die Bedrohungsakteure zu einem alten Favoriten zurückkehrten, nämlich MalSpam. Dadurch wurden 2018 Exploits als wichtigster Mechanismus zur Verbreitung von Bedrohungen abgelöst.

## Betrügerische Erweiterungen und bösartige Apps erscheinen in legitimen Webstores

Die browserbasierte Sicherheit wurde 2018 noch wichtiger, weil betrügerische Apps und Erweiterungen Benutzer und App Stores gleichermaßen an der Nase herumführten und sich mit hinterhältigen Social-Engineering-Taktiken an allen Sicherheitsüberprüfungen vorbei in Google Play, iTunes und die offiziellen Webstores für Chrome, Firefox, Safari und andere einschlichen.

## Diebstahl von Benutzerdaten durch Angriffe auf Websites

Hinter einer Reihe spektakulärer Angriffe auf eCommerce-Websites stand die kriminelle Gruppe „Magecart“. Sie stahlen Kreditkartendaten und andere personenbezogene Informationen (PII) in Klartext und in Echtzeit von Zahlungsplattformen.

## Sexbasierte Erpressungskampagnen (Sextortion)

Und schließlich ist noch eine weitere wichtige Betrugsmasche des vergangenen Jahres zu nennen, bei der sich die Betrüger darauf konzentrierten, alte personenbezogene Informationen zu nutzen, die sie in der Vergangenheit durch Sicherheitsverletzungen erbeutet hatten. Dadurch wurden Millionen von Benutzern mit Phishing-E-Mails überschwemmt, mit dem Ziel, die Opfer zu erpressen (in einigen Fällen ging es sogar um Sextortion). In den Mails wurden alte, aber potenziell noch immer gültige Kennwörter verwendet und den Opfern mitgeteilt, dass man all ihre Geheimnisse aufdecken würde, wenn sie nicht zahlen würden.

# Die wichtigsten Erkennungen im Jahr 2018

## Erkennungen bei Privatanwendern

In unserem im 3. Quartal 2018 veröffentlichten Bericht zu Taktiken und Methoden der Internetkriminalität konnten wir einen Rückgang der gegen Privatanwender gerichteten Bedrohungen feststellen. Betrachtet man das ganze Jahr, zeigt sich, dass es zwischen 2017 und 2018 zu einer leichten Veränderung gekommen ist, was die Gesamtzahl der Schadsoftwareerkennungen anbelangt. Überraschenderweise macht der Rückgang der gegen Privatanwender gerichteten Bedrohungen im Vergleich zum Vorjahr insgesamt nur drei Prozent aus, was darauf zurückzuführen ist, dass die Erkennung von Trojanern, Backdoor-Programmen und Spyware zum Teil stark angestiegen ist.

| Erkennungen bei Privatanwendern 2017/2018 | | |
|---|---|---|
| **Pos.** | **Bedrohung** | **Veränderung J/J in %** |
| **1** | Adware | **-39 %** |
| **2** | Trojaner | **19 %** |
| **3** | Riskware-Tool | **7 %** |
| **4** | Backdoor | **34 %** |
| **5** | HackTool | **-36 %** |
| **6** | Hijacker | **-84 %** |
| **7** | Wurm | **-28 %** |
| **8** | Spyware | **27 %** |
| **9** | Ransomware | **-29 %** |
| **10** | Rogue | **-39 %** |
| **Erkennungen insgesamt** | | |
| **2017** | **775.327.346** | **-3 %** |
| **2018** | **750.296.307** | |

*Abbildung 1: Die 10 wichtigsten von Malwarebytes 2018 bei Privatanwendern erkannten Bedrohungen*

Abgesehen davon konnten wir bei zahlreichen Arten von Schadsoftware, die ausschließlich Privatanwender zum Ziel haben, eine Abnahme beobachten. Im Verlauf des Jahres haben wir festgestellt, dass sich mehr Angriffe gegen Unternehmen richteten und es zu mehr Erkennungen auf ihren Endpunkten gekommen ist. Wir konnten beobachten, dass sich Internetkriminelle nun stärker auf Unternehmen konzentrieren, die sie als lukrativeres Ziel betrachten.

Adware hat beträchtlich abgenommen. Das gilt auch für Hacktools, Hijacker, Würmer, Ransomware und bösartige Schadsoftware. Dieser Rückgang ist höchstwahrscheinlich darauf zurückzuführen, dass diese Arten von Schadsoftware häufig alle zusammen erkannt werden, da sie auf den betroffenen Geräten ähnliche Veränderungen am System vornehmen. So werden viele durch Adware am System vorgenommenen Veränderungen durch unser Tool zur Erkennung von Hijackern identifiziert und behoben – und die Erkennung von Hijackern hat um 84 Prozent abgenommen.

Wir konnten 2018 außerdem auch feststellen, dass die Zahl der Erkennungen von Trojanern, RiskwareTools (unser Erkennungsname für Cryptomining), Backdoor-Programmen und Spyware beträchtlich zugenommen hat. Backdoor.Vools beispielsweise, das derzeit zu den wichtigsten Backdoor-Erkennungen gehört, hat 2018 Benutzer weltweit geplagt, während es im Vorjahr noch nicht existierte. Die Zunahme bei den Erkennungen von Backdoor-Programmen, Spyware und Trojanern lässt sich auf den derzeitigen Trend zurückführen, bei dem Schwachstellen wie beispielsweise EternalBlue ausgenutzt werden, um Schadsoftware einzuschleusen, damit diese in einem Netzwerk Fuß fasst.

Auf der anderen Seite ließ sich insgesamt eine leichte Zunahme bei den RiskwareTool-Erkennungen feststellen. Das ist auf die massive Flut von Cryptomining-Schadsoftware Anfang 2018 zurückzuführen, die gegen Mitte des Jahres jedoch nachließ.

**BitCoinMiner-Erkennungen bei Privatanwendern 2018**

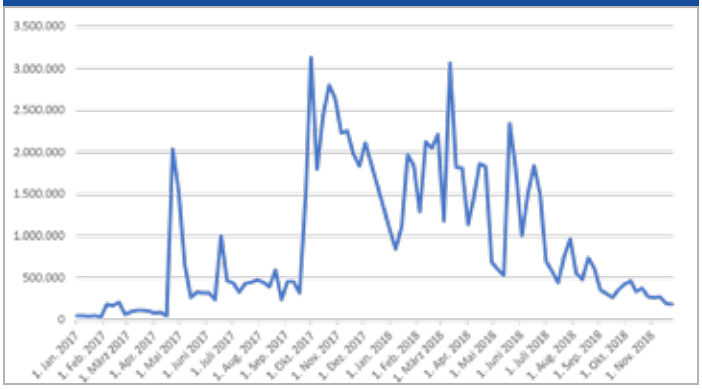


*Abbildung 2: RiskWare.BitCoinMiner-Erkennungen bei Privatanwendern im Jahr 2018*

Die Zahl der Erkennungen des bei Internetkriminellen so beliebten RiskWare.BitCoinMiner nahm im Verlauf des Jahres 2018 kontinuierlich ab. Im Juli lag die Zahl der Erkennungen in diesem Bereich ungefähr bei dem Niveau Anfang 2017. Ab Mitte September jedoch konnten wir hier bei den Erkennungen eine leichte Zunahme ausmachen.

**Cryptomining im Jahr 2017**

*Abbildung 3: Cryptomining-Zunahme im Herbst 2017*

Diese Zunahme ging dem Anstieg des Bitcoin-Wertes voraus, zu dem es rund einen Monat später, im Oktober 2017, kam. Möglicherweise hatten die Kriminellen, die hinter diesem Cryptomining steckten, Informationen, über die der Rest von uns nicht verfügte.

**Bitcoin Core (BTC) Preis Juni – Dez. 2018**

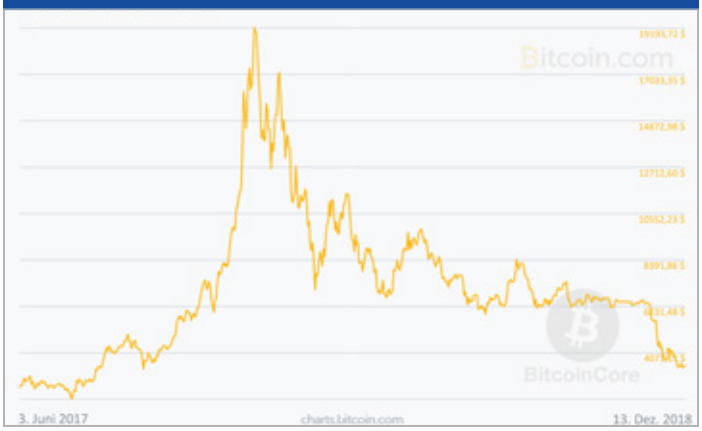


*Abbildung 4: Anstieg des Bitcoin-Wertes im Oktober 2017; Bildnachweis: Bitcoin 2018*

Zwischen Oktober 2017 und März 2018 kam es zu einer unglaublichen Flut von Minern für Kryptowährung. Während dieses Zeitraums erlebte auch die Schadsoftware, die vor allem auf Privatanwender abzielte, eine Belebung. Doch einige Monate später ließ das Kryptowährungsfieber nach, weshalb auch das Interesse der Internetkriminellen sank, Privatanwender anzugreifen.

Bei der Mehrzahl der Bedrohungen, die heute in Umlauf sind, kommen Taktiken und Methoden zum Einsatz, die wir in der Vergangenheit hauptsächlich von staatlich geförderter Schadsoftware kannten.

Das bedeutet, dass es bei größeren Zielen, d. h. Netzwerken mit zahlreichen Endpunkten, zu wesentlich umfangreicheren Störungen und Unterbrechungen kommt. Sollte es zu keinen neuen Entwicklungen bei der gegen Privatanwender gerichteten Schadsoftware kommen, die speziell Schwachstellen auf Endverbrauchersystemen ausnutzt, dann ist die Verlagerung des Fokus weg von Privatanwendern und hin zu Unternehmen weit mehr als nur ein vorübergehender Trend.

## Erkennungen bei Unternehmen

Angesichts der Tatsache, dass die Gesamtzahl der Erkennungen auf Privatanwendergeräten Jahr um Jahr um drei Prozent sinkt, könnte man davon ausgehen, dass auch die Produktion von Schadsoftware insgesamt zurückgeht. Dieser Trend zeigt jedoch nur, dass die Internetkriminellen ihren Schwerpunkt verlagert haben: weg von Otto Normalverbraucher und hin zu saftigeren Zielen, wie es z. B. Unternehmen sind. Das bestätigt auch der Anstieg um mehr als 100 Prozent bei vier unserer sieben wichtigsten Erkennungen im Unternehmsbereich von 2017 bis 2018.

**Erkennungen bei Unternehmen 2017/2018**

| Pos. | Bedrohung | Veränderung J/J in % |
|---|---|---|
| 1 | Trojaner | 132 % |
| 2 | Hijacker | 43 % |
| 3 | Riskware-Tool | 126 % |
| 4 | Backdoor | 173 % |
| 5 | Adware | 1 % |
| 6 | Spyware | 142 % |
| 7 | Ransomware | 9 % |
| 8 | Wurm | -9 % |
| 9 | Rogue | -52 % |
| 10 | HackTool | -45 % |
| **Erkennungen insgesamt** | | |
| 2017 | 39.970.812 | 79 % |
| 2018 | 71.823.114 | |

*Abbildung 5: Die 10 wichtigsten von Malwarebytes 2018 bei Unternehmen erkannten Bedrohungen*

Die Gesamtzahl der Schadsoftware-Erkennungen bei Unternehmen stieg im letzten Jahr beträchtlich – satte 79 Prozent, um genau zu sein. Das war primär auf die Zunahme von Backdoor-Programmen, Minern, Spyware und Information-Stealern zurückzuführen. Der Run auf die Kryptowährungen betraf nicht nur Privatanwender. Wir konnten feststellen, dass sich eine Vielzahl von bösartigen Cryptominern auch in Unternehmensnetzwerke eingeschlichen hatte.

Bei den Trojaner-Erkennungen spielte vor allem die Emotet-Familie eine herausragende Rolle, die sich lateral durch Unternehmensnetzwerke bewegen kann und dabei Exploits und Brute-Force-Angriffe nutzt, um Anmeldedaten abzuschöpfen. Diese Funktionalität wird auch in anderer auf Informationsdiebstahl ausgelegter Schadsoftware (z. B. TrickBot) genutzt, kommt aber ebenfalls bei Backdoor-Schadsoftware wie Vools zum Einsatz, wobei Vools 2018 zu den wichtigsten Erkennungen im Bereich der Backdoor-Infektionen gehörte. Vools nutzt die gleichen gerade erwähnten Exploits, um Endpunkte zu infizieren und sich darüber zu verbreiten.

Die Zahl der Ransomware-Erkennungen in der Unternehmenswelt hat im vergangenen Jahr nur leicht zugenommen, nämlich um neun Prozent, was vor allem auf noch bestehende, wenn auch inaktive Infektionen durch WannaCry zurückzuführen ist, die in unserem System markiert wurden. Obwohl wir bei Ransomware-Familien wie GandCrab und SamSam eine Weiterentwicklung beobachten konnten, kam es zu keinen so problematischen Ausbrüchen wie 2017.

Und schließlich ist die Zahl der Spyware-Erkennungen beträchtlich in die Höhe gegangen. Der Grund hierfür sind Varianten und Familien von Emotet und TrickBot, die in der Praxis als Spyware identifiziert werden. Sie sind ein deutliches Zeichen dafür, dass sich die Bedrohungsakteure jetzt vor allem auf den Diebstahl von Informationen verlegt haben und versuchen, sich in Unternehmensnetzwerken einzunisten.

## Regionale Bedrohungen

Nicht alle Schadsoftware-Angriffe konzentrieren sich auf einen bestimmten Teil der Welt. Viele Schadsoftware-Familien verbreiten sich – unabhängig von ihrem Ursprungsort – letztendlich in zahlreichen Ländern, weil die Angriffe opportunistisch sind und das Internet keine Grenzen hat (ausgenommen in China und Nordkorea). Es gibt jedoch auch Kampagnen, bei denen die Schadsoftware gezielt in bestimmte Länder und Regionen eingeschleust wird, in der Hoffnung, dass diese Länder oder Regionen aufgrund ihrer Kultur, ihrer Wirtschaft oder ihres politischen Klimas leichtere Opfer sind.

Auch wenn Internetkriminalität ein internationales Problem ist und wir Trends und Ereignisse gerne auf globaler Ebene analysieren, ist es wichtig, sich ausführlich damit zu beschäftigen, was in bestimmten Regionen passiert, um die Angriffsmuster zu verstehen und zu wissen, mit welchen Herausforderungen sich die Kunden in diesen Regionen konfrontiert sehen. Lesen Sie nun, was wir über die Regionen Nordamerika, asiatisch-pazifischer Raum (APAC), Europa, Naher Osten, Afrika (EMEA) und Lateinamerika (LATAM) herausgefunden haben.

### Nordamerika

**Top-Erkennungen in Nordamerika 2017/2018**

| Unternehmen | | Pos. | Privatanwender | |
|---|---|---|---|---|
| J/J | Bedrohung | | Bedrohung | J/J |
| 99 % | Trojaner | 1 | Adware | -19 % |
| 33 % | Hijacker | 2 | Trojaner | 7 % |
| 121 % | RiskwareTool | 3 | RiskwareTool | 38 % |
| 29 % | Adware | 4 | Backdoor | 10 % |
| 82 % | Spyware | 5 | Hijacker | -41 % |
| 11 % | Backdoor | 6 | Spyware | 18 % |
| -27 % | Wurm | 7 | HackTool | -40 % |
| -15 % | Ransomware | 8 | Rogue | -35 % |
| -55 % | Rogue | 9 | Rootkit | -50 % |
| -64 % | Rootkit | 10 | Virus | -57 % |

*Abbildung 6: Die wichtigsten Erkennungen bei Unternehmen und Privatanwendern in Nordamerika*

Nordamerika hatte vor allem eine Flut von unternehmensorientierten Information-Stealern und Minern für Kyptowährung zu bewältigen, wobei Unternehmen in einem weit höheren Maße infiziert wurden als es je zuvor der Fall war. Auf Privatanwenderseite konnten wir bei den wichtigsten erkannten Schadsoftware-Kategorien mehrheitlich einen Rückgang beobachten. Eine Ausnahme stellten lediglich Miner für Kryptowährung dar.

### Asiatisch-pazifischer Raum (APAC)

**Die wichtigsten Erkennungen 2017/2018 in der APAC-Region**

| Unternehmen | | Pos. | Privatanwender | |
|---|---|---|---|---|
| J/J | Bedrohung | | Bedrohung | J/J |
| 5137 % | Backdoor | 1 | Trojaner | 88 % |
| 261 % | Trojaner | 2 | Backdoor | 591 % |
| -48 % | Adware | 3 | Adware | -36 % |
| 170 % | RiskwareTool | 4 | RiskwareTool | -18 % |
| 148 % | Ransomware | 5 | Ransomware | 79 % |
| 305 % | Wurm | 6 | Wurm | -26 % |
| 50 % | Hijacker | 7 | HackTool | -25 % |
| 3690 % | Exploit | 8 | Exploit | 740 % |
| -7 % | HackTool | 9 | Spyware | 16 % |
| 9 % | Spyware | 10 | Hijacker | -48 % |

*Abbildung 7: Die wichtigsten Erkennungen bei Privatanwendern und Unternehmen in der APAC-Region*

Der asiatisch-pazifische Raum erlebte einen massiven Anstieg von Backdoor-Schadsoftware und eine umfassende Nutzung von Exploits für den Angriff von Endpunkten. Wenn man bedenkt, dass 2018 Vools – eine Schadsoftware-Familie, die Exploits zur Verbreitung nutzt – die primäre Backdoor-Bedrohung war, ist eine Zunahme dieser beiden Bedrohungsarten logisch. Allerdings ist noch immer nicht klar, weshalb die Angriffe wesentlich stärker auf die APAC-Region als auf andere Regionen abzielten.

Auf Privatanwenderseite konnten wir den gleichen Anstieg bei den Backdoor- und Exploit-Erkennungen feststellen, wobei es zu Jahresanfang zu einer Abnahme der meisten anderen Arten von Schadsoftware kam.

### EMEA-Raum (Europa, Naher Osten und Afrika)

| Die wichtigsten Erkennungen 2017/2018 in der EMEA-Region | | | | |
|---|---|---|---|---|
| Unternehmen | | Pos. | Privatanwender | |
| J/J | Bedrohung | | Bedrohung | J/J |
| 150 % | Trojaner | 1 | Adware | -40 % |
| 122 % | Hijacker | 2 | Trojaner | -15 % |
| -59 % | Adware | 3 | RiskwareTool | -23 % |
| 20 % | RiskwareTool | 4 | HackTool | -41 % |
| -6 % | Backdoor | 5 | Backdoor | -15 % |
| -41 % | HackTool | 6 | Wurm | -5 % |
| -1 % | Spyware | 7 | Spyware | 25 % |
| -14 % | Ransomware | 8 | Hijacker | -57% |
| -37 % | Wurm | 9 | Ransomware | -53 % |
| -56 % | Rogue | 10 | Rogue | -62 % |

*Abbildung 8: Die wichtigsten Erkennungen bei Privatanwendern & Unternehmen in der EMEA-Region*

Europa, der Nahe Osten und Afrika (EMEA) hatten vielfach mit den gleichen Problemen wie Nordamerika zu kämpfen. Die gegen Unternehmen in der EMEA-Region gerichteten Trojanerangriffe haben in dem Jahr um 150 Prozent zugenommen, was vor allem auf Emotet zurückzuführen war (genau wie in Nordamerika). Da sich die Internetkriminellen derzeit sehr stark auf bestimmte Schadsoftware-Familien konzentrieren, ist es bei nahezu allen anderen Arten von Bedrohungen zu einem Rückgang gekommen.

Obwohl es bei den Privatanwendern in der EMEA-Region zu einem bemerkenswerten Anstieg der Trojaner- und Hijacker-Erkennungen kam, ließ sich andererseits bei praktisch jeder Schadsoftware-Art ein beträchtlicher Rückgang feststellen – mit Ausnahme der Spyware. Das ist ein weiteres Zeichen dafür, dass sich der Fokus der Internetkriminellen von Privatanwendern auf Unternehmen verlagert.

### Lateinamerika (LATAM)

| Die wichtigsten Erkennungen 2017/2018 in Lateinamerika | | | | |
|---|---|---|---|---|
| Unternehmen | | Pos. | Privatanwender | |
| J/J | Bedrohung | | Bedrohung | J/J |
| 176 % | Trojaner | 1 | Adware | -55 % |
| 137 % | RiskwareTool | 2 | Trojaner | -1 % |
| -56 % | Adware | 3 | RiskwareTool | -25 % |
| 137 % | Ransomware | 4 | HackTool | -32 % |
| 23 % | Backdoor | 5 | Backdoor | -33 % |
| 343 % | Spyware | 6 | Wurm | -16 % |
| 101 % | Wurm | 7 | CrackTool | -35 % |
| -47 % | HackTool | 8 | Spyware | 43 % |
| -60 % | Hijacker | 9 | Ransomware | 59 % |
| 473 % | Rootkit | 10 | FraudTool | -97 % |

*Abbildung 9: Die wichtigsten Erkennungen in der LATAM-Region*

Lateinamerika hat ein spannendes Jahr erlebt, was die Entwicklung von Schadsoftware anbelangt. Die Kriminellen, die diese Region zum Ziel ihrer Angriffe machen, haben alles stehen und liegen lassen, um sämtliche Arten von Schadsoftware für Angriffe auf Unternehmen auszubauen und zu vermehren. Das reichte von Trojanern über Miner bis hin zu Spyware und sogar Rootkits. Organisationen, die von Lateinamerika aus arbeiten, sollten in Betracht ziehen, ihre Sicherheitsmaßnahmen schnellstens zu verstärken, da es im nächsten Jahr sogar zu einer noch stärkeren Zunahme kommen könnte.

Während die Verbreitung der Schadsoftware auf Unternehmensseite für Turbulenzen sorgte, sieht die Sache bei den Privatanwendern anders aus. Hier konnten wir lediglich bei den Erkennungen von Spyware und Ransomware einen Anstieg beobachten. Denken Sie jedoch daran, dass viele der Ransomware-Erkennungen in diesem Jahr darauf zurückzuführen waren, dass WannaCry sich so richtig ausgelebt hat, Systeme mit Schwachstellen identifizierte und infizierte, aber keine Dateien verschlüsselte. Stattdessen springen die Infektionen mehr oder weniger von System zu System, anscheinend ohne negative Konsequenzen zu haben. Aus diesem Grund lassen sich zahlreiche WannaCry-Infektionen in Bereichen erkennen, in denen die Installation von Patches zum Schutz vor dieser Bedrohung nicht prioritär war.

## Bedrohungen nach Ländern

| Die 10 Länder mit den meisten Erkennungen bei Privatanwendern | | |
|---|---|---|
| | **Land** | **Größte Bedrohung** |
| 1 | Vereinigte Staaten | Informationsdiebstahl |
| 2 | Brasilien | Klickbetrug |
| 3 | Vereinigtes Königreich | Adware |
| 4 | Vietnam | Backdoor-Programme |
| 5 | Indien | Backdoor-Programme |
| 6 | Indonesien | Backdoor-Programme |
| 7 | Frankreich | Adware |
| 8 | Italien | Cryptomining |
| 9 | Thailand | Backdoor-Programme |
| 10 | Russland | Backdoor-Programme |

*Abbildung 10: Die zehn Länder mit den meisten Erkennungen bei Privatanwendern und ihre größten Bedrohungen*

Die USA waren das Land mit den meisten Schadsoftware-Erkennungen bei Privatanwendern, wobei Emotet in dem Jahr das größte Problem war. Das sollte keine große Überraschung sein, da sich die Mehrzahl der Schadsoftware aufgrund der starken Volkswirtschaften vor allem gegen westliche Länder und insbesondere gegen die USA richtet.

Brasilien hat 2018 mit Klickbetrug-Schadsoftware auch seinen Teil abbekommen; übrigens ein ähnliches Problem wie im Vorjahr. Das Vereinigte Königreich und Frankreich waren eher das Ziel von Adware als von anderen Schadsoftware-Kategorien. Denken Sie jedoch daran, dass die Fähigkeiten von Adware nicht länger in Frage gestellt werden sollten. Adware kann Systemeinstellungen verändern und die Sicherheitssoftware deaktivieren, um Schadsoftware zu installieren.

Die größte Bedrohung für Privatanwender, die in vielen dieser Länder besteht, fällt in die Kategorie „Backdoor". Hierbei handelt es sich um eine Art von Schadsoftware, die einen Weg in das System findet und dort dann eine Tür offen lässt, durch die zukünftige Angreifer immer wieder eindringen können. Vietnam, Indien, Indonesien, Thailand und Russland – praktisch alle APAC-Länder – hatten ernsthafte Probleme mit Backdoor-Programmen, was wahrscheinlich darauf zurückzuführen ist, dass hier noch immer ein höherer Bedarf besteht, Endpunkte zu patchen und zu sichern.

| Die 10 Länder mit den meisten Erkennungen bei Unternehmen | | |
|---|---|---|
| | **Land** | **Größte Bedrohung** |
| 1 | Vereinigte Staaten | Informationsdiebstahl |
| 2 | Indonesien | Backdoor-Programme |
| 3 | Vereinigtes Königreich | Informationsdiebstahl |
| 4 | Frankreich | Informationsdiebstahl |
| 5 | Malaysia | Backdoor-Programme |
| 6 | Thailand | Backdoor-Programme |
| 7 | Australien | Cryptomining |
| 8 | Deutschland | Informationsdiebstahl |
| 9 | Brasilien | Adware |
| 10 | Philippinen | Informationsdiebstahl |

*Abbildung 11: Die zehn Länder mit den meisten Erkennungen bei Unternehmen und ihre größten Bedrohungen*

Unsere Liste der 10 Länder mit den meisten Erkennungen bei Unternehmen zeigt, dass in einem großen Teil der Welt ein bedeutendes Problem durch so genannte Information-Stealer besteht, d. h. Schadsoftware, die auf Informationsdiebstahl ausgelegt ist. Diese Schadsoftware-Kategorie infiziert einen Endpunkt, hinterlässt zusätzliche Schadsoftware und bewegt sich dann lateral durch das Netzwerk, wobei sie jeden angeschlossenen Computer infiziert, den sie erreichen kann. Danach kann diese Schadsoftware Anmeldedaten stehlen, weitere Bedrohungen installieren und sich selbst per E-Mail weiterverbreiten.

Obwohl auch viele andere Länder betroffen waren, scheinen doch vor allem westliche Länder wie die USA, das Vereinigte Königreich, Frankreich und Deutschland die Hauptleidtragenden dieser auf Informationsdiebstahl ausgelegten Angriffe zu sein. Währenddessen mussten sich im Osten Länder wie Indonesien, Malaysia und Thailand in ihren Unternehmensnetzen gegen eine wahre Flut von Backdoor-Schadsoftware wehren.

Länder wie Australien und Brasilien, in denen Adware und Cryptomining 2018 die Hauptbedrohungen darstellten, haben ausreichend Grund, um besorgt zu sein, da viele Miner und Adware-Familien zusätzliche Schadsoftware installieren, die Systemeinstellungen verändern, die Rechenleistung verlangsamen oder aufbrauchen oder den Betrieb anderweitig lahmlegen.

## Bedrohungen nach vertikalen Branchen

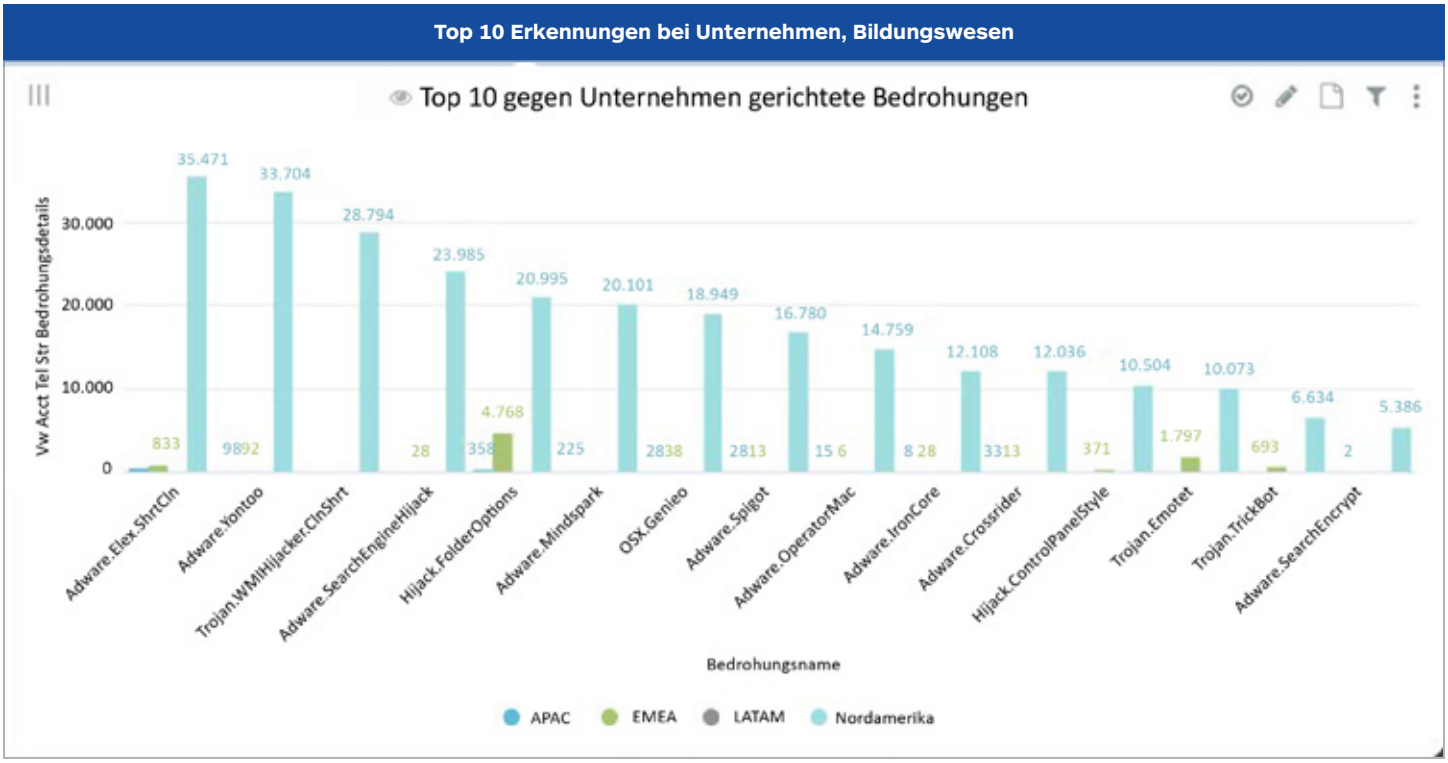


*Abbildung 12: Top 10 Erkennungen bei Unternehmen aus dem Bildungswesen 2018*

Bildungswesen, Fertigung und Einzelhandel waren die Branchen, die am stärksten unter der Top-Schadsoftware des Jahres zu leiden hatten: den Trojanern. Betrachtet man die Kategorie der Trojaner jedoch genauer und hier insbesondere die Emotet-Familie, tauschen die Branchen ihre Plätze. Consulting-Unternehmen schießen an die Spitze der Liste, während das Hotel- und Gaststättengewerbe den vierten Platz einnimmt.

Hinzu kam Ransomware, die einige wenige andere Branchen zum Ziel hatte. Erneut waren die Consulting-Unternehmen das Top-Ziel für die Autoren der Schadsoftware, während das Bildungswesen einen starken zweiten Platz belegte. Fertigung, Einzelhandel und Behörden vervollständigten die Liste der fünf wichtigsten Branchen.

Doch was passiert, wenn wir die Tabellen beiseite lassen und unser Telemetriesystem für Unternehmensprodukte heranziehen, um einen Blick auf die einzelnen Branchen zu werfen? Betrachtet man beispielsweise das Bildungswesen, so stellt man fest, dass es in praktisch allen Bedrohungskategorien auftaucht und 2018 am härtesten durch Adware betroffen war.

Beachtenswert ist, dass die beiden Schadsoftware-Familien für Mac, die als OSX.Genieo und Adware.OperatorMac erkannt werden, es auch auf die Liste geschafft haben. Das zeigt, dass Mac-Geräte sowohl im Bildungswesen als auch als vertikale Ziele ausgesprochen beliebt sind.

Dagegen sah sich die Consulting-Branche, die sowohl bei der Ransomware als auch bei der Trojaner-Familie Emotet an oberster Stelle stand, in dieser Kategorie noch mit verschiedenen weiteren Trojanern konfrontiert, darunter Banker, Downloader und Packer. Zudem haben Backdoor-Programme, Hijacker und Würmer die Consulting-Unternehmen 2018 aufs Korn genommen.

**Top 10 Erkennungen bei Unternehmen, Gesundheitswesen**

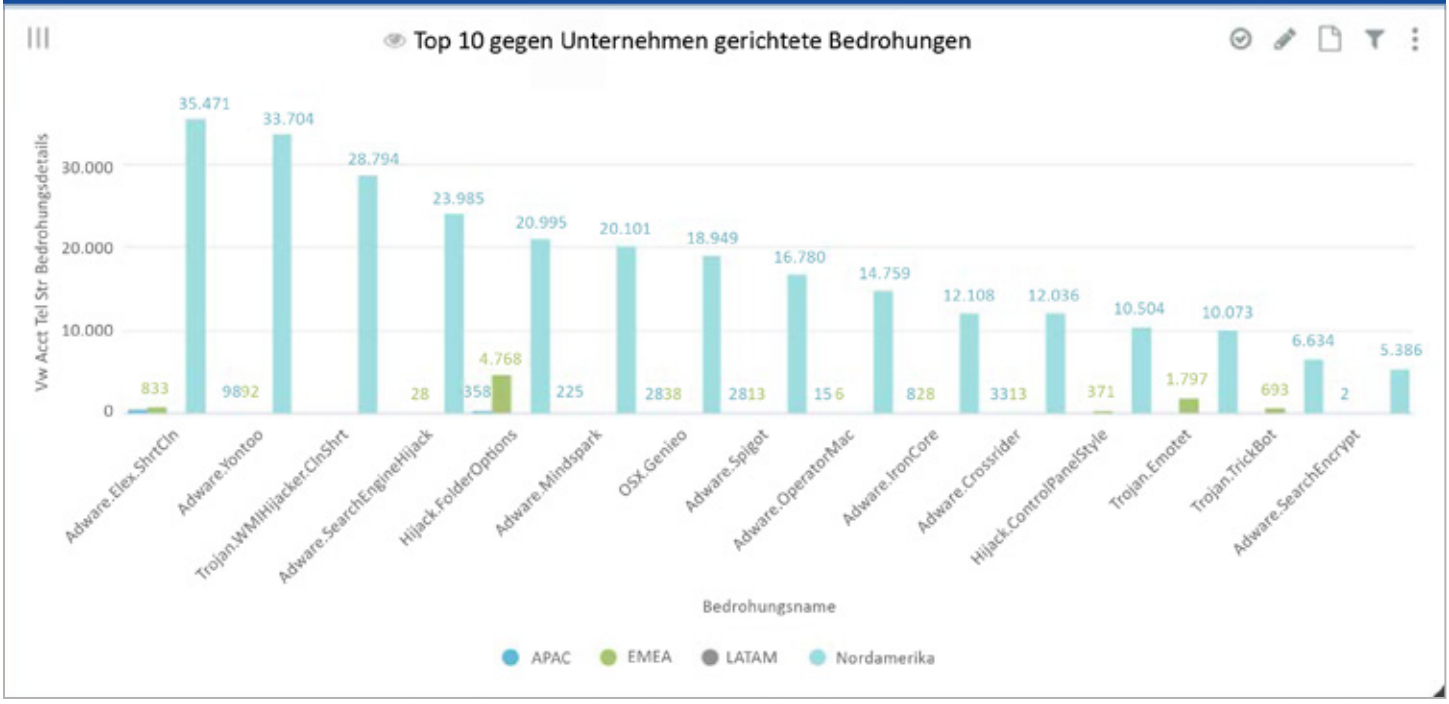


*Abbildung 13: Top 10 gegen das Gesundheitswesen gerichtete Bedrohungen*

Doch trotz der zahlreichen aufsehenerregenden Geschichten über Angriffe auf den Gesundheitssektor und Behörden, die wir 2018 zu hören bekommen haben, sind diese Branchen als vertikale Ziele eher im Hintergrund geblieben und haben es zum Teil nicht einmal unter die 10 Top-Branchen geschafft, die im vergangenen Jahr den am weitesten verbreiteten Bedrohungen ausgesetzt waren. Betrachtet man jedoch das Gesundheitswesen genauer, dann wird sofort klar, für welche Art von Schadsoftware diese Branche besonders attraktiv war: Emotet und TrickBot, eine Neuauflage von Bonnie und Clyde. Die Bedrohungen, die sich gegen das Gesundheitswesen richteten, wurden noch um Hijacker, Rootkits und Riskware ergänzt.

Behörden und Regierungen sahen sich ähnlichen Bedrohungen gegenüber wie das Gesundheitswesen, obwohl Emotet hier von den Hijackern überflügelt wurde und auf den zweiten Platz rutschte. Außerdem schafften es weitere Adware-Varianten auf die Liste, während TrickBot nicht zur Party bei den Behörden eingeladen war.

# Nennenswerte Schadsoftware

Zwar waren Kategorien wie Adware und Backdoor-Programme deutlich präsent, aber die echten Sterne am Himmel waren in diesem Jahr die Trojaner (Information-Stealer) und Cryptominer. Ransomware kam dagegen auf leisen Sohlen daher und nahm klammheimlich im Hintergrund bedeutende Änderungen vor. Lassen Sie uns nun einen genaueren Blick auf diese Bedrohungen werfen und wie sie sich 2018 auf Privatanwender und Unternehmen ausgewirkt haben.

## Cryptominer

Unsere wichtigste Prognose für 2018 lautete, dass der Cryptomining-„Goldrausch" für Internetkriminelle in dem Jahr oberste Priorität haben würde. Tatsächlich konnten wir im Zuge der Bewertung von Kryptowährungen eine Reihe von Bedrohungsakteuren beobachten, die Coin-Miner sowohl in der klassischen Form als binäre Schadsoftware als auch über Drive-by Mining verbreiteten.

### Mining auf infizierten Geräten

Die Onlinekriminellen schleusten über Exploit-Kits, wie u. a. RIG, eine Vielzahl von Cryptominern ein und luden dabei oftmals sogar mehrere Miner auf das Gerät desselben Opfers. Im Gegensatz zu anderen Bedrohungen (wie z. B. Ransomware) möchte diese Art von Schadsoftware unerkannt bleiben. Doch eine hohe CPU-Auslastung, ein immer langsamer werdender Rechner und das unaufhörliche Summen des Lüfters sind in der Regel die ersten Anzeichen dafür, dass etwas nicht stimmt.

### Drive-by-Mining: keine Infektion erforderlich

Im Bereich der Browser wurde Drive-by-Mining sehr schnell zu der am häufigsten erkannten Web-Bedrohung, die die Exploit-Kits vollkommen in den Schatten stellte. Aufgrund der Schwachstellen in Content-Management-Systemen – hier sind insbesondere die berüchtigten Drupalgeddon-Kampagnen zu nennen – waren die Internetkriminellen im 1. und 2. Quartal damit beschäftigt, Cryptojacking-Skripte in Websites einzuschleusen.

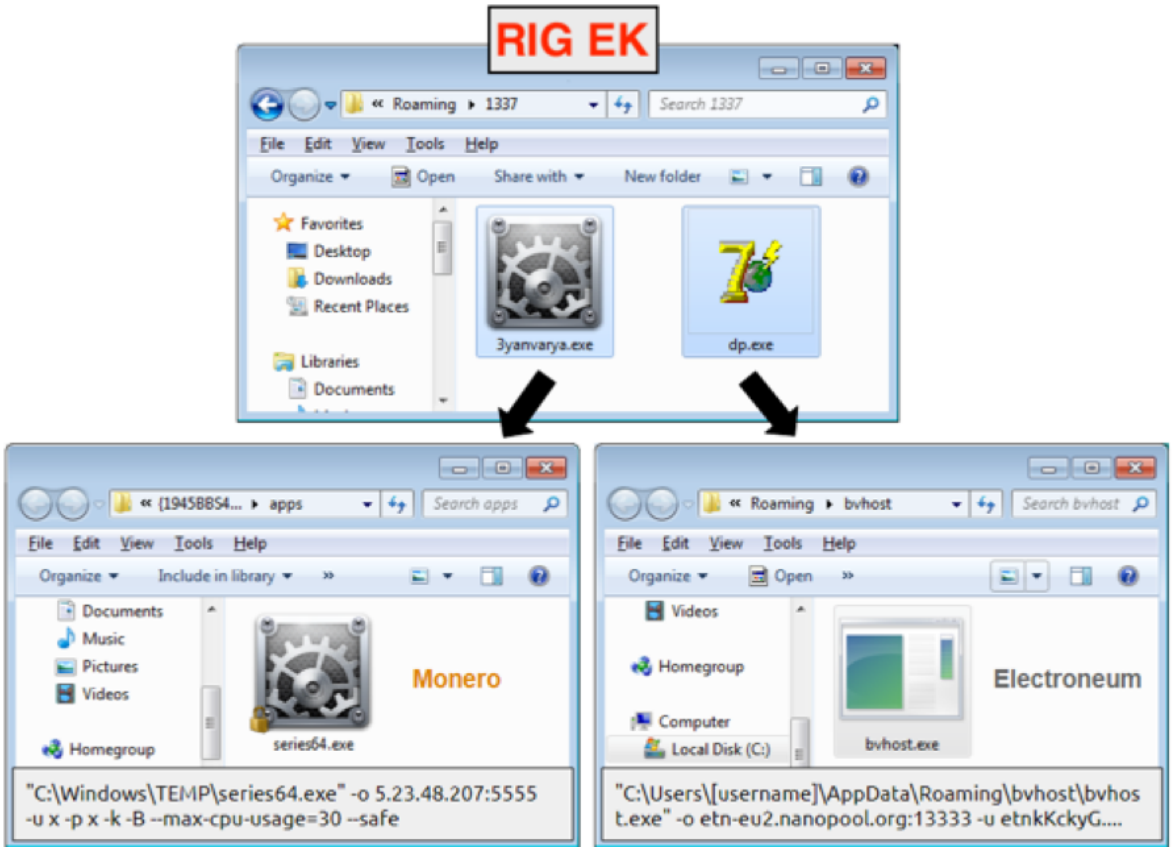


*Abbildung 14: RIG EK hinterlässt die Miner Monero und Electroneum*

| # | Server IP | Protocol | Host | URL | Body | Comments |
|---|---|---|---|---|---|---|
| 882 | 223.165.64.100 | HTTP | www.nzsap.org | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 883 | 13.228.219.59 | HTTPS | www.odysseypremier.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 884 | 118.143.50.216 | HTTPS | www.orbusneich.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 885 | 136.243.4.40 | HTTP | www.pixshock.net | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 886 | 52.64.6.39 | HTTP | www.progility.com.au | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 887 | 143.106.32.80 | HTTPS | www.prp.unicamp.br | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 888 | 35.200.201.129 | HTTPS | www.questin.co | /sites/default/files/advag... | 365,227 | Drupal Drive-by Mining HTML/JS |
| 889 | 80.241.209.95 | HTTPS | www.radiodogo.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 890 | 139.162.23.226 | HTTP | www.sankalpindia.net | /sites/default/files/js/js_0... | 23,757 | Drupal Drive-by Mining HTML/JS |
| 891 | 217.218.243.197 | HTTP | www.semnaniau.ac.ir | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 892 | 81.246.25.226 | HTTPS | www.sesvanderhave.com | /RU/misc/jquery.once.js?... | 3,670 | Drupal Drive-by Mining HTML/JS |
| 893 | 173.44.46.188 | HTTPS | www.sicrediuniaomsto.coop.br | /sites/default/files/js/js_-... | 96,973 | Drupal Drive-by Mining HTML/JS |
| 894 | 202.146.214.234 | HTTPS | www.silver-sewing-sisters.com.au | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 895 | 162.144.65.226 | HTTP | www.snellrealestate.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 896 | 91.194.60.51 | HTTP | www.spil.org | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 897 | 104.200.18.26 | HTTP | www.thebigwiki.com | /sites/default/files/js/js_... | 98,825 | Drupal Drive-by Mining HTML/JS |
| 898 | 205.186.132.167 | HTTPS | www.thenationalpastimemuseum.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 899 | 104.199.98.224 | HTTPS | www.thense.co.uk | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 900 | 151.80.115.77 | HTTPS | www.tmtg.org.uk | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 901 | 184.168.231.182 | HTTPS | www.umbiesoft.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 902 | 83.169.6.193 | HTTP | www.welayetnews.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 903 | 76.72.163.154 | HTTPS | www.wood-mode.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 904 | 23.196.199.47 | HTTPS | www.wowengage.com.au | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 905 | 34.232.250.21 | HTTPS | www.xplor.ai | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 906 | 46.243.119.189 | HTTP | www10.pmu.ro | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 907 | 216.187.97.215 | HTTP | www3.zipangcasino.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 908 | 41.87.228.50 | HTTP | zainbspectramedwhl01.spectramed.co.za | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |

*Abbildung 15: Tausende von Drupal-Websites mit Cryptomining-Skripten infiziert*

### Keine Plattform ist vor dem Mining sicher

Auch andere Plattformen wie Android oder macOS waren gegen Cryptomining nicht gefeit. Im Februar haben wir in einem Blog über einen Cryptominer für Mac berichtet, von dem sich nach genauerem Hinsehen herausstellte, dass es bereits 23 Varianten davon gab. Nur wenige Monate später haben wir über einen anderen Miner berichtet, der eine bösartige Implementierung des XMRig-Programms nutzt.

Unsere neueste Entdeckung war OSX.DarthMiner, der zusammen mit dem EmPyre Backdoor-Programm installiert und über eine als harmlos getarnte Applikation eingeschleust wurde, wie es bei Schadsoftware für Mac-Systeme oft der Fall ist.

### Rückgang der Mining-Angriffe: Ist es vorbei?

Nach unserem Telemetriesystem bestätigen das 3. und 4. Quartal, dass sich bei den Cryptominern ein Abwärtstrend abzeichnet. Verschiedenen Studien zufolge scheint die Euphorie, zu der es durch die hohe Bewertung des Bitcoin kam, etwas abgeebbt und Mining (das gilt insbesondere für webbasierte Miner) enttäuschend weniger Gewinn als erwartet erzielt zu haben.

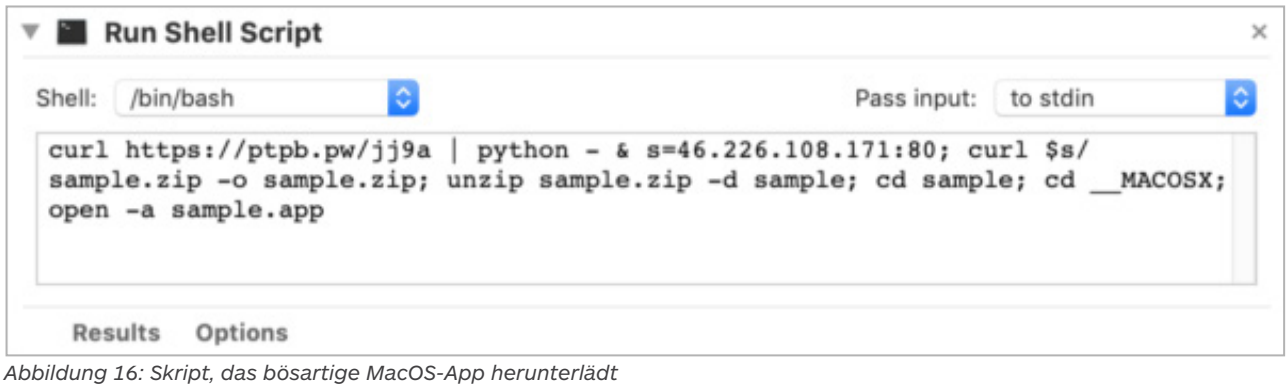


*Abbildung 16: Skript, das bösartige MacOS-App herunterlädt*

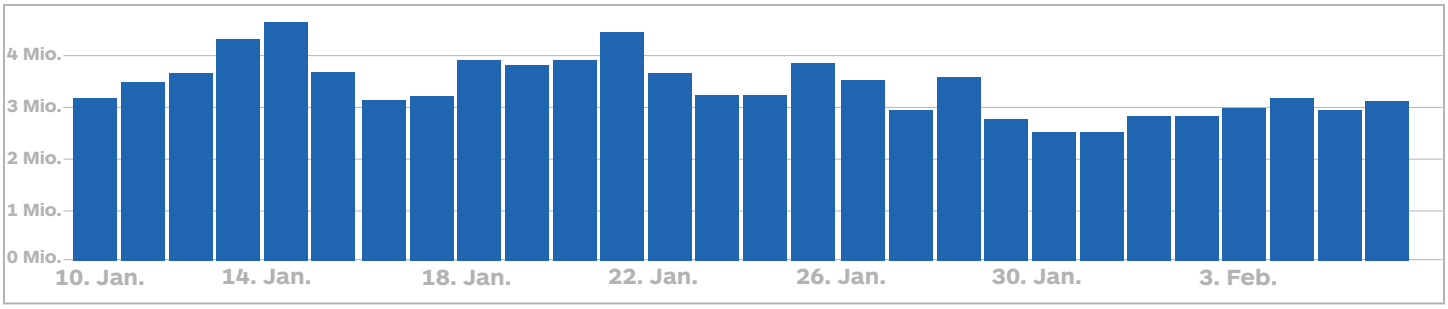


*Abbildung 17: Täglich durchschnittlich 3 Millionen Coinhive-Erkennungen von Januar bis Februar 2018*

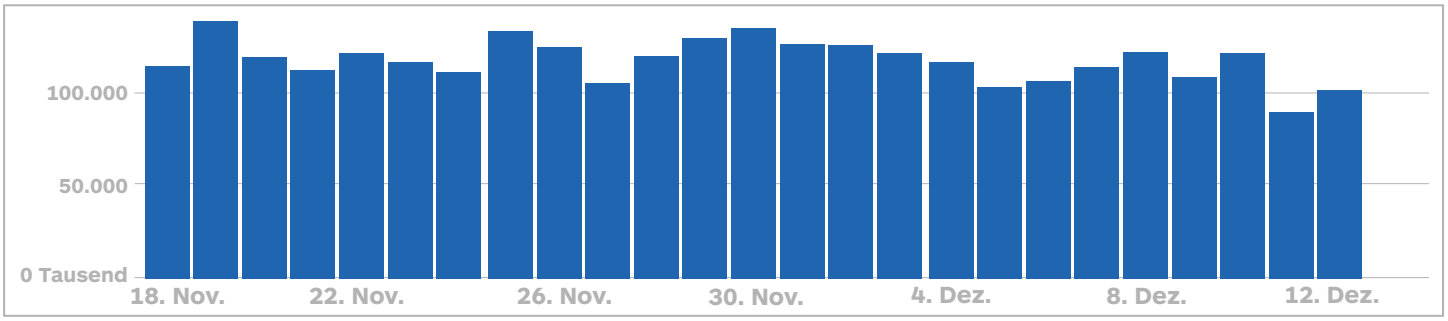


*Abbildung 18: Täglich durchschnittlich 100.000 Coinhive-Erkennungen von November bis Dezember 2018*

Doch trotz der nachlassenden Aktivität von Coinhive lassen andere Services, die sich auch auf Monero konzentrieren, Anzeichen erkennen, dass es mit dem browserbasierten Mining noch nicht gänzlich vorbei ist. So ist insbesondere CoinIMP in den letzten Monaten sehr populär geworden.

Insgesamt sieht es so aus, als seien die Internetkriminellen übereinstimmend zu dem Schluss gekommen, dass Stehlen manchmal besser ist als Mining. Tatsächlich wurde eine ganze Reihe von Schadsoftware-Familien, wie beispielsweise TrickBot, um die Funktionalität erweitert, mit der direkt ganze Cryptowallets geleert werden können. Ebenso besteht bei den Angreifern ein großes Interesse daran, die Schwachstellen in der JSON-RPC-Protokollimplementierung vieler Kryptowährungen auszunutzen.

In diesen Fällen konnte oftmals schon das simple Browsen auf einer bösartigen Website dazu führen, dass Ihre digitale Brieftasche geleert wurde.

Doch trotz ihres gesunkenen Wertes bleiben Kryptowährungen auch weiterhin für Onlinekriminelle attraktiv. Daher ließen sich auch 2018 große Kampagnen beobachten, bei denen Miner mit beträchtlichem Erfolg über zahlreiche Plattformen verbreitet wurden. Aber möglicherweise beschränkte sich die Blütezeit des Cryptojacking auf den Zeitraum zwischen Herbst 2017 und den ersten Monaten des Jahres 2018 – insbesondere was das browsergestützte Modell anbelangt. Tatsächlich gibt es andere Arten von Payloads, die bei Weitem lukrativer sind, wie wir bei der jüngsten Welle von digitalen Skimming-Angriffen sehen konnten.

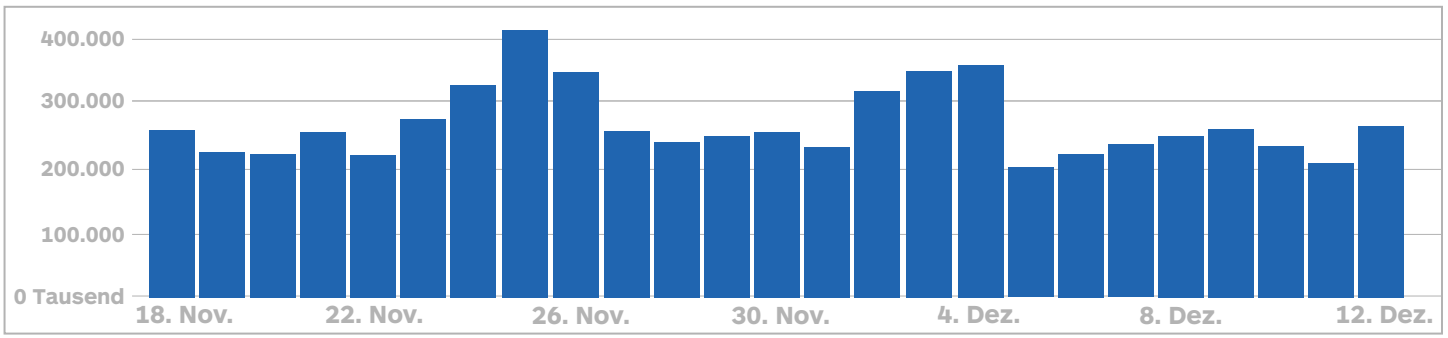


*Abbildung 19: CoinIMP-Erkennungen November bis Dezember 2018*

## Trojaner

Der Begriff „Trojaner“ ist sehr weit gefasst und bezeichnet eine große Bandbreite von Schadsoftware mit unterschiedlichen Zielen und Verhaltensweisen. Während der Begriff „Trojaner“ normalerweise mit der Legende um das Trojanische Pferd verbunden wird, bedeutet er für all jene, die im Bereich der Cybersicherheit tätig sind, dass eine Schadsoftware in der Lage ist, sich als harmloses Programm zu tarnen, um sich unerkannt in ein System einzuschleichen, d. h. dass sich ein Code in einem anderen Code verbergen kann, um die vorhandenen Sicherheitsmaßnahmen zu umgehen.

Als der Begriff „Trojaner“ zum ersten Mal verwendet wurde, um eine bestimmte Art von Schadsoftware zu beschreiben, gab es noch nicht viele andere Bedrohungen, die die gleiche Taktik nutzten, um Systeme zu infizieren. Heute jedoch umfasst praktisch jede Schadsoftware irgendeine Art von „Trojaner“-Funktionalität, denn im modernen Cyberkrieg besteht einer der Grundpfeiler der Angreifersoftware darin, sich vor der Sicherheitssoftware zu verbergen. Abgesehen davon ist der Begriff „Trojaner“ sehr nützlich, wenn man von Schadsoftware-Familien spricht, die sich nicht eindeutig den Kategorien Spyware, Adware oder Backdoor-Programm zuordnen lassen, sondern von jeder Kategorie ein paar Merkmale aufweisen.

So begann die Emotet-Familie beispielsweise als gewöhnlicher Banking-Trojaner. Nach erfolgter Infektion versuchte sie festzustellen, ob die Benutzer bei ihren Bankkonten angemeldet waren oder Finanzdaten auf einer Website eingaben, stahl dann diese Daten und schickte sie zurück an den Command-and-Control-(C&C-)Server.

Im Laufe der Zeit hat sich Emotet auf eine interessante Art weiterentwickelt: Die Schadsoftware ist nun in der Lage, Exploits zu nutzen, um Systeme zu infizieren, weitere Schadsoftware zu verbreiten und sogar E-Mails an die in der Kontaktliste enthaltenen Adressen zu versenden. Betrachtet man jede dieser Funktionen individuell, müsste man Emotet in mehrere Schadsoftware-Kategorien einreihen, z. B. Würmer, Spyware, Backdoor-Programme und Downloader. Alle zusammen ergeben einen Trojaner.

In diesem Abschnitt werden wir uns damit beschäftigen, in welchem Umfang – im Vergleich zum Vorjahr – Trojaner in diesem Jahr ein globales Problem waren und welche Trends bei den größten Trojaner-Familien bestehen, deren Entwicklung wir verfolgen.

### Gegen Unternehmen gerichtete Trojaner

Trojaner waren 2017 weniger auf Unternehmensendpunkten zu beobachten. Die Flut an Informationsdiebstahl-Trojanern wurde vor allem 2018 zum Problem. Abbildung 20 zeigt die geringe Zahl der Trojaner-Erkennungen vom 1. bis 3. Quartal 2017. Erst im September kam es zu einem sprunghaften Anstieg, der gleichzeitig den Anstoß für eine neue Art von Trojanern gab, die von unseren Unternehmenskunden erkannt wurden.

**Weltweite Trojaner-Erkennungen bei Unternehmen 2017 - 2018**

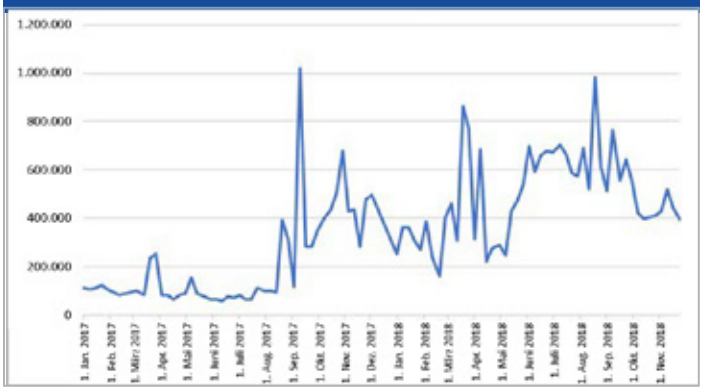


*Abbildung 20: Weltweite Erkennung von gegen Unternehmen gerichteten Trojanern*

Auf Informationsdiebstahl ausgelegte Schadsoftware machte den größten Teil der 2018 erkannten Trojaner aus. Zu den zahlreichen möglichen Gründen hierfür gehören u. a. die Auswirkungen von neuen Richtlinien, wie z. B. die Datenschutz-Grundverordnung (DSGVO) oder die Nutzung von Exploits wie EternalBlue und Backdoor-Programmen wie DoublePulsar.

Der Trend, dass auf den Informationsdiebstahl ausgelegte Trojaner gegen Unternehmen eingesetzt werden, scheint nicht nachzulassen. Allerdings können die Implementierung von Patches, die Netzwerk- und Datensegmentierung sowie die Konfiguration von Benutzerrechten dazu beitragen, dass sich die Flut von Trojanern nicht so leicht verbreitet.

### Gegen Privatanwender gerichtete Trojaner

Während Unternehmen in diesem Jahr stark von Trojanern geplagt waren, blieb ihre Zahl auf Privatanwenderseite relativ stabil. Hier kam es zwischen 2017 und 2018 nur zu geringen Veränderungen.

**Weltweite Trojaner-Erkennungen bei Privatanwendern 2017 - 2018**

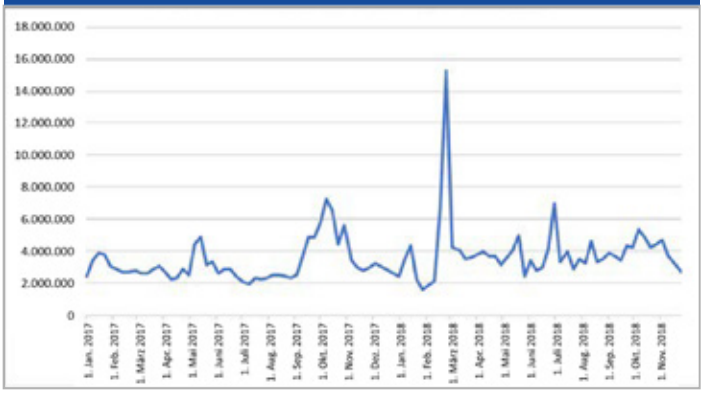


*Abbildung 21: Weltweite Erkennung von gegen Privatanwender gerichteten Trojanern*

Insgesamt kam es 2018 zu rund 30 Millionen mehr Erkennungen von Trojanern als 2017. So wurden 2017 etwa 160 Millionen Trojaner registriert, während sich die Zahl 2018 auf 190 Millionen belief. Soweit wir feststellen konnten, handelte es sich bei der Mehrzahl entweder um Information-Stealer, bösartige Miner oder generische Erkennungen.

Wir erwarten nicht, dass es 2019 zu einer bedeutenden Veränderung bei diesem Trend kommt. Allerdings wird unsere vierteljährliche Analyse interessante Varianten der Trojaner-Familien aufdecken.

## Information-Stealer

Zwei der wichtigsten Trojaner-Bedrohungen 2018 waren Emotet und TrickBot. Hierbei handelte es sich um auf Informationsdiebstahl ausgelegte Schadsoftware, die ein System infiziert, sich dann selbst verbreitet und erneut alles infiziert, dessen sie habhaft werden kann. Wir haben uns mit beiden Familien ausführlich in unserem Blog und in anderen, 2018 veröffentlichten Berichten beschäftigt. Werfen wir nun einen Blick auf die Trends, die wir im vergangenen Jahr bei den Erkennungen insgesamt feststellen konnten.

### Emotet

Dieses auf Informationsdiebstahl ausgelegte Spam-Programm stellte 2018 eine große Bedrohung dar, da es sich hierbei um eine der Schadsoftware-Familien handelt, die sowohl auf Unternehmens- als auch Privatanwenderseite Infektionen im großen Stil verursacht.

**Weltweite Emotet-Erkennungen bei Unternehmen 2017 - 2018**

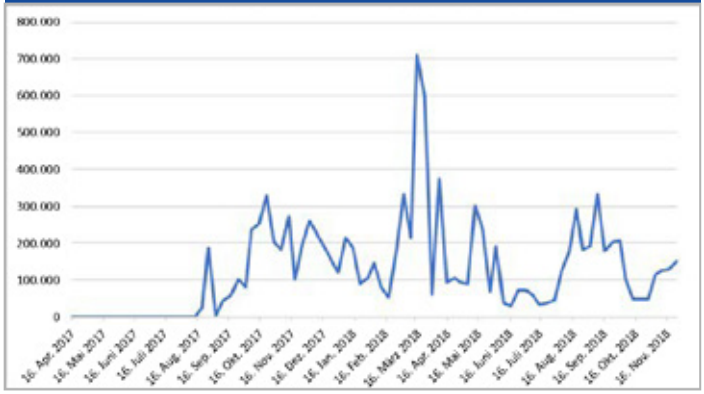


*Abbildung 22: Emotet-Erkennungen bei Unternehmen, April 2017 bis November 2018*

Die Emotet-Erkennungen bei Unternehmen ähneln den Erkennungen bei Privatanwendern; haben allerdings einen geringeren Umfang. Wie Sie in Abbildung 23 sehen, ist die Zahl der erkannten Emotet-Infektionen auf Privatanwender- und Unternehmensseite parallel angestiegen.

Betrachten Sie nun Form und Größe der Linie für die Erkennungen bei Unternehmen und Privatanwendern im 3. Quartal 2018; sie hat die Form eines Hundekopfes. Der Unterschied zwischen den beiden Linienformen beträgt 78.000 Erkennungen. Betrachtet man dagegen die beiden Linienformen zu Anfang des Beobachtungszeitraums, zeigt sich, dass die Zahl der Erkennungen auf Privatanwenderseite um rund 475.000 Erkennungen höher lag als auf Unternehmensseite.Weshalb sind diese

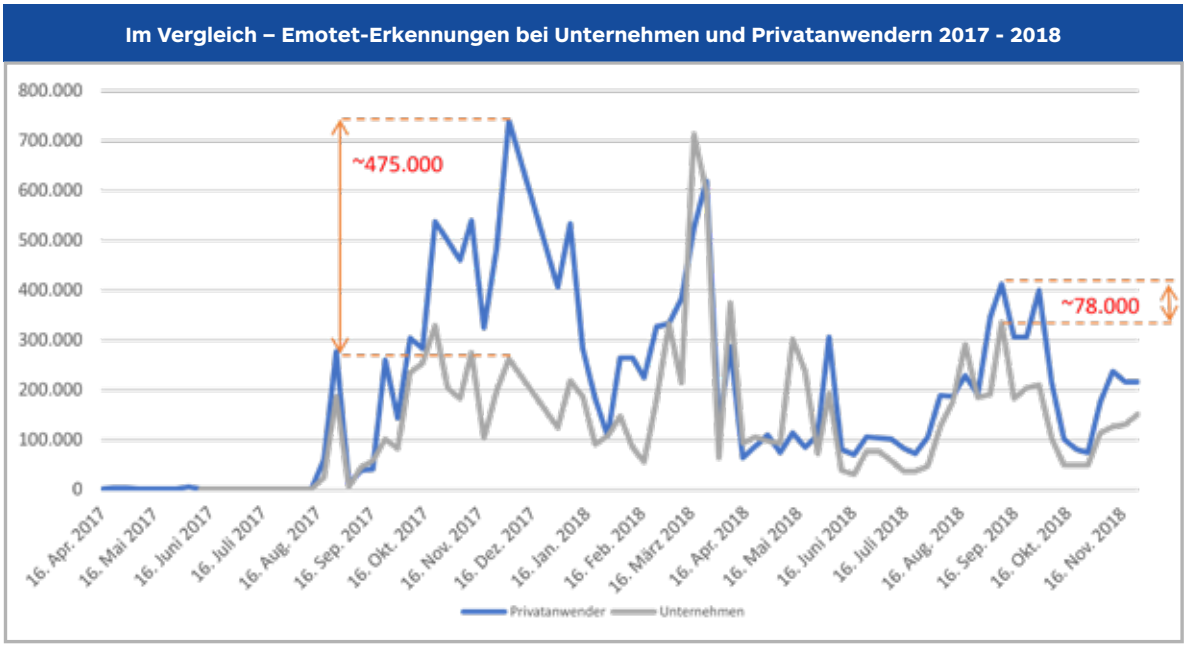


*Abbildung 23: Im Vergleich – Emotet-Erkennungen bei Unternehmen und Privatanwendern*

Zahlen so bedeutend? Nun, die ähnlich verlaufenden Linien mit ihren Erkennungsspitzen auf Unternehmens- und Privatanwenderseite während desselben Zeitraums zeigen uns, dass Emotet-Kampagnen großflächig angelegt sind, damit ihnen sowohl Privatanwender als auch Unternehmen ins Netz gehen. In der Vergangenheit gab es dabei wesentlich mehr Opfer unter den Privatanwendern. Jetzt dagegen schließt sich diese Lücke zwischen Privatanwendern und Unternehmen langsam.


*Abbildung 24: Emotet-Erkennungen bei Privatanwendern, April 2017 bis November 2018*

Die Angreifer hinter Emotet versuchen bewusst, ihre Schadsoftware jetzt auch bei Unternehmen zu verbreiten. Und angesichts der Tatsache, dass die Angreifer diese Schadsoftware-Familien ständig weiterentwickeln und um neue Funktionen bereichern, sodass sie sich lateral durch Unternehmensnetze bewegen und bösartige Spam-Mails von einem infizierten Endpunkt aus versenden können, wird sehr schnell klar, welche Motive diejenigen verfolgen, die Emotet steuern.

**TrickBot**

Wenn die zunehmende Zahl von Emotet-Angriffen gegen Unternehmen Sie noch nicht auf den Gedanken gebracht hat, dass Information-Stealer jetzt ein besseres Ziel gefunden haben, dann brauchen Sie nur einen Blick auf all jene Schadsoftware-Programme zu werfen, die nicht nur selbst Opfer anhäufen, sondern auch von Emotet als sekundärer Payload hinterlassen werden.

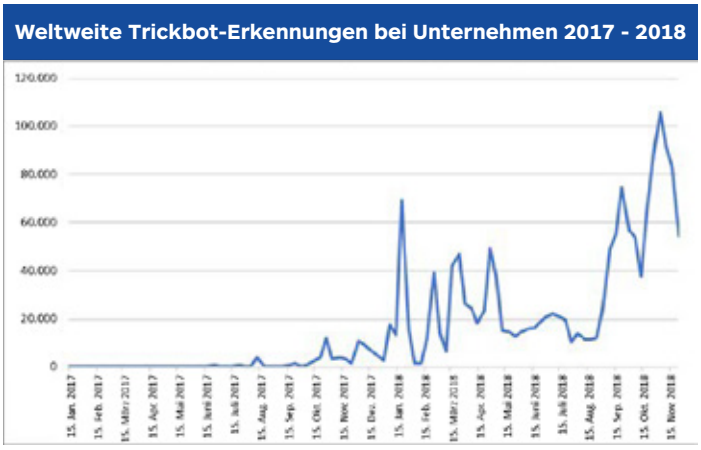


*Abbildung 25: Weltweite TrickBot-Erkennungen bei Unternehmen*

TrickBot ist ein übler Information-Stealer, der Komponenten für spezifische bösartige Vorgänge – wie z. B. Keylogging und Lateralbewegungen in einem Netzwerk – herunterladen kann. Wie Abbildung 25 zeigt, hat diese Schadsoftware-Familie erst gegen Ende 2017 angefangen, Wellen zu schlagen, und gehörte zu den üblichen Payloads, die von Emotet verbreitet wurden.

**Weltweite Trickbot-Erkennungen bei Privatanwendern 2017 - 2018**

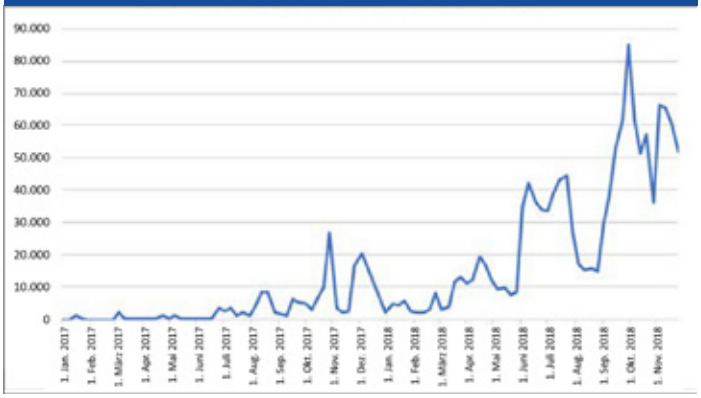


*Abbildung 26: Weltweite TrickBot-Erkennungen bei Privatanwendern*

Vergleicht man die Gesamtzahl der TrickBot-Erkennungen auf Endpunkten von Unternehmen und Privatanwendern, ergibt sich ein Unterschied von 200.000 Erkennungen, wobei die Unternehmen an der Spitze stehen. Auf den Endpunkten von Unternehmen wurden 1,5 Millionen Instanzen von TrickBot erkannt, während es bei den Privatanwendern rund 1,3 Millionen waren.

Die meiste Schadsoftware, mit der wir zu tun haben, wird eher bei Privatanwendern erkannt als auf den Endpunkten von Unternehmen. Als wir diese im Unternehmensbereich neu festgestellten Erkennungen analysierten, zeigte sich deutlich die Absicht der Internetkriminellen, Unternehmen zu ihren Zielen zu machen und ihre Schwachstellen auszunutzen.

### Trojaner nach vertikalen Branchen

Wie bereits in unserer Einführung zu Trojanern erwähnt, bezieht sich der Begriff auf eine Vielzahl von Schadsoftware-Arten, die entweder ihre Absicht verschleiern oder sich nicht so recht in eine bestimmte Kategorie einordnen lassen. Wenn wir das Ganze nun aus einem etwas allgemeineren Blickwinkel betrachten und einen Blick auf die Branchen werfen, an die sich Trojaner richten, ergibt sich ein Bild, das dem unserer weltweiten kombinierten Erkennungen ähnelt. Bildungswesen, Fertigung und Einzelhandel führen die Liste an, während sich Consulting-Unternehmen, Regierungsbehörden und das Gesundheitswesen im Mittelfeld bewegen. Die Nahrungsmittel- und Getränkeindustrie belegt den letzten Platz, während das Hotel- und Gaststättengewerbe, trotz der starken Medienaufmerksamkeit, die die Sicherheitsverletzung bei der Hotelkette Marriott hervorgerufen hat, es gar nicht erst auf die Liste schafft.

| Die 10 Top-Branchen, die von Trojanern betroffen waren | |
|---|---|
| 1 | Bildungseinrichtungen |
| 2 | Fertigung |
| 3 | Einzelhandel |
| 4 | Consulting |
| 5 | Regierungsbehörden |
| 6 | Telekommunikation |
| 7 | Gesundheitswesen |
| 8 | Technologie |
| 9 | Unternehmensdienstleistungen |
| 10 | Nahrungsmittel und Getränke |

*Abbildung 27: Die 10 Top-Branchen, die von Trojanern betroffen waren*

Betrachtet man die Kategorie der Trojaner allerdings genauer, und hier insbesondere die Trojaner-Familie Emotet, die zu den wichtigsten überhaupt gehört, dann tauschen die Branchen ihre Plätze. Consulting-Unternehmen schießen an die Spitze der Liste, während das Hotel- und Gaststättengewerbe den vierten Platz einnimmt. Zu dieser Liste der wichtigsten 10 Branchen gesellen sich zudem noch das Transportwesen und die Logistik sowie die Chemikalienbranche; sie verdrängen die Branchen Telekommunikation, Unternehmensdienstleistungen und die Nahrungsmittel- und Getränkeindustrie.

| Die 10 Top-Branchen, die durch den Trojaner Emotet angegriffen wurden | |
|---|---|
| 1 | Consulting |
| 2 | Bildungseinrichtungen |
| 3 | Fertigung |
| 4 | Hotel- und Gaststättengewerbe/Freizeit |
| 5 | Regierungsbehörden |
| 6 | Einzelhandel |
| 7 | Transportwesen und Logistik |
| 8 | Chemikalien |
| 9 | Gesundheitswesen |
| 10 | Technologie |

*Abbildung 28: Die 10 Top-Branchen, die von Emotet betroffen waren*

### Die Trojaner von morgen

Die derzeitigen Trends, die wir im Bereich der Trojaner ausmachen konnten, werden sich höchstwahrscheinlich fortsetzen, solange die Internetkriminellen eine Möglichkeit sehen, schwache Konfigurationen und veraltete Ressourcen auszunutzen. Den größten Anlass zur Sorge geben jedoch Nachahmer und neue Generationen von Schadsoftware-Familien, die 2019 wahrscheinlich vorherrschen werden.

Derzeit besteht keine große Konkurrenz für Emotet (abgesehen von TrickBot), da diese Schadsoftware entweder selbstständig Unternehmen als Ziel anvisiert oder als Infektionsvektor für eine andere Familie dient. Wenn allerdings die Trends, die sich von 2012 bis 2016 bei der Ransomware beobachten ließen, ein Indikator für das sind, was uns erwartet, dann werden wir in den nächsten 12 Monaten Konkurrenzprogramme wie Pilze aus dem Boden sprießen sehen.

## Ransomware

Ransomware ist zwar nicht mehr die weitreichende Bedrohung, die sie 2017 noch war, aber sie ist noch immer ein übles Ärgernis, mit dem man rechnen muss. Die Trends zeigen insgesamt für 2018 eine Abnahme der Ransomware-Angriffe, dagegen aber eine Zunahme von zielgerichteten, raffinierten Angriffen, die sich gegen Unternehmen richten. Tatsächlich haben die Ransomware-Erkennungen nur im beruflichen Umfeld einen Spitzenwert erreicht. Bei den Angriffen auf Privatanwender dagegen zeichnete sich ein deutlicher Mangel an Interesse und Innovationen ab.

Zwar ist es zu einer überraschenden Überarbeitung älterer Dateien gekommen, um damit neue Angriffe zu starten, und berühmte Varianten wie WannaCry haben vereinzelt Aufsehen erregt, doch im Großen und Ganzen lag Ransomware 2018 zum größten Teil im Dornröschenschlaf.

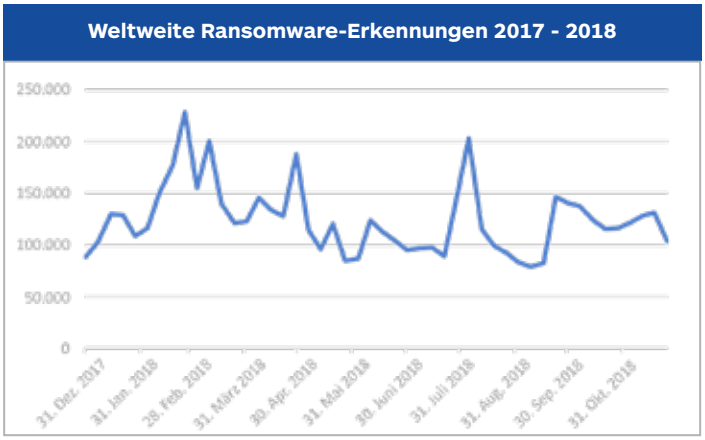


*Abbildung 29: Weltweite Ransomware-Erkennungen im Jahr 2018*

### Privatanwender vs. Unternehmen

Der allgemeine Rückgang in den Angriffen ist bedeutend: 2017 stellten wir weltweit 8.016.936 Angriffe fest, die sowohl Unternehmen als auch Privatanwender betrafen. Vergleicht man diese Zahl mit den 5.948.417 registrierten Erkennungen, zu denen es 2018 kam, dann ist das ein Rückgang von 26 Prozent.

Dabei wird offensichtlich, dass sich das Interesse der Angreifer von den Privatanwendern auf Unternehmen als bevorzugte Ziele verlagert hat, denn während die Zahl der Erkennungen auf der einen Seite kontinuierlich steigt, nimmt sie auf der anderen Seite ab.

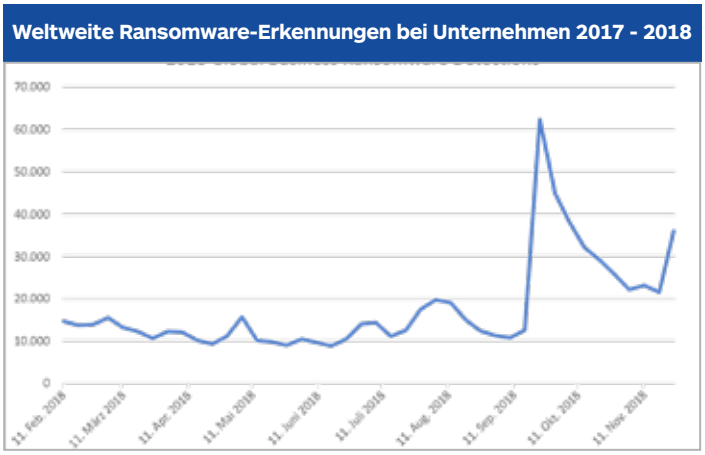


*Abbildung 30: Weltweite Ransomware-Erkennungen bei Unternehmen*

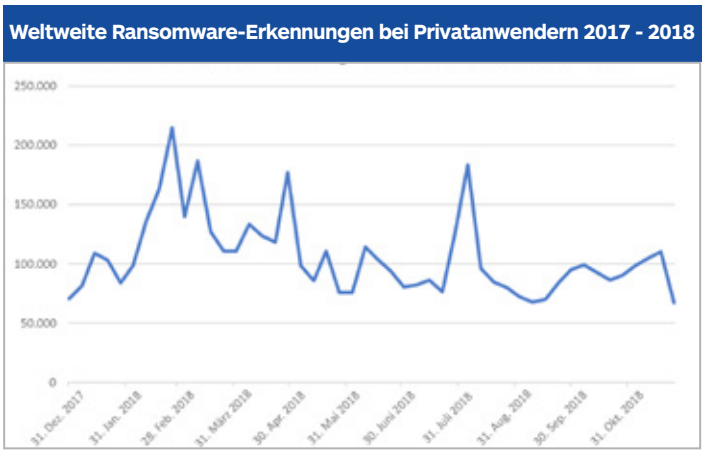


*Abbildung 31: Weltweite Ransomware-Erkennungen bei Privatanwendern*

Da Unternehmen mit einer Vielzahl von wertvollen Daten und kritischen Systemen arbeiten, haben sie sich für die Internetkriminellen als deutlich profitablere Ziele erwiesen. Sie verfügen nicht nur über die potenziellen Mittel, um ein Lösegeld zu zahlen, sondern haben in der Regel auch zahlreiche zwingende Gründe, um so schnell wie möglich ihre Arbeit wieder aufzunehmen. Verzögerungen durch Ransomware können unglaublich kostspielig sein – insbesondere dann, wenn die betroffene Organisation über keinen Plan zur Datensicherung verfügt und eine Vielzahl von Endpunkten bereinigen muss. Und schließlich kommen noch Incident Response und digitale Forensik zu den Kosten hinzu, sodass sich die Betroffenen letztendlich oftmals einer Summe gegenübersehen, die deutlich höher als das geforderte Lösegeld ist, weshalb die Zahlung des Lösegeldes einfacher und günstiger zu sein scheint (eine Vorgehensweise, die wir nicht empfehlen).

### Statistik zu vertikalen Branchen

Möglicherweise fragen Sie sich: Wie weit ist Ransomware in den verschiedenen Branchen verbreitet? Welche vertikalen Branchen sind am stärksten betroffen? Unsere Daten zeigen, dass Consulting-Unternehmen an der Spitze stehen, während sich das Bildungswesen auf den zweiten Platz drängt.

| Die 10 Top-Branchen, die von Ransomware betroffen waren | |
|---|---|
| 1 | Consulting |
| 2 | Bildungseinrichtungen |
| 3 | Fertigung |
| 4 | Einzelhandel |
| 5 | Regierungsbehörden |
| 6 | Transportwesen |
| 7 | Telekommunikation |
| 8 | Elektronik |
| 9 | Gesundheitswesen |
| 10 | Technologie |

*Abbildung 32: Die Top-Branchen, die von Ransomware betroffen waren*

Trotz der zahlreichen aufsehenerregenden Geschichten über Angriffe auf das Gesundheitswesen und Regierungsbehörden, die 2018 die Runde machten, hatten andere Branchen weitaus stärker mit der Ransomware-Bedrohung zu kämpfen. Tatsächlich liegen die Regierungsbehörden in der Statistik nur im Mittelfeld, während das Gesundheitswesen gerade mal den neunten Platz belegt.

### SamSam

SamSam verursachte in den medizinischen Netzwerken der USA ein Chaos, nutzte Schwachstellen und Brute Force, um sich seinen Weg in die Systeme zu bahnen und durch die Geiselnahme der Systeme mehr als 1 Million US-Dollar zu erbeuten. Eine seiner vielen älteren Varianten wurde aufpoliert, um für Internetkriminelle attraktiver zu sein. Diese Version forderte von den Opfern ein Lösegeld, das deutlich niedriger ausfiel als die Kosten für alle alternativen Wiederherstellungsverfahren. Folglich erbeuteten die Kriminellen so wesentlich mehr Geld.

Von Januar bis März brachte SamSam so ziemlich alles zur Strecke, von Krankenhäusern bis hin zu städtischen Diensten. Das schloss sogar Bereiche des Verkehrsministeriums und stadtinterne Anwendungen in Atlanta ein. Zu weiteren großen Angriffen kam es im September, als es im Hafen von San Diego und Barcelona jeweils zu einem Ausbruch kam.

**Weltweite SamSam-Erkennungen 2017 - 2018**

*Abbildung 33: Weltweite SamSam-Erkennungen im Jahr 2018*

Obwohl die Strafverfolgungsbehörden zu wissen glauben, wer hinter der Infektion steckt, ist das mutmaßliche Täterduo noch immer auf freiem Fuß und wir können weiterhin beobachten, wie die Linie bei den Erkennungen nach oben ausschlägt. SamSam wird auch bis weit in das Jahr 2019 eine wesentliche Quelle für Infektionen mit Schadsoftware sein.

### Gandcrab

GandCrab gehörte 2018 ebenfalls zu den wichtigsten Akteuren und nutzte kurz nach seinem ersten Auftreten im Januar verschiedene Exploit-Kits. Die Zahl der Infektionen sank dann etwas und blieb während des größten Teils des Jahres konstant. Nur im Februar kam es zu einer deutlichen Spitze in der Aktivität, was auf zahlreiche Spam-Kampagnen im 1. Quartal zurückzuführen ist.

Nachdem GandCrab das Magnitude Exploit-Kit für seine Weiterverbreitung nutzte, verursachte diese Schadsoftware auch weiterhin Probleme für Netzwerkadministratoren und Privatnutzer. Das ist teilweise auf die unkonventionellen Methoden zum Laden von Schadsoftware zurückzuführen, durch die sich Magnitude auszeichnet. Im Wettrennen um den ersten Platz als schlimmster Bedrohungsakteur überhaupt wurde von dateilosen Techniken bis hin zum Binary-Padding (bei dem zusätzliche Daten zu Dateien hinzugefügt werden, um Scanvorgänge zu umgehen) so ziemlich alles eingesetzt.

**Weltweite GandCrab-Erkennungen 2017 - 2018**

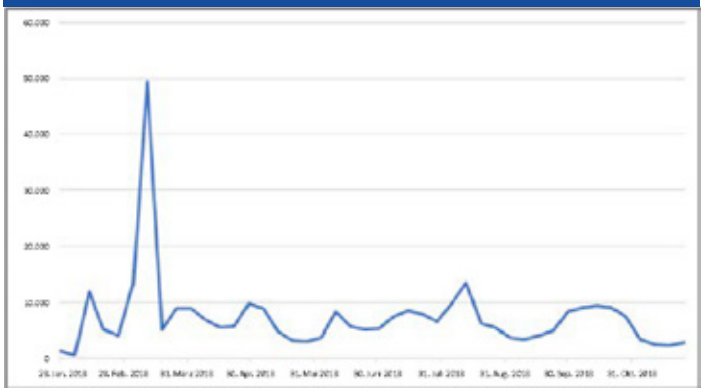

*Abbildung 34: Weltweite GandCrab-Erkennungen im Jahr 2018*

GandCrab, die wichtigste Ransomware-Variante des 2. Quartals 2018, ist auch deshalb bemerkenswert, weil sie die erste Ransomware ist, die von den Opfern die Lösegeldzahlung in einer anderen Kryptowährung als Bitcoin fordert. Zu dem Zeitpunkt, als die Ransomware-Erkennungen bei den Unternehmen um 28 Prozent gestiegen waren, das Gesamtvolumen jedoch weiterhin niedrig blieb, wurde GandCrab zu einer der führenden Quellen für Kampagnen mit bösartiger Ransomware – zum unendlichen Ärger der Opfer.

### Jahresende

Obwohl die Ransomware im Vergleich zu anderen Bedrohungen wie Cryptominern und Trojanern an Boden verloren hat, muss noch immer mit ihr gerechnet werden. Und so war 2018 das Jahr des heimlichen Experimentierens und der Neubewertung. Im Allgemeinen ist die Öffentlichkeit heute wesentlich sensibilisierter, was solche Angriffe anbelangt, und die gleichen alten Tricks funktionieren eben nicht ewig. Wir erwarten daher weitere Überarbeitungen von älteren Dateien und stärkere Verbindungen zu den neuesten Exploit-Kits, um die Verbreitung von Ransomware auch weiterhin voranzutreiben.

# Nennenswerte Angriffsvektoren

2018 war ein Mix aus Alt und Neu: Die Autoren von Schadsoftware griffen einerseits auf herkömmliche Techniken wie MalSpam und Social Engineering zurück, um ihre Software zu verbreiten, und erkundeten andererseits mit dem browserbasierten Cryptomining auch ganz neue Gefilde. Zudem wurden die Bedrohungsakteure bei der Vermeidung einer Erkennung noch kreativer, indem sie bösartigen Code in Online-Zahlungsplattformen einspeisten, bösartige Apps in legitime Webstores einschleusten und mit Plug-ins, die mehr Schaden als Gutes anrichteten, vertrauliche Informationen direkt vor den Augen der Benutzer stahlen. Werfen wir nun einen Blick auf die nennenswertesten Angriffsvektoren des vergangenen Jahres.

## MalSpam

Emotet und TrickBot, zwei der schlimmsten Albträume, die uns 2018 heimsuchten, machten gemeinsame Sache, um zu einem effektiven Angriffsschlag auszuholen. Das beinhaltete u. a. auch die Verbreitung der Schadsoftware über MalSpam, die sich als legitime E-Mail tarnte – ganz im Stil einer klassischen Phishing-/Spear-Phishing-Kampagne. Was diese Angriffe jedoch so unglaublich wirksam machte, war nicht nur die Art, wie die Schadsoftware eingeschleust wurde, sondern wie sie sich verbreitete.

Emotet wird im Allgemeinen über MalSpam verbreitet, die infizierte Anhänge oder eingebettete URLs enthält. Dabei spielt Social Engineering eine Rolle. Da Emotet die E-Mail-Konten des Opfers übernimmt, erhalten die Empfänger bösartige E-Mails, die von vertrauenswürdigen Quellen zu stammen scheinen. Der infizierte Anhang besteht in der Regel aus einem Microsoft Word-Dokument mit aktivierten Makros.

Sobald Emotet ein Netzwerk infiltriert hat, nutzt es EternalBlue, eine der SMB-Schwachstellen, die von der Gruppe „The Shadow Brokers“ im letzten Jahr veröffentlicht wurde, um nicht gepatchte Systeme auszunutzen. Die infizierten Rechner versuchen zum einen, Emotet extern über das integrierte Spam-Modul und zum anderen lateral zu verbreiten, wobei die für die Domäne geltenden Anmeldeinformationen mittels Brute-Force-Angriffen ausgespäht werden. Aus diesem Grund ist das Emotet-Botnet noch immer ziemlich aktiv und für einen großen Teil der uns über den Weg laufenden MalSpams verantwortlich.

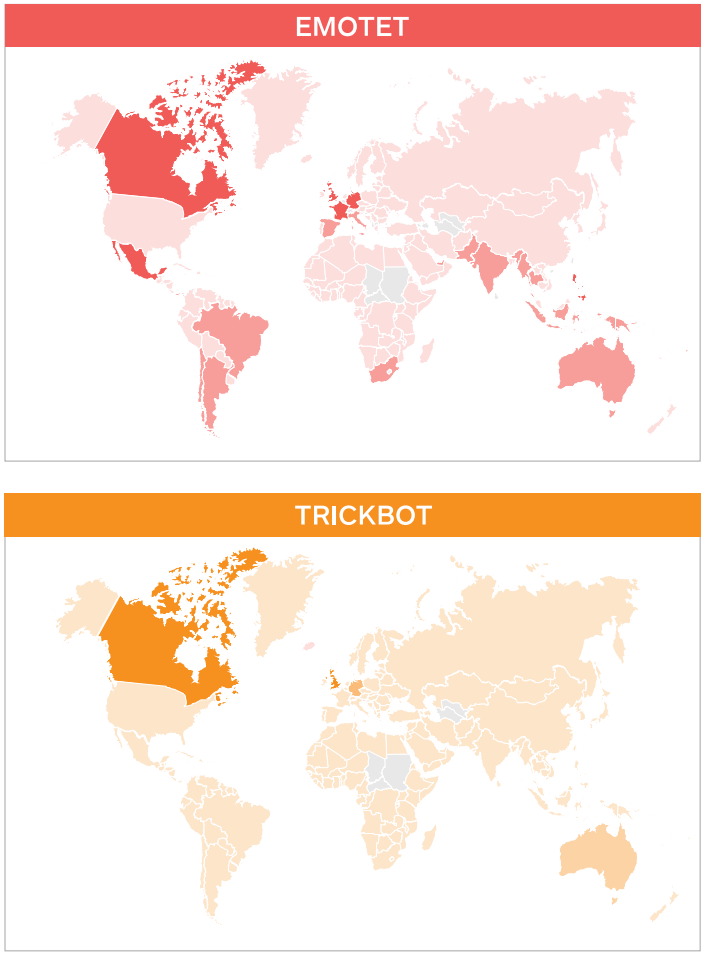


*Abbildung 35: Weltweite Erkennungen von Emotet im Vergleich zu TrickBot*

TrickBot ist ein weiterer aktiver Trojaner, der MalSpam nutzt, um Systeme zu infizieren. Dieser Trojaner arbeitet primär mit infizierten Word-Dokumenten, nutzt aber auch eingebettete URLs, die zu infizierten PDF-Dateien führen. Wie Emotet verwendet auch TrickBot eine der SMB-Schwachstellen – in diesem Fall EternalRomance –, um sich lateral in einem Netzwerk zu bewegen.

Relativ neu an der MalSpam-Front sind Office-Dokumente, die es schaffen, dem macOS-Sandkasten für Office-Makros zu entgehen. Die in Word-Makros eingebettete Schadsoftware, derzeit als OSX.BadWord erkannt, richtet mithilfe von Python eine Backdoor auf dem betroffenen System ein.

## Angriffe auf Websites

2018 konnten wir eine stetige Zunahme von spektakulären Angriffen auf vertrauenswürdige, legitime eCommerce-Websites beobachten. Dabei werden Softwarekomponenten, die von Dritten stammen und Bestandteil dieser Websites sind, manipuliert, um auf Kreditkartendaten und andere personenbezogene Informationen zuzugreifen. Ein solcher Angriff auf British Airways betraf rund 400.000 Kunden, deren Namen, Privatanschriften und Finanzdaten gestohlen wurden.

Die als „Magecart" bekannte Gruppe von Bedrohungsakteuren lauerte auf vertrauenswürdigen Websites und stahl so Zahlungs- und Kontaktdaten, die Website-Besucher beim Abschluss ihres Einkaufs eingaben. Die Magecart-Angriffe nutzten Schwachstellen im Code der Seiten aus, die zur Zahlungsabwicklung dienten, und verwendeten Cross-Site-Scripting (XXS). Mehrere Gruppen, die die Magecart-Taktik nutzen, konkurrieren manchmal miteinander, indem sie den Code der anderen Gruppen manipulieren.

Der unten abgebildete bösartige Code ist das Werk von Magecart und wurde in einem verschleierten Format an ein legitimes und vertrauenswürdiges Skript angefügt.

Nach dem Decodieren des Skripts ist der Code sichtbar, der für das Abschöpfen der Daten verantwortlich ist, sobald die Kunden auf die Schaltfläche für „Kasse" klicken. Auf Netzwerkebene sieht dies wie eine POST-Anfrage aus, bei der jedes Feld (Name, Adresse, Kreditkartennummer, Gültigkeitsdauer, CVV-Sicherheitscode etc.) im Base64-Format an einen betrügerischen Server (in diesem Fall info-stat[.]ws) gesendet wird, den die Kriminellen kontrollieren.

Diese Art von Angriff erfolgt sowohl für den Händler als auch den Kunden auf transparente Weise. Im Gegensatz zu Sicherheitsverletzungen, die Datenbanklecks betreffen und bei denen die Daten verschlüsselt sein können, sind Web-Skimmer in der Lage, die Daten im Klartext und in Echtzeit zu erfassen.

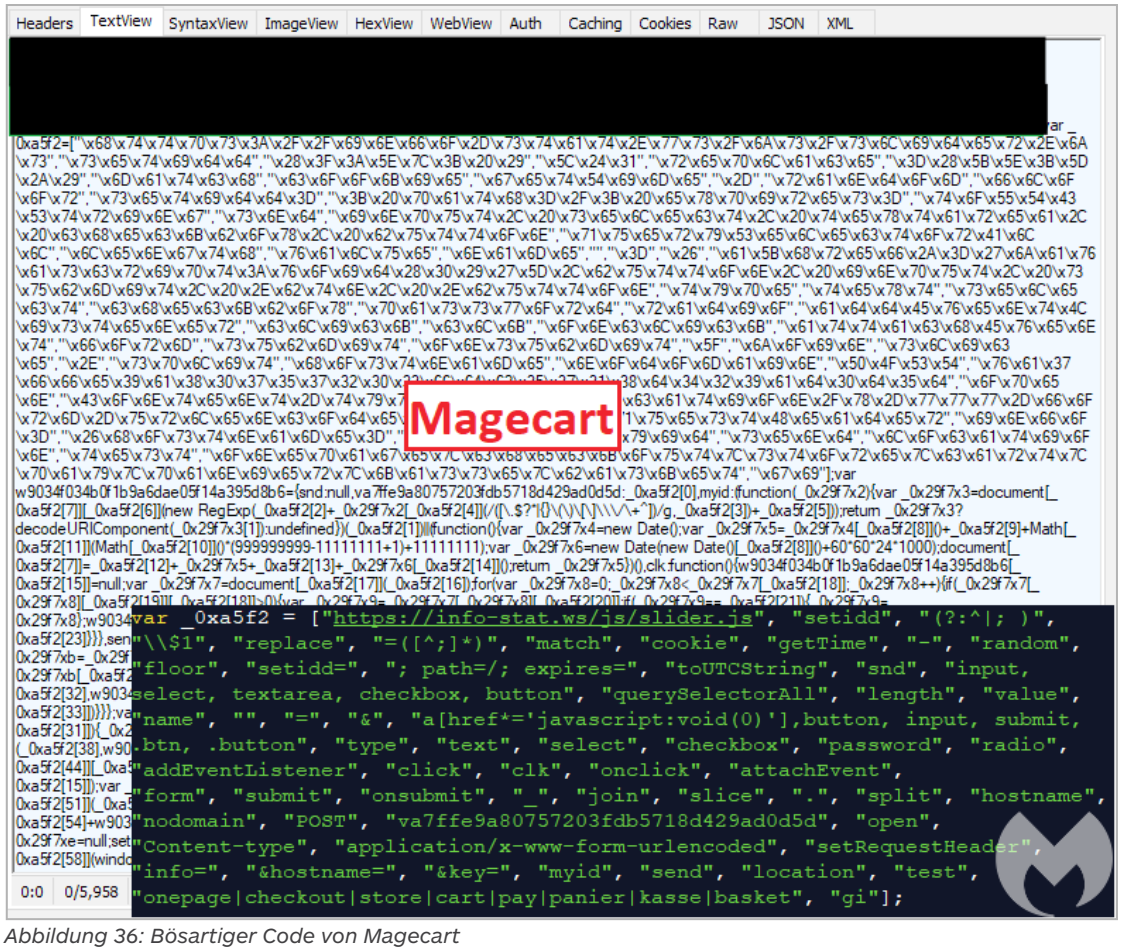

*Abbildung 36: Bösartiger Code von Magecart*

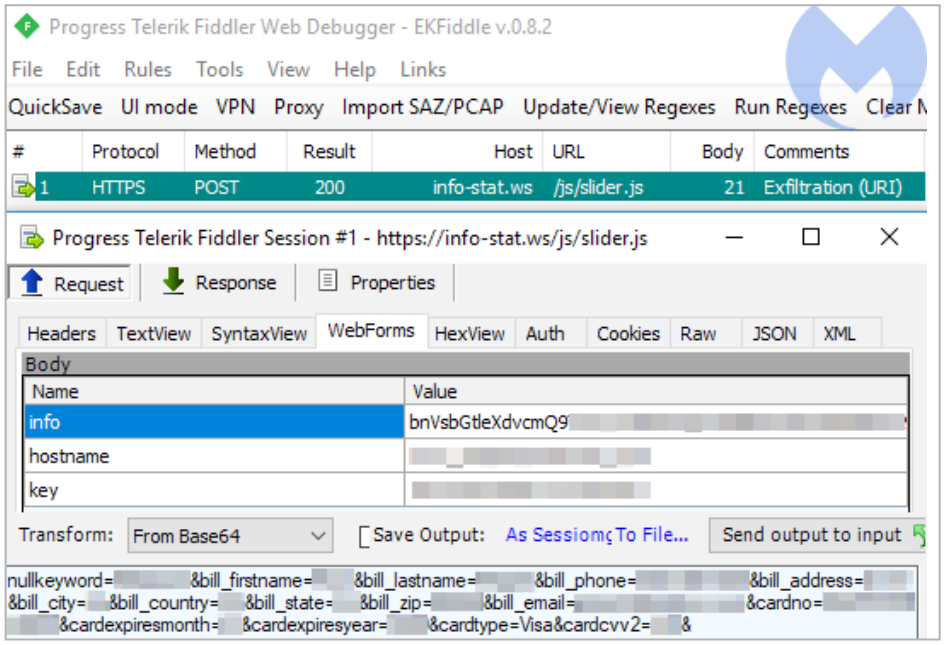


*Abbildung 37: Magecart-Code sendet Details über einen bösartigen Server*

## Bösartige Browser-Erweiterungen

2018 schlugen bösartige Browser-Erweiterungen (Plug-ins) hohe Wellen. Mal wurden legitime Erweiterungen manipuliert und bei Angriffen auf Lieferketten verwendet, mal versprachen bösartige Erweiterungen dem Benutzer Datenschutz, während sie gleichzeitig seine gesamten Online-Bewegungen nachverfolgten. Kurzum: Es gab zahlreiche Beispiele und Varianten. Einige der herausragenderen Fälle, die wir beobachten konnten, waren:

» Manipulierte legitime Erweiterungen wurden bei Angriffen auf Lieferketten eingesetzt. Hier ist vor allem die Chrome-Erweiterung für den File-Sharing-Dienst MEGA.nz zu nennen, deren manipulierte Version Benutzernamen und Kennwörter stahl. Die Benutzer konnten den Unterschied zu der echten Erweiterung nur bemerken, weil die gehackte Version einige zusätzliche Berechtigungen anforderte.

» Eine ganze Reihe von Firefox-Erweiterungen (und auch einige von Chrome) wurden auf frischer Tat ertappt, während sie den Browser-Verlauf ihrer Benutzer ausspähten.

» Verschiedene Erweiterungen ahmten beliebte Plug-ins nach, um die Benutzer dazu zu verleiten, sie zu installieren. Dazu gehörte u. a. auch eine Erweiterung, die behauptete, dass sie das Online-Verhalten ihrer Benutzer nicht nachverfolgen und auch keine Daten speichern, sondern die Benutzer stattdessen vor den neugierigen Blicken der Browser selbst schützen würde. Doch stattdessen erhielten die Benutzer eine Erweiterung, die ihre Homepage einfach an Yahoo! umleitete.

Die gute Nachricht ist allerdings, dass sich die wichtigsten Browser-Anbieter dadurch genötigt sahen, Maßnahmen gegen diese bösartigen Erweiterungen zu ergreifen. Nachfolgend erfahren Sie, welche Änderungen sie bisher implementiert haben:

» Inline-Installationen wurden unterbunden. Jetzt muss alles über die offiziellen Webstores laufen.

» Verschleierter Code in den Erweiterungen wurde blockiert.

» Support für Legacy-Protokolle wie TLS 1.0 und 1.1 wird eingestellt; dies wurde für 2020 angekündigt.

Zwar haben die wichtigsten Browser-Anbieter Maßnahmen ergriffen, um zu verhindern, dass bösartige Erweiterungen in ihre Webstores eindringen, doch schleicht sich trotzdem noch immer eine hohe Zahl von Adware und PUPs ein. Bei der Mehrzahl handelt es sich um Hijacker, die die Standardsuchmaschine Ihres Browsers oder die Startseiten und Seiten für neue Registerkarten ändern können. In manchen Fällen behaupten sie, Ihre Privatsphäre bei der Suche zu verbessern.

Und während wir den Benutzern immer wieder ans Herz legen, all ihre Apps nur über die offiziellen Webstores zu beziehen, entschieden die Anbieter des beliebten Spiels „Fortnite“, die Android-Version des Spiels außerhalb von Google Play anzubieten. Um das Spiel zu erhalten, müssen Benutzer die Option „Apps aus unbekannten Quellen installieren“ aktivieren, die zur Installation unerwünschter anderer Programme führen kann. Und um alles noch schlimmer zu machen, ließ ihr Installer Man-in-the-Disk-Angriffe zu: eine Möglichkeit für bösartige Apps, den Installer zu übernehmen und statt der legitimen App die eigene Junkware zu installieren.

## Exploits

Wir hatten erwartet, dass es auch 2018 zu Angriffen mithilfe von bösartigen Spam-E-Mails und Microsoft Office-Dokumenten kommen würde, da wir diesen Trend bereits im Vorjahr ausgemacht hatten.

Allerdings konnten wir eine interessante Verlagerung beobachten, was die Ausnutzung von Schwachstellen betrifft. Da die Browser sicherer geworden sind und automatisch aktualisiert werden, ist die Anzahl der Drive-by-Downloads mittlerweile deutlich geringer. Daher gehört der E-Mail-Vektor jetzt zu den Methoden, auf die sich Bedrohungsakteure in der Hauptsache verlassen, um in Systeme einzudringen.

### Plug-in- und Browser-Exploits

Gleich zu Beginn des Jahres konnten wir beobachten, dass eine Zero-Day-Schwachstelle im Flash Player (CVE-2018-4878) für gezielte Angriffe auf Südkorea genutzt wurde, die von vielen der Lazarus-Gruppe zugeschrieben werden.

Der Exploit war in eine Excel-Tabelle eingebettet, die als Köder diente, und wurde als ActiveX-Objekt geladen. Schon bald setzte auch eine ganze Reihe von anderen Exploit-Kit-Autoren diese Schwachstelle in den webbasierten Toolkits ein, die sie zur Verbreitung ihrer Schadsoftware nutzen.

Ende April wurde ein weiterer Zero-Day für die VBScript Engine (CVE-2018-8174) entdeckt. Dies war deshalb so bedeutend, weil schon seit zwei Jahren kein neuer Exploit mehr aufgetreten war, der sich auf den beliebten Internet Explorer auswirkt. Außerdem ist es bemerkenswert, dass auch dieser Zero-Day wieder in ein Dokument eingebettet war, statt als Drive-by Download verbreitet zu werden. Nach dem typischen Zyklus Zero-Day ➔ Patch ➔ Proof-of-Concept (PoC) hat sich dieser neue Exploit neben anderen Exploit-Kits für Browser etabliert und löst damit seinen Vorgänger, CVE-2016-0189, ab.

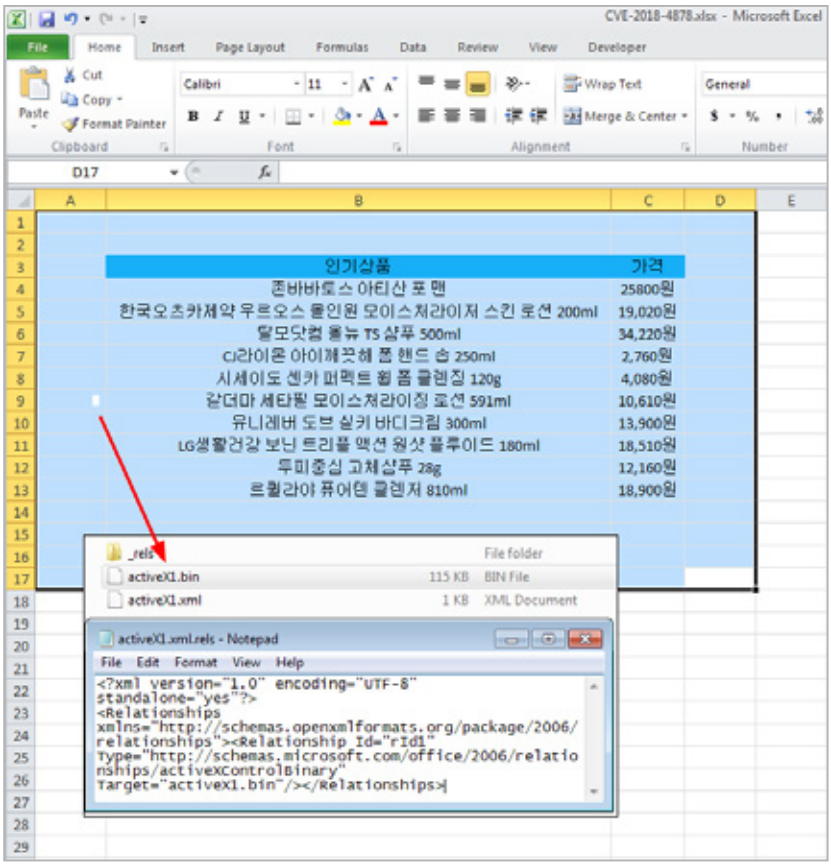


*Abbildung 38: Verborgenes Flash ActiveX-Objekt in anscheinend harmlosem Dokument, das als Köder dient*

## Massensicherheitsverletzungen über Router

Tatsächlich erwies sich der gesamte Monat April als turbulent, da in RouterOS, dem Betriebssystem, mit dem MikroTik-Router arbeiten, ein kritischer Fehler gefunden wurde, der eben diese Router beeinträchtigt (CVE-2018-14847).

Um ein Eindringen zu vermeiden, wurde dringend empfohlen, den Zugriff auf Winbox (das Management-Panel von MikroTik) über die Firewall zu beschränken. Die Angreifer automatisierten Anmeldeversuche und nutzten sogar Schadsoftware, um die als Path bzw. Directory Traversal bezeichnete Schwachstelle auszunutzen.

Zur Beseitigung des Problems mussten nicht nur die entsprechenden Sicherheitspatches installiert, sondern auch bestimmte Konfigurationsdateien bereinigt werden. Diese Dateien wurden oftmals genutzt, um Coinhive Cryptojacking-Skripte einzuschleusen, sodass jeder, der mit einem infizierten Router verbunden war, nach Kryptowährungen schürfte. Dabei spielte es keine Rolle, welches Gerät verwendet oder welche Website besucht wurde.

| Destination | Protocol | Length | Host | Destination Port | Info |
|---|---|---|---|---|---|
| 205.75.189.11 | TCP | 66 | | 8291 | [TCP Retransmission] 51413 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 117.110.101.12 | TCP | 66 | | 8291 | 51612 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 141.48.175.12 | TCP | 66 | | 8291 | 51613 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 145.18.117.6 | TCP | 66 | | 8291 | 51614 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 149.169.155.11 | TCP | 66 | | 8291 | 51615 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 14.197.184.11 | TCP | 66 | | 8291 | [TCP Retransmission] 51412 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 149.186.248.5 | TCP | 66 | | 8291 | [TCP Retransmission] 51415 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 117.253.121.6 | TCP | 62 | | 8291 | [TCP Retransmission] 51072 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 108.170.10.5 | TCP | 62 | | 8291 | [TCP Retransmission] 51076 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 65.145.62.4 | TCP | 62 | | 8291 | [TCP Retransmission] 51075 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 185.191.70.10 | TCP | 66 | | 8291 | 51618 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 23.170.31.7 | TCP | 62 | | 8291 | [TCP Retransmission] 51077 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| [illegible] | TCP | 66 | | 8291 | [TCP Retransmission] 51416 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 120.158.22.4 | TCP | 62 | | 8291 | [TCP Retransmission] 51074 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 20.30.98.11 | TCP | 62 | | 8291 | [TCP Retransmission] 51079 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 45.41.146.10 | TCP | 66 | | 8291 | 51619 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 81.47.189.5 | TCP | 66 | | 8291 | 51620 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 135.122.138.5 | TCP | 62 | | 8291 | [TCP Retransmission] 51078 → 8291 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |

*Abbildung 39: Schadsoftware scannt standardmäßigen Winbox-Port (8291) auf andere Geräte mit Schwachstellen*

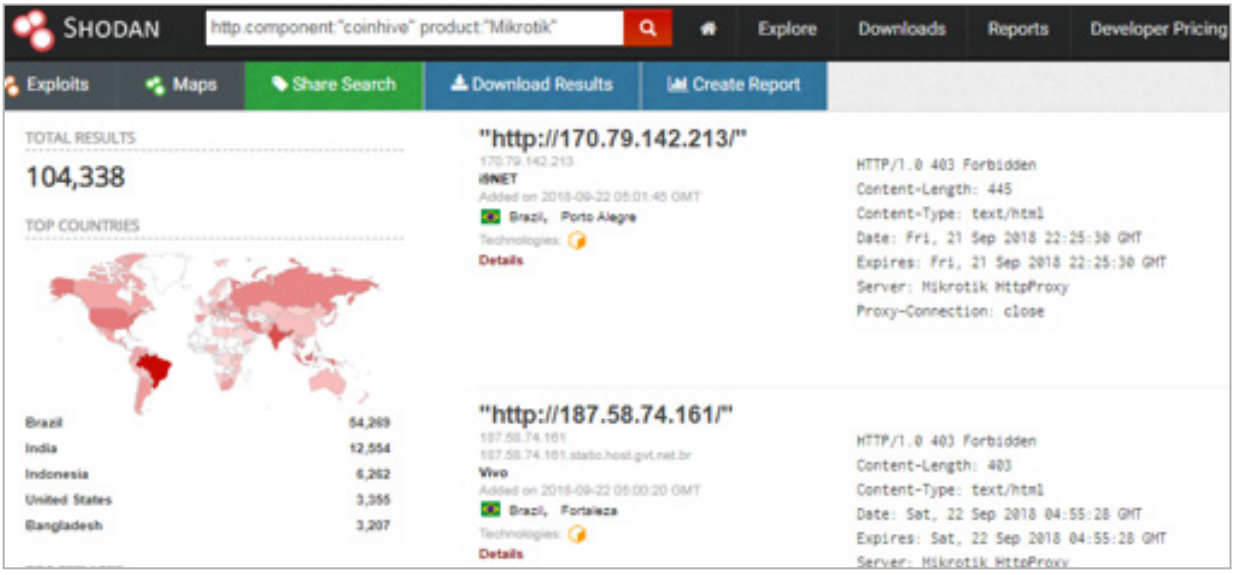


*Abbildung 40: Shodan-Scan ergibt mehr als 100.000 beeinträchtigte MikroTik-Geräte*

## CMS-Hackerangriffe

Man kann nicht von der Bedrohungslandschaft 2018 sprechen, ohne zu erwähnen, inwiefern Content Management Systeme (CMS) von Exploits betroffen waren. Die Angreifer entdeckten oder nutzten häufig Remote Code Execution-Schwachstellen in beliebter Software wie WordPress, Jooma oder Drupal aus.

Drupal gehörte zu den CMS-Systemen, die in der ersten Jahreshälfte 2018 am härtesten getroffen wurden, was zu einem großen Teil auf fortlaufende Schwachstellen (CVE-2018-7600 und CVE-2018-7602) zurückzuführen war, die zu massiven Beeinträchtigungen führten.

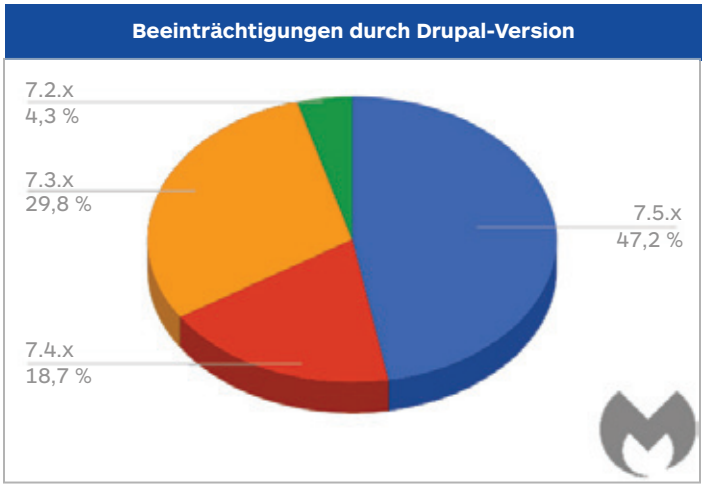


*Abbildung 41: Am stärksten betroffene Sites nach Drupal-Version (7.x-Zweig)*

Die meisten Website-Besitzer achten nicht darauf, ihre CMS-Systeme (oder die Plug-ins dieser Systeme) auf dem neuesten Stand zu halten, weshalb es keine Überraschung ist, dass sie zu Opfern werden. Als Grund dafür, dass sie lieber mit einer älteren Version arbeiten, wird häufig die Sorge genannt, eine Website könnte durch ein Upgrade plötzlich nicht mehr funktionieren. Das bedeutet jedoch, dass diese Websites – sofern sie nicht durch irgendeine Art von Anwendungsfirewall geschützt sind – ganz einfach gehackt werden können.

Zero-Days in Browsern und Plug-ins standen 2018 auf der Liste ganz oben – wurden jedoch nicht unbedingt so genutzt, wie man es erwarten würde. Die Angreifer haben sie vielmehr mit Spear-Phishing- oder Social-Engineering-Angriffen kombiniert, die in Office-Dateien versteckt waren.

Außerdem hatten es die Kriminellen auch auf Hardware – insbesondere Router – abgesehen, um im großen Umfang Schaden anzurichten. Wie wir wissen, sind diese Geräte oftmals veraltet und werden höchstwahrscheinlich nie gepatcht, bis sie einfach aufhören zu arbeiten. Das ist das perfekte Szenario für Angreifer und solange sich die Benutzer der Gefahr nicht bewusst sind, ist dieses Szenario für Anbieter von Sicherheitsprodukten nur schwer zu bekämpfen.

# Nennenswerte Scams

2018 konnten wir eine Vielzahl von Scams ausmachen, die oftmals die Entwicklung der Schadsoftware-Erzeugung und -Verbreitung widerspiegelten. Im 1. Quartal beherrschte das Cryptomining praktisch jeden Aspekt der Internetkriminalität. Das schloss auch Scams ein. Die erfolgreichsten Akteure konsolidierten ihre Ressourcen und nutzten einfallsreichere Taktiken, durch die sie einfache als technischer Support getarnte Betrugsmaschen hinter sich ließen und sich stattdessen nun gleich selbst in den Cryptowallets bedienen. Im 2. Quartal ging der Trend weg von den Cryptoscams und hin zum Abschöpfen personenbezogener Informationen – eine Taktik, die heute noch immer aktiv genutzt wird.

Besonders nennenswert sind dabei als technischer Support getarnte Maschen mit Bezug auf Coinbase, bei denen spektakulär abgeräumt wurde – vor allem aufgrund mangelnden Betrugsschutzes von Bitcoin und Coinbase selbst. In Berichten von Opfern auf Twitter ist die Rede von leergeräumten Konten und Verlusten in fünfstelliger Höhe. Es ist daher zu vermuten, dass es sich für diese Bedrohungsakteure als einfacher erwiesen hat, nach Belieben Wallets zu leeren als technischen Support vorzutäuschen.

Zudem wurde Anfang 2018 eine neue Art der Leadgenerierung beobachtet, bei der mittels API-Missbrauch der Browser des Opfers gesperrt wird und dann nicht mehr reagiert. Primäres Ziel für diese Angriffsart war Chrome, doch auch Firefox und Brave wurden in Mitleidenschaft gezogen.

## Ausnutzbare Geschäftspraktiken

Als technischer Support getarnte Betrugsmaschen sind vor allem von ausnutzbaren Geschäftspraktiken abhängig und nicht von bestimmten Tools. Bei den Betrugsmaschen in Zusammenhang mit Coinbase wurde die Tatsache ausgenutzt, dass es bei Bitcoin-Transaktionen an Betrugsschutz mangelt. Aus diesem Grund machten die Betrüger überdurchschnittlich hohe Gewinne. Beim API-Missbrauch ist die eigentliche Schwachstelle die lange Zeit, die zwischen dem Bericht an das Unternehmen und einem späteren Patch vergeht.

Da Browserfunktionen im Allgemeinen ganz legitime Funktionen für viele Nutzer erfüllen, ist die Wartezeit auf einen Patch in Support-Betrugsfällen in der Regel relativ lang. Betrüger können dies entsprechend ausnutzen.

Wir gehen davon aus, dass Betrugsmaschen in Verbindung mit Bitcoin und Browser-Missbrauch noch für längere Zeit zum Portfolio von Betrügern zählen werden.

## Personenbezogene Daten (PII) als Ziel

Im Verlauf des 2. Quartals zielten Scammer zunehmend auf personenbezogene Informationen ab. Wir haben Betrüger dabei beobachtet, wie sie über Bitcoin-Maschen von ihren Opfern unverhohlen PII stehlen. Geringe Reglementierung, beschränkter Betrugsschutz und unzureichender Support beim Geldwechsel haben dazu beigetragen, dass Social-Engineering-Angriffe auf Bitcoin-Wallets äußerst lukrativ sind. Doch da sich der Pool an Opfern für traditionelle, als technischer Support getarnte Betrugsmaschen angesichts der zunehmenden Achtsamkeit bei den Benutzern und der verstärkten gesetzlichen Vollstreckung verkleinert hat, haben Betrüger immer häufiger Kennwörter, Bankkontodaten und E-Mail-Konten gestohlen. Neue DSGVO-Regelungen haben wahrscheinlich noch Öl auf dieses Feuer gegossen, da die Art von Daten, die aus PII-Diebstahl hervorgehen, auf dem Schwarzmarkt ein ansehnliches Gehalt einbringen.

## Sextortion

Anfang Juli machte eine Erpressungskampagne aufgrund ihres Ausmaßes und einer Neuerung auf sich aufmerksam. Im Gegensatz zu traditionellen sexbasierten Erpressungskampagnen wurde in dieser E-Mail-Kampagne ein Benutzerkennwort des E-Mail-Empfängers verwendet. Damit sollte bewiesen werden, dass der Sender die Daten des Opfers gehackt hatte. Diese Anmeldeinformationen stammen wahrscheinlich aus einer Vielzahl von zurückliegenden, spektakulären Sicherheitsverletzungen, bei denen während der letzten vier Jahre große Mengen an Daten durchgesickert sind. Die Anmeldeinformationen waren korrekt, obwohl die Mehrzahl der Opfer angab, dass die Bedrohungsakteure alte und oftmals abgelaufene Kennwörter verwendeten.

Die Verwendung von durchgesickerten Anmeldeinformationen als ein Social-Engineering-Tool ist ein relativ neues Konzept dieser Angriffsart und eine zusätzliche Möglichkeit, um diese Anmeldeinformationen in klingende Münze umzuwandeln und der anschließenden Erpressung einen Anschein von Glaubwürdigkeit zu verleihen. Da sich bei den Einbrüchen in Fremdsysteme keine Anzeichen für einen Rückgang erkennen lassen, ist zu erwarten, dass diese Technik auch in Zukunft als Unterstützung bei Phishing, Erpressung und anderen Betrugsversuchen verwendet werden wird.

## Die Schlinge enger ziehen

Im letzten Quartal konnten wir feststellen, dass sich Betrüger, die es auf die Kreditkartendaten von Malwarebytes-Kunden abgesehen hatten, anderen Dingen zuwandten. Kreditkartenverarbeiter haben zunehmend Maßnahmen gegen Betrüger ergriffen, die ihre Plattformen missbrauchten. Das hat dazu geführt, dass sich die Internetkriminellen auf weniger stark überwachte Plattformen wie PayPal und Formate mit geringerem Betrugsschutz (wie Bitcoin) und weniger persönlichen Überprüfungen verlagert haben. Zwar erhalten die Bedrohungsakteure so einen stabileren Geldstrom, allerdings wird dadurch auch der Umfang ihrer Aktivitäten eingeschränkt, wodurch es im letzten Quartal zu einer geringeren Zahl von gemeldeten Opfern kam.

Eine weitere Reaktion auf die zunehmenden Schutz- und Sicherheitsmaßnahmen bestand darin, dass Internetkriminelle nach und nach immer weniger Kaltanrufe nutzen und stattdessen Sprachnachrichten hinterlassen, in denen um Rückruf gebeten wird. Rückrufe sind ein erprobtes Mittel, um nur mit den leichtgläubigsten Opfergruppen in Kontakt zu treten und all jene auszuschließen, die bereits beim ersten Anruf dazu neigen, bohrende Fragen zu stellen.

## Ausblicke

Für dieses Jahr erwarten wir, dass – ähnlich wie bei der Welle der Sextortion-E-Mails – Social-Engineering-Angriffe auf Basis von PII bei Internetkriminellen an Popularität gewinnen werden. Angesichts des zunehmenden Geschwindigkeit, mit der es zu umfangreichen Sicherheitsverletzungen kommt, und der weitverbreiteten Angewohnheit, Anmeldeinformationen plattformübergreifend immer wieder zu verwenden, steht Bedrohungsakteuren dank der durchgesickerten PII ein hervorragendes Druckmittel zur Verfügung, um Social-Engineering-Angriffe noch effizienter zu gestalten – und das mit begrenzten Verlusten oder Kosten für die Angreifer. Und das Beste für den Angreifer ist, wie die Sextortion-Kampagne gezeigt hat, dass die personenbezogenen Informationen, die bei einem Social-Engineering-Angriff verwendet werden, nicht einmal genau oder aktuell zu sein brauchen, um effektiv zu sein. Demzufolge ist für die Zukunft mit weiteren Kampagnen dieser Art zu rechnen.

# Prognosen für 2019

Im Hinblick auf das neue Jahr werden wir oft gebeten, Prognosen darüber abzugeben, welche Trends einschlafen und welche neuen Trends aufkommen werden. Zwar können wir aufgrund unserer Erfahrung und logischer Schlussfolgerungen begründete Vermutungen über die möglichen Höhen und Tiefen im Bereich der Internetkriminalität anstellen, aber im Grunde kann uns selbst alle Erfahrung dieser Welt nicht auf die immer neuen Tricks und Betrugsmaschen vorbereiten, wie wir sie beispielsweise im Zuge der Cryptomining-Euphorie erlebt haben. Wenn es um Internetkriminalität geht, lässt sich nichts wirklich mit hunderprozentiger Sicherheit vorhersagen.

Aber das heißt nicht, dass wir uns nicht etwas Zeit nehmen sollten, um uns ein paar Gedanken über die Zukunft zu machen und uns gegen mögliche Gefahren zu wappnen, die schon an der nächsten Ecke lauern. Lesen Sie nun, was unserer Meinung nach 2019 passieren wird. Ziehen Sie sich warm an!

## Neue, spektakuläre Sicherheitsverletzungen werden die Sicherheitsindustrie antreiben, endlich eine Lösung für das Benutzername/Kennwort-Problem zu entwickeln.

Das ineffektive Benutzername/Kennwort-Verfahren plagt Privatanwender und Unternehmen bereits seit Jahren. Es gibt viele Lösungen – asymmetrische Kryptografie, Biometrik, Blockchain, Hardware-Lösungen etc. –, aber bisher konnte man sich in der Cybersicherheitsbranche nicht auf einen Standard einigen, um das Problem zu beheben. 2019 wird es zu besser konzertierten Anstrengungen kommen, um Kennwörter komplett zu ersetzen.

## IoT-Botnets werden auch in Ihre Nähe rücken.

In der zweiten Jahreshälfte 2018 wurden mehrere Tausend MikroTik-Router gehackt, um Coin-Miner einzuschleusen. Und das dürfte erst der Anfang gewesen sein. Höchstwahrscheinlich müssen wir in diesem neuen Jahr mit weiteren Angriffen dieser Art rechnen, wobei immer mehr Hardware beeinträchtigt werden wird, um von Cryptominern bis zu Trojanern so ziemlich alles einzuschmuggeln. Angriffe auf Router und IoT-Geräte werden im großen Stil stattfinden.

Das Problem ist, dass diese Geräte weitaus schwieriger zu patchen sind als Computer. Selbst durch Patches lässt sich das Problem nicht mehr beheben, wenn ein Gerät erst einmal infiziert ist.

## Digitales Skimming (das illegale Ausspähen von Bank- oder Kreditkartendaten) wird an Häufigkeit zunehmen und immer raffinierter werden.

Die Internetkriminellen sind hinter Websites her, die Zahlungen bearbeiten, und manipulieren die Checkout-Seite direkt. Gleichgültig, ob Sie Roller Skates oder Konzerttickets kaufen: Wenn die Software für den Einkaufswagen gehackt wurde, werden Ihre Daten, sobald Sie sie auf der Checkout-Seite (zur Bezahlung Ihres Einkaufs) eingeben, in Klartext versendet, wodurch Angreifer die Möglichkeit haben, die Daten in Echtzeit abzufangen. Sicherheitsunternehmen konnten dies bei den Hacker-Angriffen auf British Airways und Ticketmaster beobachten.

## EternalBlue oder ein Nachahmer werden 2019 zur De-facto-Methode für die Verbreitung von Schadsoftware.

Da sie in der Lage sind, sich selbst zu verbreiten, stellen EtnernalBlue und andere Schadprogramme, die die SMB-Schwachstellen ausnutzen (darunter auch EternalRomance und EternalChampion), eine besondere Herausforderung für Organisationen dar. Genau das werden Internetkriminelle ausnutzen, um neue Schadsoftware zu verbreiten.

## Cryptomining auf Desktops steht – zumindest auf Privatanwenderseite – vor dem Aus.

Auch hier gilt, wie wir im Oktober 2018 beobachten konnten, als MikroTik-Router gehackt wurden, um Miner einzuschleusen, dass es sich für Internetkriminelle nicht lohnt, einzelne Privatanwender mit Cryptominern anzugreifen. Stattdessen werden sich Angriffe, bei denen Cryptominer verbreitet werden, auf Plattformen konzentrieren, die höhere Umsätze generieren können (Server, IoT), und werden von anderen Plattformen langsam verschwinden (browserbasiertes Mining).

## Schadsoftware, die darauf ausgelegt ist, unerkannt zu bleiben (wie z. B. Soundlogger), wird in Umlauf gebracht werden.

Keylogger, die Geräusche aufzeichnen, werden gelegentlich auch als Soundlogger bezeichnet, und können anhand von Lautstärke und Frequenz des Tippens feststellen, welche Tastaturtasten gedrückt werden. Diese Angriffsart wurde von nationalstaatlichen Akteuren entwickelt, um sie gegen Gegner zu richten, und besteht daher schon eine Weile. Wahrscheinlich werden Angriffe, die diese und andere neue Methoden nutzen und darauf ausgelegt sind, der Erkennung zu entgehen, in Umlauf gebracht werden und Unternehmen sowie die allgemeine Öffentlichkeit zum Ziel haben.

## Internetkriminelle werden zur Erstellung bösartiger ausführbarer Dateien künstliche Intelligenz einsetzen.

Zwar ist die Vorstellung, dass bösartige künstliche Intelligenz auf dem System eines Opfers ausgeführt wird, mindestens noch für die nächsten zehn Jahre reine Science Fiction, aber Schadsoftware, die von KI modifiziert und erstellt wird und mit der KI kommuniziert, ist bereits eine sehr gefährliche Realität. Eine KI, die mit manipulierten Computern kommuniziert und überwacht, wie bestimmte Schadsoftware erkannt wird, kann innerhalb kürzester Zeit Gegenmaßnahmen implementieren. KI-Steuerungen werden Schadsoftware möglich machen, die darauf ausgelegt ist, ihren Code selbstständig zu verändern, um der Erkennung auf einem System zu entgehen, wobei es keine Rolle spielt, welches Sicherheits-Tool eingesetzt wird. Stellen Sie sich eine Schadsoftware-Infektion vor, die sich praktisch wie die „Borg“ aus Star Trek verhält und ihre Angriffs- und Verteidigungsmechanismen spontan an alles anpasst, das sich ihr entgegenstellt.

## Bring-Your-Own-Security wird in dem Maße zunehmen, in dem das Vertrauen abnimmt.

Immer mehr Privatanwender bringen ihre eigenen Sicherheitslösungen als erste oder zweite Schutzebene mit an den Arbeitsplatz, um ihre persönlichen Informationen zu schützen. Da man sich in den einzelnen Branchen nach und nach der Gefahren bewusst wird, die mit BYOS einhergehen, ergreifen die Unternehmen proaktive Maßnahmen, um sich vor einer Sicherheitsverletzung und dem Diebstahl sensibler Daten zu schützen. Tatsächlich konnten wir in einer kürzlich weltweit von Malwarebytes durchgeführten Studie feststellen, dass bei rund 200.000 Unternehmen eine Privatanwenderversion von Malwarebytes installiert war.

Das Bildungswesen gehörte zu den Branchen, in der BYOS am häufigsten auftrat, direkt gefolgt von den Branchen Software/Technologie und Unternehmensdienstleistungen.

# Schlussfolgerungen

2018 war ein weiteres erfolgreiches Jahr für Schadsoftware. Von fieberhaften, neuen Cryptomining-Angriffen, die praktisch täglich stattzufinden schienen, bis hin zu kühl kalkulierten Ransomware-Kampagnen ist das Pendel immer wieder mal in die eine oder die andere Richtung ausgeschlagen, um Markttrends zu folgen, sich an die Auswirkungen neuer Vorschriften anzupassen und sowohl Unternehmen als auch Privatanwender und ja, auch uns Sicherheitsforscher auf Trab zu halten.

Wenn wir einen Blick in die Zukunft werfen, kommen wir zu dem Schluss, dass sich auch 2019 dieses Katz-und-Maus-Spiel fortsetzen wird – mit alten Tricks, die für neue Bedrohungen verwendet werden, und mit neuen Taktiken für alte Favoriten. Und wie immer lautet unser Rat: Bleiben Sie informiert, bleiben Sie wachsam und nehmen Sie die Sicherheit Ihrer Daten oder Geräte niemals als gegeben hin.

Die Anwender werden sich zunehmend der Gefahren bewusst und die Bedrohungsakteure passen sich entsprechend an. Doch wenn wir dafür sorgen, dass ihre Ziele schwerer zugänglich sind, können wir uns, unsere Unternehmen und unsere Online-Communitys 2019 wesentlich besser schützen.

## Beitragende

*Adam Kujawa: Direktor Malwarebytes Labs*

*Wendy Zamora: Head of Content, Chefredakteur*

*Jovi Umawing: Senior Content Writer, Redakteur*

*Jerome Segura: Head of Threat Intelligence*

*William Tsing: Head of Threat Operations*

*Pieter Arntz: Senior Malware Analyst*

*Chris Boyd: Senior Malware Analyst*