2017 Jährlicher Sicherheits-Roundup:

Das Paradoxon der Cyberbedrohungen

HAFTUNGSAUSSCHLUSS

Die in diesem Dokument bereitgestellten Informationen sind lediglich allgemeiner Natur und für Aufklärungszwecke gedacht. Sie stellen keine Rechtsberatung dar und sind nicht als solche auszulegen. Die in diesem Dokument bereitgestellten Informationen finden womöglich nicht auf alle Sachverhalte Anwendung und spiegeln womöglich nicht die jüngsten Sachverhalte wider. Die Inhalte in diesem Dokument sind ohne eine Rechtsberatung auf der Grundlage der vorgestellten besonderen Fakten und Umstände nicht als verlässlich oder als Handlungsanweisungen zu verstehen und nicht in anderer Weise auszulegen. Trend Micro behält sich das Recht vor, die Inhalte dieses Dokuments zu jeder Zeit und ohne Vorankündigung zu ändern.

Übersetzungen in andere Sprachen sind ausschließlich als Unterstützung gedacht. Die Genauigkeit der Übersetzung wird weder garantiert noch stillschweigend zugesichert. Bei Fragen zur Genauigkeit einer Übersetzung lesen Sie bitte in der offiziellen Fassung des Dokuments in der Ursprungssprache nach. Diskrepanzen oder Abweichungen in der übersetzten Fassung sind nicht bindend und haben im Hinblick auf Compliance oder Durchsetzung keine Rechtswirkung.

Trend Micro bemüht sich in diesem Dokument im angemessenen Umfang um die Bereitstellung genauer und aktueller Informationen, übernimmt jedoch hinsichtlich Genauigkeit, Aktualität und Vollständigkeit keine Haftung und macht diesbezüglich keine Zusicherungen. Sie erklären Ihr Einverständnis, dass Sie dieses Dokument und seine Inhalte auf eigene Gefahr nutzen und sich darauf berufen. Trend Micro übernimmt keine Gewährleistung, weder ausdrücklich noch stillschweigend. Weder Trend Micro noch Dritte, die an der Konzeption, Erstellung oder Bereitstellung dieses Dokuments beteiligt waren, haften für Folgeschäden oder Verluste, insbesondere direkte, indirekte, besondere oder Nebenschäden, entgangenen Gewinn oder besondere Schäden, die sich aus dem Zugriff auf, der Verwendung oder Unmöglichkeit der Verwendung oder in Zusammenhang mit der Verwendung dieses Dokuments oder aus Fehlern und Auslassungen im Inhalt ergeben. Die Verwendung dieser Informationen stellt die Zustimmung zur Nutzung in der vorliegenden Form dar.

Für Raimund Genes (1963 – 2017)

Inhalt

5

Ransomware verursacht größere globale Ausbrüche trotz weniger großer Malware-Player

10

Anpassbare Bedrohungen missbrauchen auf neue Art bekannte Sicherheitslücken

13

Trotz steigender Wahrnehmung der Bedrohung nimmt BEC-Betrug zu

16

Der kometenhafte Aufstieg von Kryptowährung führt zu neuer Mining Malware und weiteren Bedrohungen

19

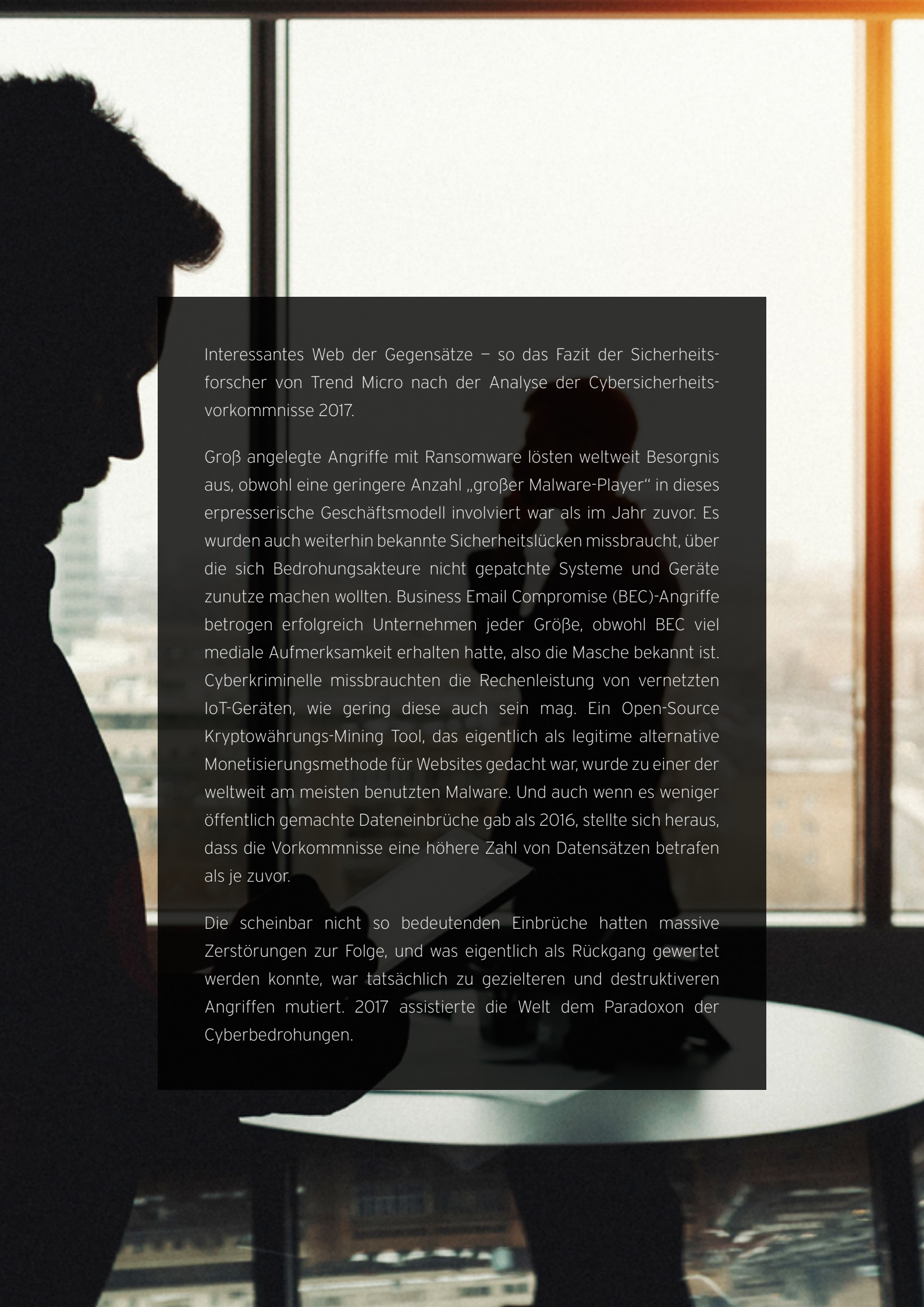
Cyberkriminelle missbrauchen begrenzte Rechnerleistung vernetzter IoT-Geräte

22

Weniger Veröffentlichungen von Datendiebstählen, dennoch mehr Unternehmensdatensätze bei Einbrüchen kompromittiert

25

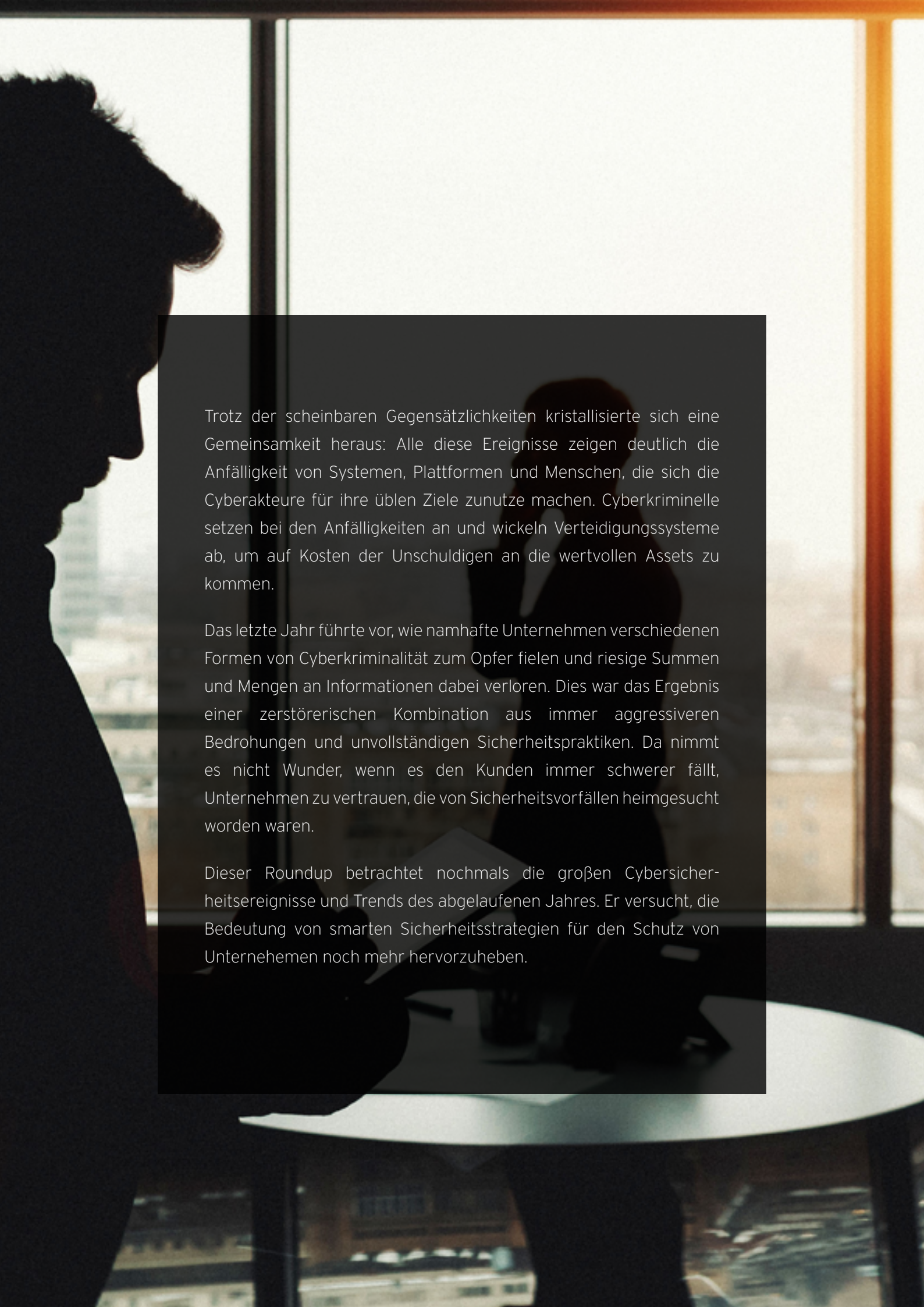
Bedrohungslandschaft: Review



Interessantes Web der Gegensätze – so das Fazit der Sicherheitsforscher von Trend Micro nach der Analyse der Cybersicherheitsvorkommnisse 2017.

Groß angelegte Angriffe mit Ransomware lösten weltweit Besorgnis aus, obwohl eine geringere Anzahl „großer Malware-Player" in dieses erpresserische Geschäftsmodell involviert war als im Jahr zuvor. Es wurden auch weiterhin bekannte Sicherheitslücken missbraucht, über die sich Bedrohungsakteure nicht gepatchte Systeme und Geräte zunutze machen wollten. Business Email Compromise (BEC)-Angriffe betrogen erfolgreich Unternehmen jeder Größe, obwohl BEC viel mediale Aufmerksamkeit erhalten hatte, also die Masche bekannt ist. Cyberkriminelle missbrauchten die Rechenleistung von vernetzten IoT-Geräten, wie gering diese auch sein mag. Ein Open-Source Kryptowährungs-Mining Tool, das eigentlich als legitime alternative Monetisierungsmethode für Websites gedacht war, wurde zu einer der weltweit am meisten benutzten Malware. Und auch wenn es weniger öffentlich gemachte Dateneinbrüche gab als 2016, stellte sich heraus, dass die Vorkommnisse eine höhere Zahl von Datensätzen betrafen als je zuvor.

Die scheinbar nicht so bedeutenden Einbrüche hatten massive Zerstörungen zur Folge, und was eigentlich als Rückgang gewertet werden konnte, war tatsächlich zu gezielteren und destruktiveren Angriffen mutiert. 2017 assistierte die Welt dem Paradoxon der Cyberbedrohungen.



Trotz der scheinbaren Gegensätzlichkeiten kristallisierte sich eine Gemeinsamkeit heraus: Alle diese Ereignisse zeigen deutlich die Anfälligkeit von Systemen, Plattformen und Menschen, die sich die Cyberakteure für ihre üblen Ziele zunutze machen. Cyberkriminelle setzen bei den Anfälligkeiten an und wickeln Verteidigungssysteme ab, um auf Kosten der Unschuldigen an die wertvollen Assets zu kommen.

Das letzte Jahr führte vor, wie namhafte Unternehmen verschiedenen Formen von Cyberkriminalität zum Opfer fielen und riesige Summen und Mengen an Informationen dabei verloren. Dies war das Ergebnis einer zerstörerischen Kombination aus immer aggressiveren Bedrohungen und unvollständigen Sicherheitspraktiken. Da nimmt es nicht Wunder, wenn es den Kunden immer schwerer fällt, Unternehmen zu vertrauen, die von Sicherheitsvorfällen heimgesucht worden waren.

Dieser Roundup betrachtet nochmals die großen Cybersicherheitsereignisse und Trends des abgelaufenen Jahres. Er versucht, die Bedeutung von smarten Sicherheitsstrategien für den Schutz von Unternehemen noch mehr hervorzuheben.

Ransomware wird von einer kleineren Zahl großer Malware-Player für größere weltweite Ausbrüche eingesetzt

Zum Ende des Jahres hin wurde offensichtlich, wie Ransomware die Spielregeln geändert hatte.

Wie bereits in den vergangenen Jahren machten Ransomware-Angriffe 2017 einen Großteil der Cybersicherheitsvorfälle aus. Große Ausbrüche mit weltweiten Infektionen beherrschten die Schlagzeilen und verdeutlichten, dass Ransomware immer noch eine belastende Bedrohung für Einzelne und Unternehmen darstellt.

In der ersten Hälfte 2017 berichtete Trend Micro, dass die Zunahme von Ransomware einen Spitzenwert erreicht habe[1], was unseren Voraussagen für das Jahr entsprach[2]. Doch bis zum Jahresende gab es dann eine 32 prozentige Steigerung in der Anzahl der Ransomware-Familien im Vergleich zu 2016. Trotzdem blieb die Anzahl der darin involvierten großen Malware-Player deutlich unter der des Vorjahres. Und diese kleinere Zahl führte zu einem bemerkenswerten Schwenk: ein paar dieser großen Ransomware Player waren für breite, komplexe Bedrohungen verantwortlich, wie die besonders zerstörerischen Angriffe mit WannaCry und Petya bewiesen. Der Schaden für die Opfer weltweit betrug geschätzte 5 Milliarden $.[3]

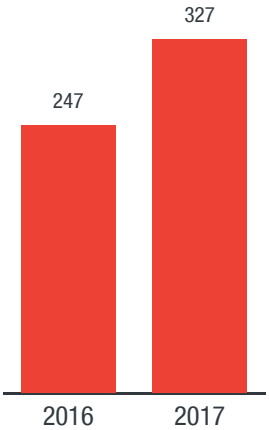


Bild 1. 2017 gab es mehr Ransomware Familien.
Vergleich der gesamten Zahl der neuen Ransomware Familien

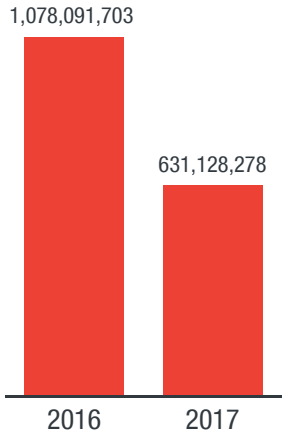


Bild 2. Weniger Big Player trotz der Steigerung bei neuen Ransomware Familien: Vergleich zwischen der Gesamtzahl der entdeckten Ransomware-bezogenen Bedrohungen

Ransomware	Grand Total
LOCKY	82,805
KOVTER	50,390
NEMUCOD	46,276
CERBER	40,788
CRYPTESLA	26,172
CRYPWALL	9,875
CRYPCTB	4,773
CRYSIS	3,493
RANSOM	3,210
WALTRIX	2,998

Ransomware	Grand Total
WANNACRY/WCRY	321,807
CERBER	40,493
LOCKY	29,436
CRYSIS	10,573
SPORA	8,044
CANTIX	6,269
EXMAS	5,810
CRYPTESLA	4,608
CRYPTLOCK	3,007
ZERBER	2,691

Bild 3. Vorherrschende Ransomware-Familien: Top Ransomware-Familien, die von 2016 an tätig waren

Eine Variante von WannaCry, von Trend Micro als RANSOM_WANA.A und RANSOM_WCRY.I erkannt, stellte 2017 eine der größten Ransomware-Bedrohungen dar und hatte sowohl für Einzelne als auch Unternehmen verheerende Folgen. Sie enthielt eine sich selbst verbreitende Komponente und ermöglichte Mitte Mai einen der weltweit ersten Wurm-basierten Ransomware-Angriffe[4]. Die Variante nutzte den EternalBlue-Exploit, um eine Schwachstelle zu missbrauchen, die bereits im März gepatcht worden war[5]. WannaCry infizierte in nur wenigen Tagen 300.000 Computer in 150 Ländern, verschlüsselte Dateien und forderte ein Lösegeld für deren Entschlüsselung[6].

Die Gesamtzahl der WannaCry-Entdeckungen überstieg die von Cerber und Locky, zwei der größten Ransomware Player, was ihre Langlebigkeit anbelangt, und war sogar höher als der Rest der Ransomware-Familien zusammen. WannaCry dominierte 2017 mit 57% der Ransomware-Erkennungen, während die anderen Ransomware-Familien, Cerber und Locky nur 31%, beziehungsweise 7% und 5% ausmachten.

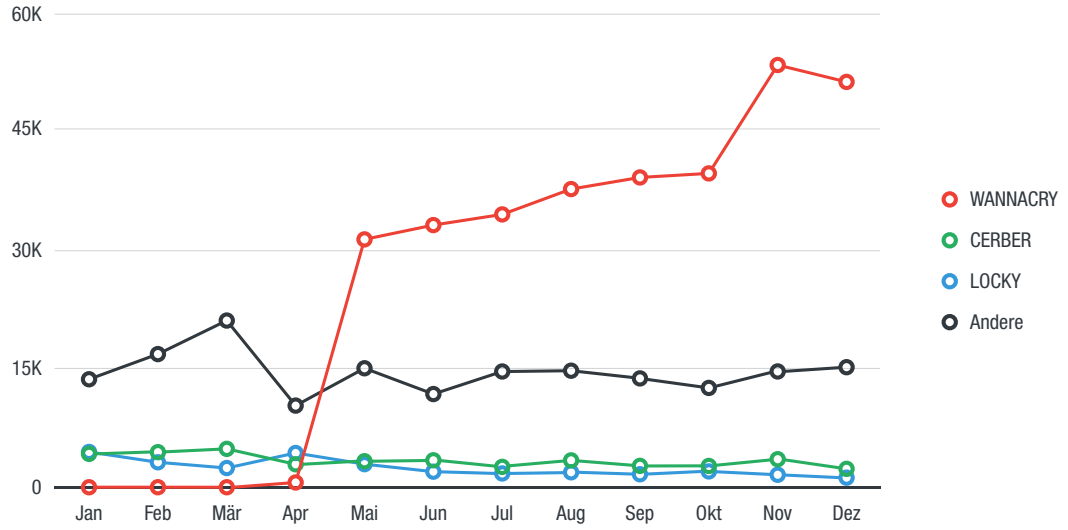


Bild 4. Der Aufstieg von WannaCry 2017: WannaCry-Erkennung auf der Basis der Daten aus dem Trend Micro™ Smart Protection Network™

Die weite Verbreitung dieser Ransomware wurde auch dadurch angeschoben, dass sie im Untergrundmarkt zu einem erstaunlich niedrigen Preis verkauft worden ist. Die Forscher stellten fest, dass Upgrade-fähige Varianten von WannaCry im Middle Eastern and North African (MENA)-Untergrund bereits für 50$ zu haben waren, und zwar nur zwei Tage nach dem ersten Ausbruch der Ransomware[7]. Infolge dieses einfachen Zugangs zu bezahlbarer Ransomware war eine Steigerung der Angriffe zu erwarten, vor allem da Malware-as-a-Service (MaaS) zu den beliebtesten Angeboten im MENA-Untergrund gehört[8]. Dazu muss man wissen, dass günstige Ransomware eine Eigenart dieser Kreisen darstellt, weil es dort eine einzigartige Kamaraderie zwischen den Bedrohungsakteuren gibt.

Auch Petya ist der Bedrohungsszene nicht fremd. Eine neue Variante der Ransomware, von Trend Micro als RANSOM_PETYA.SMA erkannt, schlug 2017 hohe Wellen dank der Fähigkeit, Systemfestplatten zu modifizieren oder ganz zu löschen, um dann den berüchtigten „Blue Screen“ mit der Nachricht anzuzeigen[9].

Die Ransomware wurde zuerst in der Ukraine entdeckt, verbreitete sich jedoch schnell in anderen Ländern und traf einige Regierungsabteilungen, Kommunaleinrichtungen und auch Unternehmungen[10]. Mitte 2017 hatte Petya mehr als 12.500 Maschinen in 65 Ländern infiziert[11].

Im Oktober traf ein neuer Ransomware-Angriff osteuropäische Länder. Bad Rabbit, mit gewisser Ähnlichkeit zu Petya, nutzte als Verbreitungsmethode Fake Adobe Flash Update Installer von kompromittierten

Websites[12]. Sie verbreitete sich über infizierte Netzwerke hinweg, indem sie Kopien ihrer selbst ablegte und ausführte via Windows Management Instrumentation (WMI) und Service Control Manager Remote Protocol[13]. Des Weiteren nutzt die Schadsoftware zur Verbreitung auch das Windows Server Message Block (SMB) File Sharing Protocol und versucht über Brute-Force, auf administrative Freigaben zuzugreifen und eine Kopie der bösartigen Datei dort abzulegen. Bei Misserfolg nutzt sie EternalRomance, um eine SMB-Sicherheitslücke auszunutzen, die schon Monate vor dem Angriff gepatcht worden war[14].

Im Juni hatte eine neue Variante von Erebus den südkoreanischen Hoster Nayana getroffen, und die Angreifer verlangten für die Entschlüsselungsdatei 550 Bitcoins (1.62 Mio. $ damals). Von Trend Micro als RANSOM_ELFEREBUS.A erkannt, infizierte die Ransomware 153 Linux-Server, und der Angriff betraf 3.400 Geschäfts-Websites, die vom Unternehmen gehostet wurden[15].

Auch das Auftauchen einer neuen Variante von Erebus, die Linux-Systeme anvisiert, bestätigte die Vorhersagen von Trend Micro bezüglich der Diversifizierung der Angriffsmethoden[16]. Tatsächlich gab es ältere Arten von Ransomware, die nun mit neuen Techniken ausgerüstet schnell zu größeren, zerstörerischeren Bedrohungen wurden.

Cerber, von Trend Micro als RANSOM_CERBER-Familie erkannt, erwies sich als eine der sich am schnellsten entwickelnden Bedrohungen des Jahres und durchlief eine Reihe von verschiedenen Versionen mit Variationen seiner Routinen[17]. Im März wurde Cerber mit einem neuen Loader ausgestattet, der offenbar darauf ausgerichtet war, Entdeckung durch Pre-Execution Machine Learning-Lösungen zu vermeiden[18]. Im August dann wurde eine Cerber-Variante gefunden (RANSOM_HPCERBER.SMALY5A), die Wallet-Dateien aus Kryptowährungs-Anwendungen sowie gespeicherte Passwörter aus Webbrowsern wie Google Chrome, Internet Explorer und Mozilla Firefox stahl[19]. All diese Taktiken führten dazu, dass Cerber als die am besten funktionierende Ransomware in 2017 gewertet wurde[20].

Locky, von Trend Micro als RANSOM_LOCKY-Familie erkannt, schaffte es ebenfalls, sich mit neuen Kampagnen weiterzuentwickeln. Die Vielfalt der Verbreitungsmethoden von Locky wurden um Fake Voicemail-Benachrichtigungen und bösartige Dateien oder Links erweitert[21], betrügerische Rechnungsmails, die mit Ransomware infizierte HTML-Anhänge umfassten[22], und um verstecktere Taktiken, wie das Anwenden von technischen Änderungen in ihren Angriffsmethoden über verschlüsselte Dynamic Link Libraries (DLLs)[23]. Eine weitere Kampagne umfasste die Verteilung von Locky zusammen mit einer anderen Ransomware namens FakeGlobe, die Nutzer in mehr als 70 Ländern ins Visier nahm[24]. Im Rahmen einer der bislang größten Ransomware-Kampagnen wurde eine neue Locky-Variante in nur 24 Stunden mit 23 Mio. Mails verteilt[25].

Das letzte Jahr führte auch vor, wie sich Bedrohungen diversifizieren, um verschiedene Angriffsroutinen anzuwenden, so etwa mit dateilosen Eigenschaften. Sorebrect, von Trend Micro als RANSOM_SOREBRECT.A und RANSOM_SOREBRECT.B erkannt, ist ein Beispiel dafür, nämlich eine dateilose Ransomware, die bösartigen Code in einen legitimen Systemprozess einschleust, um Dateien zu verschlüsseln. Diese

versteckte Bedrohung geht so weit, Event-Logs und andere Dateien zu löschen, um ihre Spuren zu verwischen. Die Bedrohung betraf seit Mai verschiedene Branchen, einschließlich Fertigung, Technologie und Telekommunikation in mindestens neun Ländern[26].

Jahr für Jahr orientierten sich Ransomware-bezogene Bedrohungen weiter in Richtung Mail-Format. Dies überrascht nicht, denn Spam war bei Kriminellen lange Zeit der beliebteste Verbreitungsmechanismus.

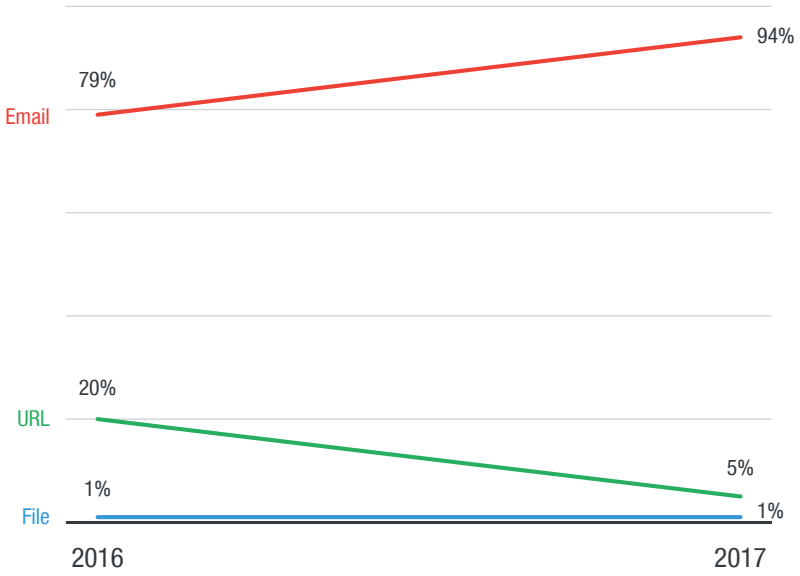


Bild 5. Email regiert auch weiter bei Ransomware:
Vergleich der Ransomware-bezogenen Bedrohungen 2016 und 2017

Solche Wandel in der Ransomware-Szene zeigen deutlich, wie Cyberkriminelle schnell ihre Richtung ändern, Bedrohungen mit neuen Taktiken, Techniken und Prozeduren erstellen, um größeren Erfolg zu haben. Daher ist es wichtig, verlässliche Sicherheitslösungen zu haben, die mit einem mehrschichtigen Ansatz vor diesen sich ändernden Bedrohungen schützen können.

Anpassbare Bedrohungen missbrauchen auf neue Weise bekannte Sicherheitslücken

Im April ermöglichte die Shadow Brokers Hacker-Gruppe, die 2016 einen Daten-Dump fabriziert hatte, wieder die Ausnutzung von schweren Sicherheitslücken in Systemen, Netzwerken und Firewalls, indem sie ein weiteres Leak anboten, das Hacking-Tools von der National Security Agency (NSA) umfasste. Einige der Exploits aus diesem Leak, einschließlich EternalBlue und EternalRomance, wurden in großen Kampagnen des letzten Jahres eingesetzt, vor allem in den WannaCry-, Petya- und Bad Rabbit-Angriffen.

Später im Jahr wurde eine bekannte Sicherheitslücke für einen Angriff missbraucht, der eine riesige Mobilnutzerbasis traf. Dirty COW (CVE-2016-5195), eine Privilege-Escalation-Lücke, die Angreifern die Möglichkeit des Root-Zugangs auf den Zielsystemen eröffnet, wurde im Oktober 2016 bekannt [27], und man fand sie im Dezember auf Upstream Linux-Plattformen wie Redhat und auch auf Android (setzt auf einen Linux-Kernel)[28]. 2017 entdeckten die Sicherheitsforscher von Trend Micro die erste Malware, die die Lücke in Android ausnutzte: ZNIU (ANDROIDOS_ZNIU). Zur Zeit seiner Entdeckung hatte der Schädling mindestens 5.000 Nutzer in mehr als 40 Ländern angegriffen, und zwar versteckt in mehr als 1.200 bösartigen Apps[29].
Das bedeutet jedoch keinesfalls, dass ältere Schwachstellen aus dem Fokus geraten waren. Im Gegenteil, im letzten Jahr wurden etwa 200.000 ungepatchte Systeme als anfällig auf die Heartbleed-Lücke (seit 2014 bekannt) gemeldet[30].
Auch Downad (DOWNAD-Familie), ebenfalls als Conficker bekannt, seit 2008 in den Schlagzeilen, war sehr präsent und gehörte zu den Top-Detections des letzten Jahres. Wie schon 2016 wies der Wurm, eine Variante dessen die neun Jahre alte CVE-2008-4250-Sicherheitslücke ausnutzt, 2017 mindestens 20.000 Detections auf[31].

Mit Hilfe von mehr als 3.000 unabhängigen Forschern, die beim Programm der Zero Day Initiative (ZDI) mitmachen, entdeckte und veröffentlichte Trend Micro 2017 1.008 neue Schwachstellen. Dabei lässt sich ein Anstieg an Sicherheitslücken für Adobe-, Google- und Foxit-Produkte feststellen, und ein Rückgang bei solchen für Apple und Microsoft. Doch unabhängig von den Zahlen bleibt die Tatsache bestehen, dass permanent neue Sicherheitslücken entdeckt werden und ein Sicherheitsrisiko für Büros und ähnliche Umgebungen sowie IoT-Geräte und Systeme darstellen.

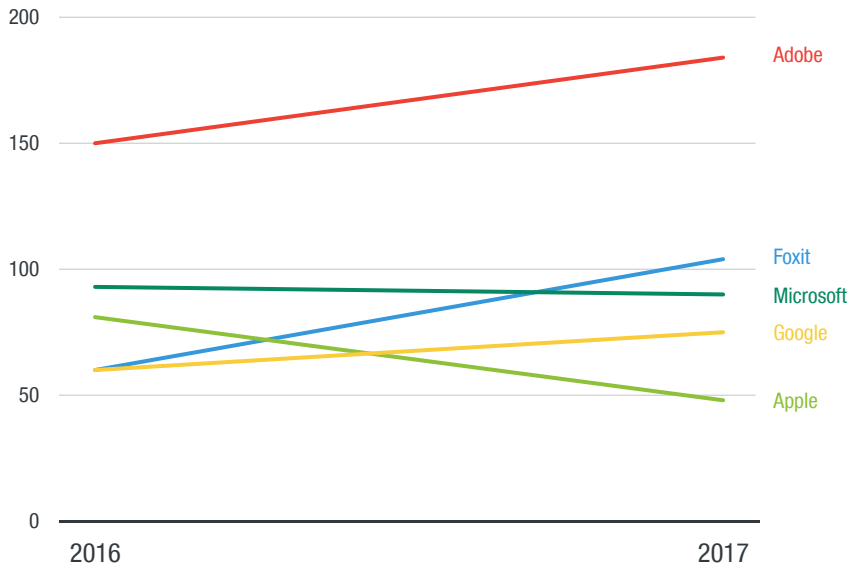


Bild 6. Vergleich der Anzahl der gefundenen Schwachstellen nach Hersteller 2016 und 2017

Mit Hilfe der mit dem ZDI zusammen arbeitenden Forschern fand Trend Micro auch heraus, dass die Zahl der Sicherheitslücken für Supervisory Control and Data Acquisition (SCADA)-Systeme von 177 2016 auf 144 im letzten Jahr gefallen ist — ein 19-prozentiger Rückgang. Doch gab es 2017 einen steilen Anstieg bei Zero-Day-Lücken. Sie stiegen um 98 Prozent im Vergleich zu 2016, und bis auf sechs waren alle SCADA-bezogen. Zero-Day-Lücken mit Bezug zu SCADA schnellten von 46 2016 auf 113, ein Sprung von 146 Prozent.

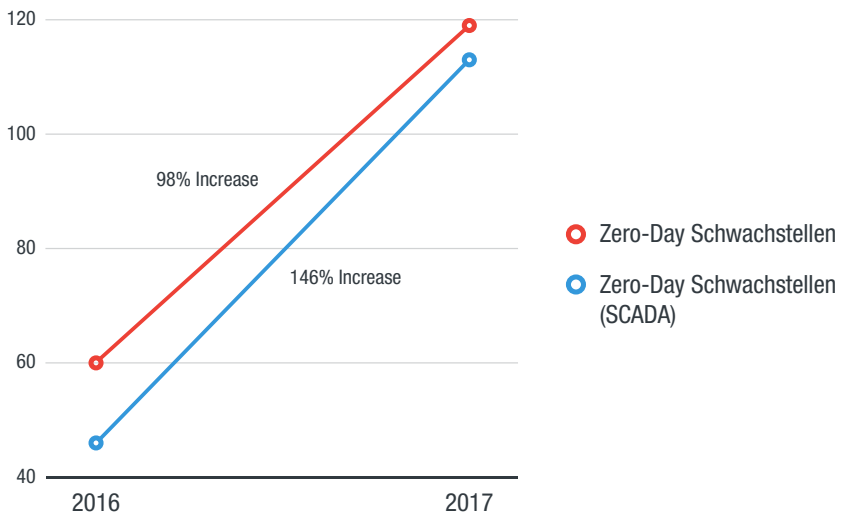


Bild 7. Ein markanter Anstieg bei Zero-Day-Lücken: Vergleich der Anzahl von Zero-Day-Schwachstellen und SCADA-bezogener Zero-Day-Lücken 2016 und 2017

Das letzte Jahr hat auch vorgeführt, wie Bedrohungsakteure ständig auf der Suche nach Schwächen in Systemen und Geräten sind, denn diese dienen als Gateways für möglicherweise lukrative Einbrüche. Cyberkriminelle suchen aktiv nach Fehlern, um diese auszunutzen und Zugriff auf Systeme und dort auch höhere Privilegien zu erlangen, aber auch um Denial-of-Service-Angriffe zu fahren. Vor allem Unternehmen, die nicht aktualisierte und nicht mehr unterstützte Betriebssysteme oder Anwendungen einsetzen, also auch keine Schwachstellen-Patches und Updates dafür erhalten, sind einfache Ziele für die Bedrohungsakteure.

In dieser Situation können Unternehmen aus starken Sicherheitslösungen Vorteile ziehen. Mit proaktivem virtuellem Patching sind kritische Systeme, vor allem auch Legacy, geschützt. Ein mehrschichtiger Ansatz ist am besten geeignet, um die Auswirkungen von Bedrohungen durch die steigende Zahl von Schwachstellen-Exploits zu minimieren.

Trotz besserer Wahrnehmung der Bedrohung hat BEC-Betrug weiterhin Konjunktur

Business Email Compromise (BEC) ist seit einiger Zeit öffentlich sehr präsent. Trotzdem gelingt es Cyberkriminellen immer noch, Riesensummen von nichtsahnenden Mitarbeitern und Führungskräften abzuziehen. 2017 erwies sich als ein weiteres betriebsames Jahr für Betrüger, die diese Masche nutzen. Trend Micros Daten zeigen, dass allein 2017 vom ersten zum zweiten Halbjahr BEC-Betrug um ganze 106 Prozent zunahm. Trend Micro lag richtig mit der Vorhersage, dass BEC aufgrund seiner relativen Einfachheit 2017 an Beliebtheit bei Cyberkriminellen zulegen werde[32]. BEC-Vorfälle kosten Unternehmen Milliarden Dollar, ein riesiger Sprung vom Jahr zuvor. BEC-Betrügereien waren so effizient, dass sie vom Federal Bureau of Investigation (FBI) als „5 Milliarden Dollar Scam" bezeichnet wurden. Das FBI berichtete im Mai, dass die weltweiten Verluste durch BEC seit 2013 5,3 Milliarden Dollar erreicht hatten[33] – das sind 2.3 Milliarden mehr als die kumulativen Verluste, die das FBI im Juni 2016 veröffentlicht hatte[34].

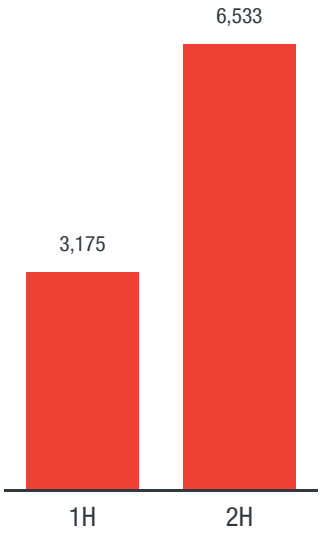


Bild 8. BEC-Versuche stiegen um mehr als das Doppelte in der Zeitspanne vom 1. Zum 2. Halbjahr: Vergleich der BEC-Angriffe zwischen H1 und H2 2017

Die Gefahr durch BEC blieb bestehen, obwohl diese Bedrohung sehr viel Medienaufmerksamkeit erhalten hatte. Im April zeigte ein brisanter Fall, dass auch Tech-Unternehmen diesen Social Engineering-Taktiken zum Opfer fallen können, einschließlich Google und Facebook. Es wurde berichtet, dass die beiden Riesen um mehr als 100 Millionen Dollar betrogen worden waren, und zwar durch einen Mann, der mutmaßlich falsche Rechnungen nutzte und beide Unternehmen davon überzeugen konnte, dass er zu einem Partner-Herstellerunternehmen gehöre. Zum Glück für die Opfer konnten die Verluste gleich nach dem Vorfall zurückerlangt werden[35].

Im Juli warnte das BSI in Deutschland 5.000 potenzielle Ziele und auch die allgemeine Öffentlichkeit vor einem BEC-Betrug, dem bereits Firmen über betrügerische Memos zum Opfer gefallen waren, wobei sich der Schaden auf Millionen Euros belief[36]. Im Oktober zeigte sich, dass auch Immobilien ein lohnendes Geschäft für BEC sein können. Betrügern gelang es Käufer um deren Anzahlungen zu bringen[37].

Einen Monat später tauchten Berichte zu einem Mail-basierten Betrug auf, im Rahmen dessen Kunstgalerien in Großbritannien und den USA mit manipulierten Rechnungen um Tausende Pfund betrogen wurden[38]. Und im Dezember verlor eine asiatische Transportfirma 3,4 Millionen Dollar durch einen BEC-Betrug. Die Firma versäumte es, Fake Zahlungsforderungen für Fahrzeugleasing und andere Dienstleistungen zu prüfen und kam den betrügerischen Forderungen nach[39].

Trend Micro berichtete im ersten Halbjahr, dass die am meisten vorgetäuschte Position der Chief Executive Officer (CEO) war, während der Chief Financial Officer (CFO) am häufigsten anvisiert wurde. Dies setzte sich auch in H2 fort.

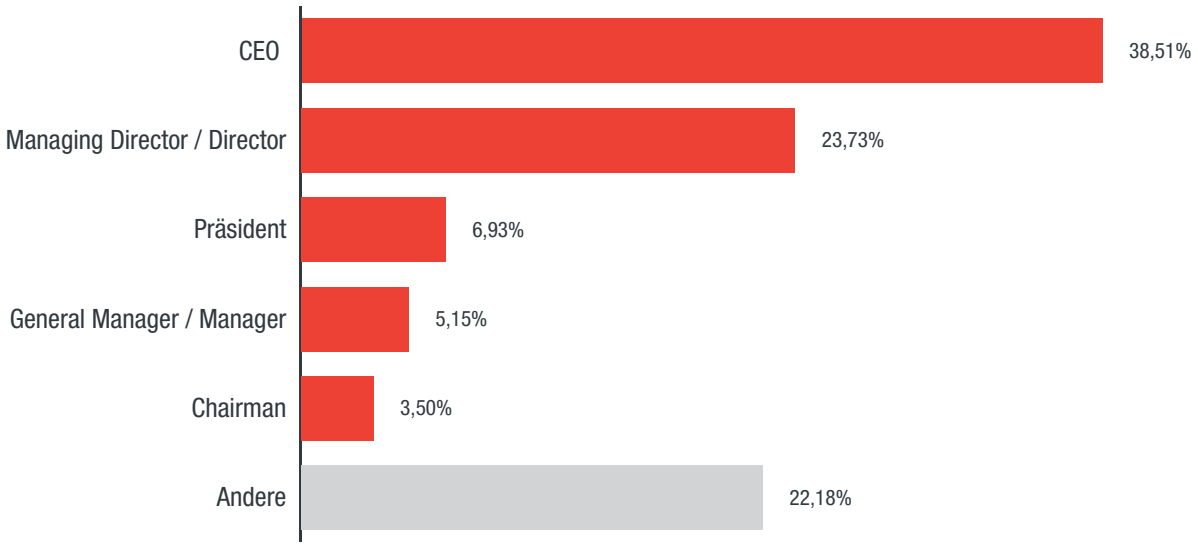


Bild 9. CEO wurde von Cyberkriminellen am häufigsten vorgetäuscht:
Anteil der versuchten BEC-Angriffe, bei denen eine spezielle Position vorgetäuscht wurde

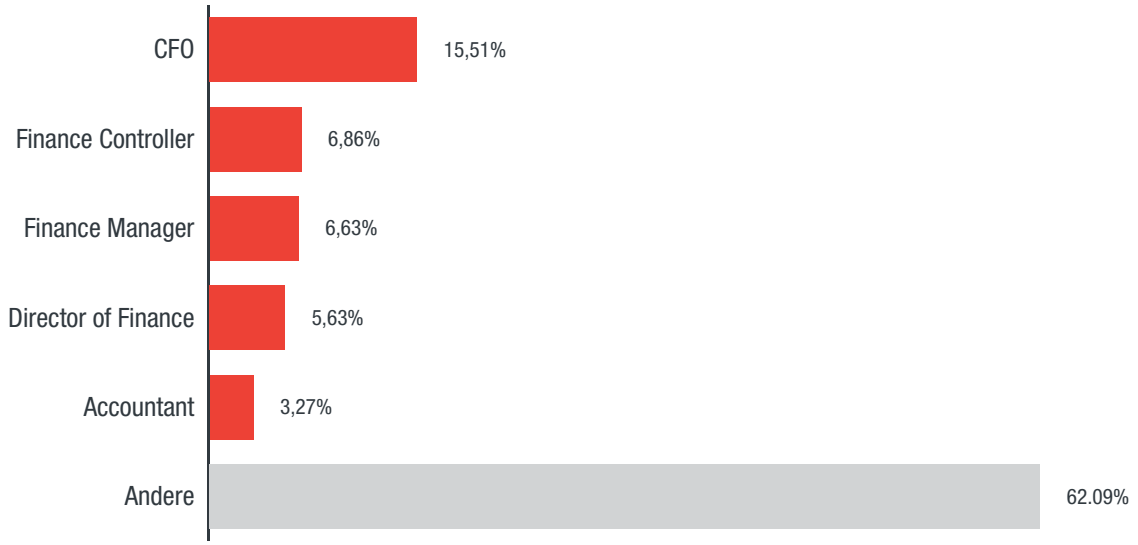


Bild 10. CFO bleibt die am meisten anvisierte Position: Anteil der versuchten BEC-Angriffe, bei denen eine spezielle Position anvisiert wurde

Angesichts der Tatsache, dass Bedrohungsakteure ihre Taktiken verfeinern, müssen Unternehmen ebenfalls ihre Cybersicherheit stärken. Dazu gehört auch die Schulung der Mitarbeiter auf allen Ebenen, einschließlich der Führungskräfte, damit diese BEC-Betrug erkennen lernen. Ebenso wichtig ist auch der Einsatz von Sicherheitslösungen, die vor Spam und Spear-Phishing-Versuchen schützen können. Es empfiehlt sich darüber hinaus, ein Multifaktor-Verifizierungssystem für finanzielle Anfragen zu implementieren, sodass Betrug erkannt werden kann, bevor eine Finanztransaktion angestoßen wird.

Der kometenhafte Aufstieg von Kryptowährung führt zu neuer Mining Malware und weiteren Bedrohungen

Die Beliebtheit der Kryptowährung hat das Interesse nicht nur einer breiten Nutzerbasis geweckt, sondern auch der Cyberkriminellen, sodass die Bedrohungen ebenfalls im Steigen sind. Den Erfolg der Kryptowährung belegt auch der Höhenflug des Bitcoin, der vor Jahresende 19.783,21$ wert war[40]. Immer mehr Einzelne, Organisationen[41, 42, 43] und auch Regierungen[44, 45] begannen, bestimmte Währungen als legale Zahlmethode zu akzeptieren. Dieser schnelle Aufstieg hat Cyberkriminelle dazu animiert, auch auf den Wagen aufzuspringen und davon zu profitieren. In einigen Fällen führen sie Raubüberfälle auf Kryptowährungs-Exchanges oder Online-Plattformen durch, wo Kryptowährungen gehandelt werden, — so geschehen im Fall von Youbit in Südkorea. Die Plattform musste schließen, nachdem sie zweimal in acht Monaten gehackt worden war[46]. In anderen Fällen wollen sie mit den Mitteln der infizierten Maschinen Kryptowährungen minen.

Bild 11. Verschiedene Angriffsmethoden: Wie Angreifer 2017 Kryptowährungen ins Visier nahmen

Im letzten Jahr zielten die Angreifer auf Mobilgeräte über Google Play-Apps mit bösartigen Kryptowährungs-Mining Fähigkeiten. Um der Erkennung zu entgehen, nutzen diese Kryptowährungs-Mining Apps (ANDROIDOS_JSMINER und ANDROIDOS_CPUMINER) das Laden von JavaScript und Einfügen von nativem Code[47].

Kryptowährungs-Malware verschonte auch die sozialen Medien nicht. Im Dezember fanden die Sicherheitsforscher von Trend Micro einen neuen Kryptowährungs-Mining Bot namens Digmine, der sich über den Facebook Messenger verbreitete. Als Videodatei getarnt, bleibt der Monero-Mining Bot so lang wie möglich auf einer Maschine des Opfers, um den größtmöglichen Betrag an Kryptowährung zu schürfen[48].

Varianten von Malware, die bereits für andere Formen der Cyberkriminalität eingesetzt worden waren, tauchten nun auch für das Schürfen von Kryptowährungen auf. Retadup, vorher bereits in israelischen Krankenhäusern angetroffen, nutzte nun die Leistung der infizierten Maschinen zum Schürfen[49].

Man darf aber nicht vergessen, dass das Mining von Kryptowährung per se nicht illegal ist. Coinhive, beispielsweise ist eine Open-Source-Plattform, die es Unternehmen erlaubt, über ihre Websites Monero-Kryptowährung zu verdienen. Doch Bedrohungsakteure haben schon bald die Programmierung der Plattform zu ihrem Nutzen missbraucht.

Im November stand eine solche bösartige Variante des Coinhive Miners an sechster Stelle der am häufigsten angetroffenen Malware der Welt[50]. Ebenfalls im letzten Jahr entdeckten die Forscher von Trend Micro, dass die ElTest-Kampagne Betrug über Tech Support nutzte, um Coinhives Kryptowährungs-Miner zu verbreiten[51].

Der Aufstieg von Kryptowährungs-Mining zeigt sich auch in den Daten von Trend Micro, die 2017 einen signifikanten Anstieg bei Mining-Erkennungen aufweisen, vor allem im letzten Quartal. In dieser Zeitspanne waren es sogar mehr als die Detections von WannaCry Ransomware.

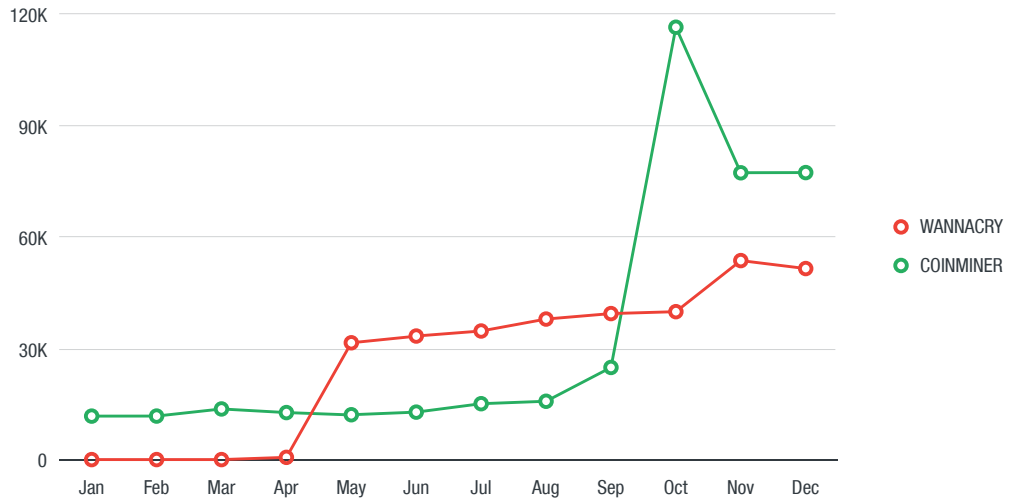


Bild 12. Anstieg der Mining-Erkennungen: Vergleich der monatilichen Erkennungen von Mining Tools und WannaCry Ransomware 2017; Basis sind Daten aus dem Trend Micro Smart Protection Network

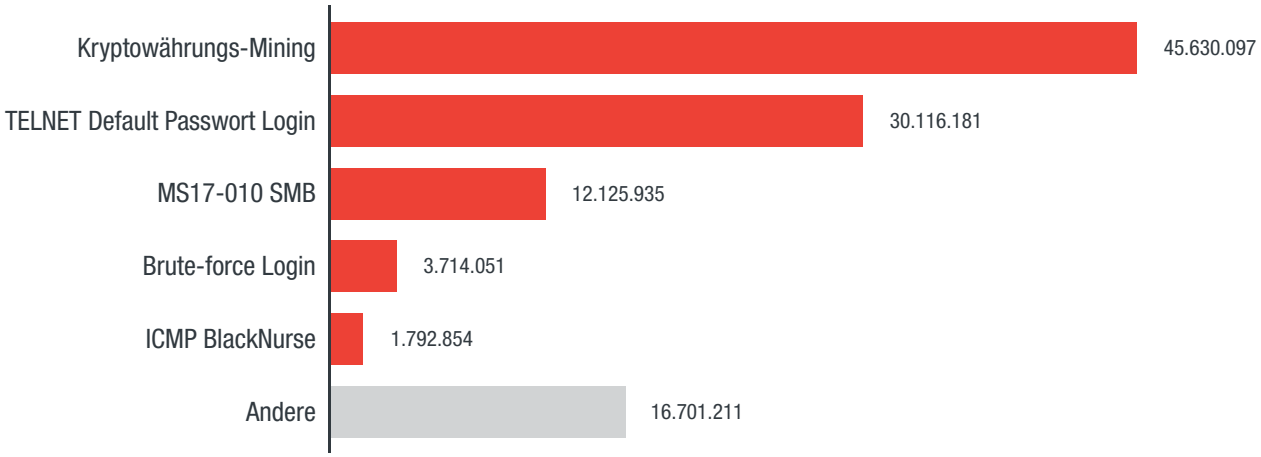
Immer mehr Länder und Geschäfte öffnen sich der Kryptowährung als virtuelles legales Zahlungsmittel. Deshalb ist es wichtig, sich vor den Bedrohungen, die damit einhergehen können, abzusichern. Dies erfordert den Einsatz von Sicherheitslösungen, die traditionellen Schutz mit neueren, fortschrittlichen Ansätzen kombinieren. Eine All-in-One-Lösung, die effizient Machine Learning-Technologie, Verhaltensmonitoring, Applikationskontrolle, Web- und mobile Sicherheit, sowie Mailschutzt verbindet, kann die mit Kryptowährung einhergehenden Bedrohungen abwehren.

Cyberkriminelle missbrauchen eingeschränkte Rechenleistung von vernetzten IoT-Geräten

Mit 20,3 Milliarden vernetzten Geräten allein 2017[52] lässt sich sicherlich feststellen, dass das Internet of Things (IoT) kein hohles Schlagwort ist. Die Möglichkeiten für operationale Effizienz und Produktivität für Einzelne und Unternehmen sind schier endlos. Das ist auch der Grund, warum Bedrohungsakteure so schnell Wege gefunden haben, diese Interkonnektivität der Geräte auszunutzen.

Der Angriff des Mirai-Botnets ist ein Beispiel dafür, wie vernetzte Geräte für bösartige Zwecke korrumpiert werden können. 2016 gelang es dem Botnet, nicht gesicherte vernetzte Geräte zu infizieren und sie dazu zu nutzen, via massiver Distributed Denial-of-Service (DDoS)-Angriffe große Websites zum Absturz zu bringen, so etwa Twitter und Netflix)[53]. Varianten von Mirai tauchten kurz danach auf, einschließlich einer, die 900.000 Heimrouter der Deutsche Telekom angriff[54]. Innerhalb weniger Stunden am 29. November des letzten Jahres führte eine neue Mirai-Kampagne, die in Südamerika und Nordafrika entdeckt wurde, 371.640 Angriffsversuche durch, die von etwa 9.000 einzigartigen IP-Adressen kamen[55].

Die Daten aus dem Trend Micro™ Smart Home Network für Netzwerkvorfälle 2017 zeigen interessanterweise, dass der Trend für IoT eine andere Route eingeschlagen hat. Statt sich auf DDoS-Angriffe zu konzentrieren, betrachten Cyberkriminelle nun IoT-Geräte als Mittel für Kryptowährungs-Mining.



Achtung: Die Kryptowährungs-Miningaktivitäten und WannaCry-bezogenen Vorfälle wurden vor allem auf Desktops und Laptops entdeckt. Die anderen Events waren Versuche, IoT-Geräte für Botnets zu sammeln — Cyberkriminelle versuchten Default-Passwörter zu nutzen für einen Zugriff auf Geräte oder wendeten Brute Force dafür an.

Bild 13. Kryptowährungs-Mining und TELNET-Events überholten andere: Netzwerkvorfälle 2017
Basierend auf Daten aus dem Trend Micro™ Smart Home Network

Die Rechenleistung von kleinen IoT-Geräten ist begrenzt und damit auch die Wahrscheinlichkeit, dass einzelne Geräte eine substanzielle Summe an Kryptowährung produzieren kann. Um ihren Return on Investment zu maximieren, übernehmen Cyberkriminelle eine größere Zahl dieser Geräte für das Schürfen von Kryptowährung. Dieser Prozess umfasst Rechenaufgaben, die viel Systemressourcen erfordern und die von Geräten wie Smartphones, IP-Kameras und smart TVs übersteigt.

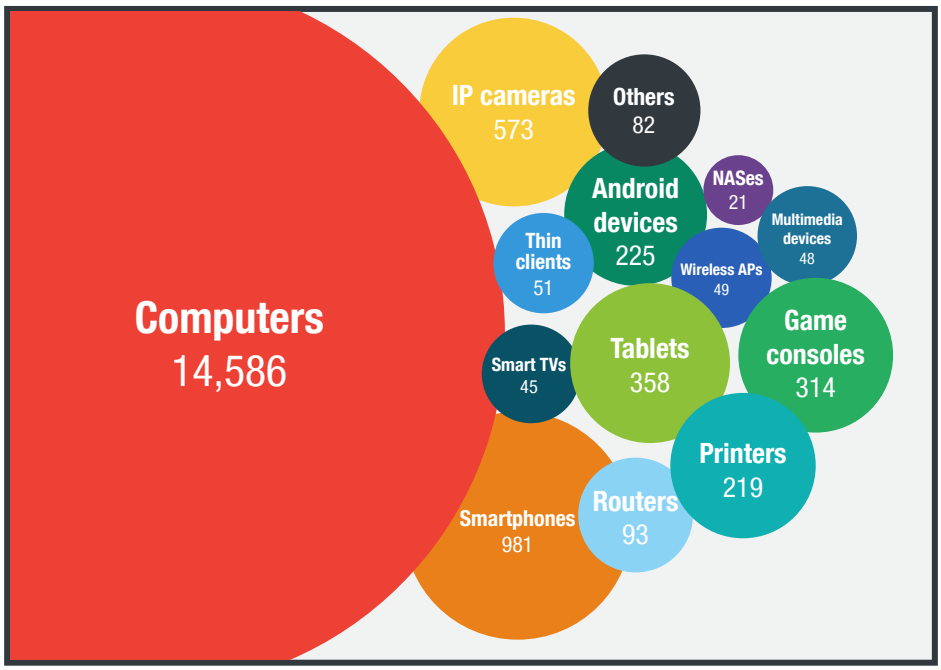


Bild 14. Computer drängen andere Kryptowährungs-Mininggeräte in den Hintergrund:
Geräte, auf denen 2017 Kryptowährungs-Mining entdeckt wurde

Bemerkenswert ist auch die Tatsache, dass die Login-bezogenen Vorfälle bei TELNET bei weitem mehr Daten betrafen als die bezüglich der SMB-Sicherheitslücke, die die WannaCry Ransomware missbraucht hatte. Obwohl die WannaCry-Ransomware weltweit Wirbel verursachte, waren von den IoT Botnet-bezogenen Vorfällen mehr Geräte betroffen – eine Tatsache, die Unternehmen genau überdenken sollten.

Um die Bedeutung von ‚Security-by-Design' weiter zu betonen, führten die Forscher IoT-Fallberichte zu Sicherheitslücken in mit dem Internet verbundenen Lautsprechern an[56] sowie einen heimlichen herstellerneutralen Fahrzeug-Hack, derzeit von moderner Fahrzeug-Sicherheitstechnik nicht abzuwehren[57]. Diese Berichte, in die auch große Unternehmen involviert waren, betonen die Anfälligkeit vernetzter Geräte für Angriffe und liefern wichtige Sicherheitseinsichten für Hersteller aller Arten von IoT-Geräten.

Mit der technologischen Weiterentwicklung gehen auch mehr Angriffe einher, die Schwachstellen von vernetzten Geräten, wie etwa intelligente Transportsysteme (ITS), ausnutzen. Mit ITS betreten die Hersteller Neuland, was die Bequemlichkeit und Zeit-, Ressourcen- sowie Kostenersparnisse anbelangt. Der innovative Einsatz der mit dem Internet verbundenen ITS wird das Pendeln und schließlich die Lebensqualität verbessern. In naher Zukunft werden vernetzte Fahrzeuge neben selbstfahrenden Autos auf so genannten „smarten Straßen" fahren, und Cyberkriminelle werden alles daran setzen, um diese Systeme, die von dieser progressiven Unternehmung abhängig sind, zu einem plötzlichen Halt zu bringen.

Im letzten Jahr berichteten die Trend Micro-Sicherheitsforscher über die möglichen physischen, drahtlosen und netzwerkbezogenen Angriffe auf ITS[58]. Die Methoden für ITS-Angriffe kommen aus scheinbar trivialen Quellen — etwa Verkehrsüberwachungskameras, Zahlautomaten und sogar Sensoren für die Messung von Abgasen oder Luftqualität[59] — und die Angriffe können nicht nur wirtschaftlichen Schaden bei ITS-Anbieter und Telekommunikationsunternehmen anrichten, sondern auch bei vielen Unternehmen, die sich auf die betroffenen Dienstleistungen verlassen.

Angesichts der bereits stattgefundenen und auch künftiger IoT-Angriffe müssen sich Unternehmen vor Geschäftsunterbrechungen durch Maschinen und kritische Abläufe schützen Neben Best Practices sollten Lösungen Endpunkte schützen und genaues Monitoring des Internetverkehrs liefern, um gezielte Angriffe und fortgeschrittene Bedrohungen rechtzeitig zu erkennen.

Mehr Unternehmensdatensätze werden bei Dateneinbrüchen kompromittiert, auch wenn die Veröffentlichungen zurückgehen

Einige der Schlagzeilen des letzten Jahres ließen die Namen von manchen großen Unternehmen in keinem guten Licht erscheinen: Diese Firmen, denen Millionen vertrauten, waren infiltriert und von massiven Dateneinbrüchen getroffen worden.

Yahoo übernahm dabei die ungewollte Führung und musste im Oktober zugeben, dass alle drei Milliarden Nutzer vom Angriff auf das Unternehmensnetzwerk im August 2013 betroffen waren – ein Dreifaches dessen, was sie vorher zugegeben hatten[60]. Equifax, eine US-Wirtschaftsauskunftei, geriet im September ebenfalls in die Schlagzeilen, weil die Firma zugeben musste, dass die Personal Identifiable Information (PII) von etwa 145,5 Millionen US-Nutzern sowie 15,2 Millionen Nutzer aus Großbritannien bei einem Einbruch im Mai 2017 kompromittiert worden waren[61]. Die Fahrdienstplattform Uber veröffentlichte die Tatsache, dass 57 Millionen Kunden- und Fahrerdatensätze bei einem Datendiebstahl im Oktober 2016 (und einem nachfolgenden Versuch, der nicht erfolgreich war) exponiert wurden[62].

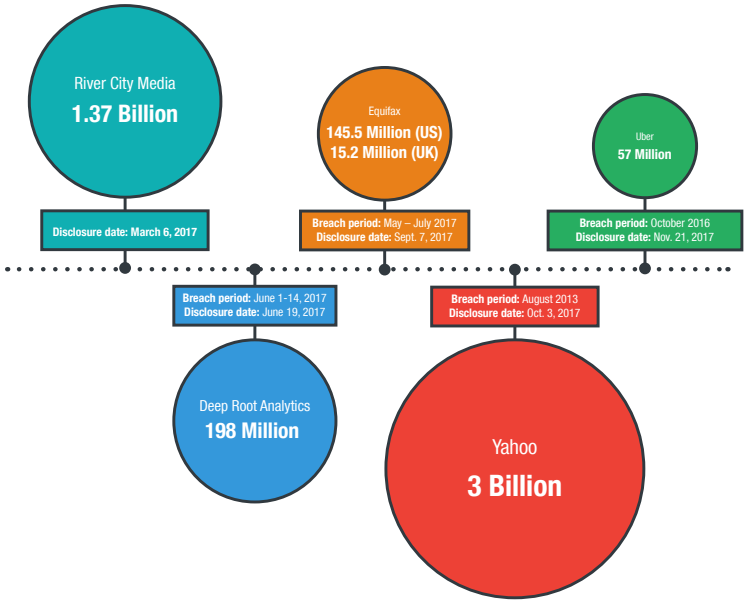


Bild 15. Yahoo führt mit 3 Milliarden betroffenen Datensätzen. Die größten veröffentlichten Datendiebstähle 2017

Das Bekanntwerden einiger schwerer Sicherheitsvorkommnisse ist nicht die einzige interessante Entwicklung im Bereich der Dateneinbrüche 2017. Obwohl die Zahl der betroffenen Datensätze höher liegt als im Jahr zuvor, ist die Zahl der Veröffentlichungen um 32 Prozent zurückgegangen.

Year	Data breaches disclosed	Affected records
2016	813	3,310,435,941
2017	553	4,923,053,245

Achtung: Yahoos Veröffentlichung des Datendiebstahls im Oktober 2017 zeigt sich in der Anzahl der betroffenen Datensätze für 2017. Die Zahlen wurden auf Basis der Daten von Privacy Rights Clearinghouse berechnet[63].

Tabelle 1. Weniger Veröffentlichungen, höhere Zahl betroffener Datensätze: Vergleich der Anzahl der veröffentlichten Dateneinbrüche und der Zahl der betroffenen Datensätze 2016 vs 2017

Der Rückgang in der Zahl der öffentlich gemachten Einbrüche scheint ein Vorspiel der Implementierung der Europäischen General Data Protection Regulation (GDPR) im Mai 2018 zu sein[64]. Die Datenschutzgrundverordnung (DGSV) umfasst strenge Compliance-Standards bezüglich der Benachrichtigung der Öffentlichkeit bei Datendiebstählen. Hohe Strafen erwarten Unternehmen, wenn sie der Verordnung nicht entsprechen. Auch außerhalb Europas gibt es ähnliche Bestrebungen, die persönlichen Informationen und deren Vertraulichkeit zu schützen, so etwa in China[65], Singapur[66], und den USA[67].

Auch wenn die Motivation für einen Einbruch in Unternehmensdatenbanken und –systeme unterschiedlich ist, so kreisen die Methoden immer um bewährte Praktiken. Wie schon 2016[68] ist Hacking immer noch die am meisten genutzte Methode. Von 553 bekannten Einbrüchen liefen 320 — 58 Prozent — über Hacking[69]. Mit dieser Methode wurden auch die Einbrüche bei Yahoo[70], 70 Equifax[71] und Uber[72] durchgeführt.

Cyberkriminelle nutzten für den Diebstahl wichtiger Daten auch Malware. Im Fall der Drive-In Fast Food-Kette Sonic diente Malware dem Abgreifen von Daten von möglicherweise fünf Millionen Kunden, deren Kredit- und Geldkartendaten exponiert wurden[73]. Die InterContinental Hotels Group (IHG) fiel ebenfalls einem Malware-Angriff zum Opfer, bei dem die Cyberkriminellen auf die Kreditkarteninformationen der Kunden zugriffen. Betroffen waren mehr als tausend der Hotels in den USA und Puerto Rico[74].

Nicht alle Dateneinbrüche werden durch fortgeschrittene Infiltration verursacht. Manchmal sind sie das Ergebnis reiner Sorglosigkeit oder gar Nachlässigkeit. Beispielsweise führte beim Spam Operator River City Media die unsachgemäße Konfiguration des Backup-Systems zur Veröffentlichung von 1,37 Milliarden Mailadressen[75]. Bei Deep Root Analytics, die 1,1 Terabytes an Informationen von mehr als 198 Millionen US-Bürgern vorhielten, kam es zum Leak, weil unbeabsichtigt die Daten auf einen öffentlich zugänglich

Server hochgeladen wurden[76]. Da gibt es auch noch den Fall von America's JobLink: Eine nicht gepatchte Schwachstelle im Anwendungscode wurde von einem Hacker ausgenutzt, der damit Zugriff auf die Daten von 4,8 Millionen Arbeitssuchenden in 10 US-Staaten erlangte[77].

Einzelne und Unternehmen sollten aus diesen Vorfällen lernen, dass Datendiebstähle ziemlich teuer werden können. Betroffene Unternehmen müssen Milliarden Dollar Verlust und Strafen hinnehmen und verlieren die Unterstützung und das Vertrauen ihrer Kunden.

Übersicht über die Bedrohungslandschaft

Die Trend Micro Smart Protection Network Sicherheitsinfrastruktrur[78] blockte 2017 mehr als 66 Milliarden Bedrohungen.

66,436,980,714

Zum Vergleich: Sie blockte 2016 mehr als 81 Milliarden Bedrohungen. Trend Micro geht davon aus, dass dieser Rückgang der Zahlen durch den Wandel von breit gestreuten Angriffen auf gezieltere Ansätze zurückzuführen ist.

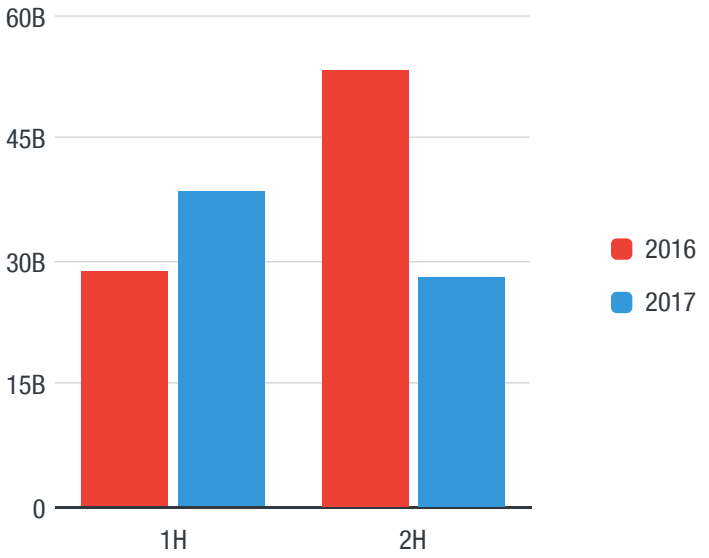


Bild 16. 2017 wurden weniger Bedrohungen geblockt als 2016:
Gesamtzahl der geblockten Bedrohungen durch das Trend Micro Smart, 2016 vs. 2017

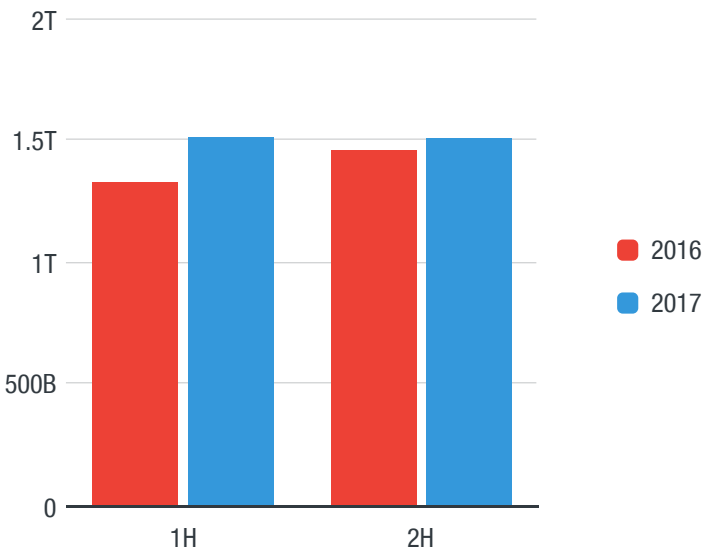


Bild 17. Mehr Client-Queries 2017: Die Menge an Queries auf der Grundlage des Feedbacks aus dem Trend Micro Smart Protection Network, 2016 vs. 2017

In der ersten Hälfte 2017 war .PDF der am häufigsten eingesetzte Dateityp für Spam-Anhänge. Gegen Ende des Jahres jedoch überholte .XLS als Dateityp pdf in den 108.926.882 Spam-Anhängen.

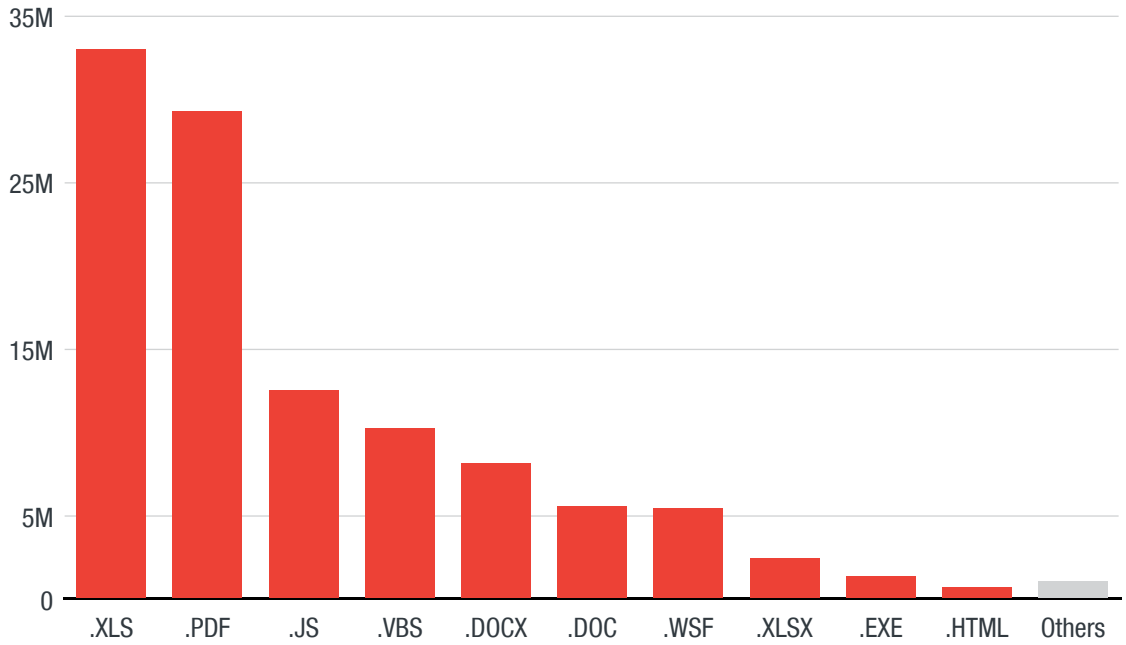


Bild 18. Der Dateityp .XLS tauchte als Top Spam-Anhang auf: Top-10 Dateitypen für Spam-Anhänge 2017

Jan	CRYPFUN	REBOLOCK	VXLOCK	NETIX
	YUHAK	CRYPRAAS	HAVOC	MABORO
	SPORA	EVILWARE	CRYPTOPIC	BLEEDGREEN
	EXMAS			
Feb	CRYPPYT	CRYPCYR	CZCRYPT	VANGUARD
	OSX_CRYPPATCHER	TUSIKSLOCK	PYLEET	KASISKI
	CRYPNTK	HERMES	ONCRYPT	JOBCRYPTER
	FAKEGLOBE	WCRY	PABLUKLOCK	SERBRAN
	SOFADE	CRYPTCONSOLE	URCRYP	EREBUS
	CUTSOME	JAVAWARE		
Mär	NEDSOM	NARLAN	NXCRYP	CRYPDNC
	HAPPYDAYZZZ	BATHIDE	DARKLOCKER	METEORITAN
	LELELOCK	KRYPTA	CRYPDEVIL	CRPTX
	STUP	ROZALOCK	GGCRYP	KIRK
	WEOGO	VORTEX	KAENLUPUF	CRYPJACKY
	CRYPDANGER	CRYPDAMG	YAFCOOKIE	
Apr	DEADSEC	EXTRACTOR	TESTLOCKER	DONTSLIP
	ZIPIAC	BTCWARE	CRYPCTF	KAHAS
	PSHCRYPT	MEDLINZ	LOLI	GOSHIFR
	CONFICKER	SHWERER	CRADLE	RUSHQL
	SHIKEY	ALKA	TRESORAS	LAMBDALOCKER
	GXFORTY	FLUFFY	JANLOCKER	SALSA
Mai	MAYKOLIN	AMNESIA	CRYPEC	VCRYPT
	WANTMYFILES	CLOUDED	BITKANGROO	VIKI
	CRYPJAFF	ANIMESCREENLOCK	UIWIX	LOCKOUT
	FAKEWCRY	LOKTROM	DTOD	VISIONCRYPT
	MEMELOCKER	WIDIALOCKER	EGLUELOCKER	XORDEOS
	MOWARE	DEADDS	RIMALOCKER	THORNIA
	MANCROS	ROBLOCKER	LIGHTNING	WIRA
	QRLOCKER	MISORRY	FAKERA	TESLAWARE
	GOMME	ZIPRAMEN	BRICKR	XORGOT
	CUTWISH			

Jun	BLACKMAIL	BLUEHOWL	JOSKY	SNEKUD
	TUBELAW	DARKENCRYPTOR	DELSCARE	OGRE
	ZILLA	MALHUNT	DESUI	DYNACRYPT
	SAWORSED	MRLOCKER	BEETHOV	XXLECXX
	SPECTRE	GPAA	CASHOUT	PROTONOSX
	CRYPAYSAVE	XINTI	ADLITTLE	FREEZESCARE
	SCARAB	SKULLSCREEN	FAKECERBER	KTZWARE
	WINBAM	LIXLOCKER	QUAKEWAY	PSCRYPT
	DARKSCARE	REETNER	MARKOLOCK	KRYPTONITE
	GOJDUE	GRIFFINLOCK	RUBY	KARO
	VIACRYPT	EXECUTIONER	TRIPM	BUBBLE
	PIRATE	RANPHP	RANSIX	PYTHOCRYP
	WIRUSLOCKER			
Jul	RANRANS	TAKEM	RADIATION	ZERO
	SHELOCKER	EIGHTZLOCK	CRYPTER	HOWLLOCK
	SUPALOCK	MAMOSHII	FAKEPETYA	STUPURGE
	MEGA	MALKI	SCARENOTE	BLACKOUT
	RANSED	STRIKED	REYPTSON	KCAUF
	OOPS	ASNONE	STUPALOISA	CRYPTOMIX
	CHIYUNLONG	BITSHIFT	BAM	SNAKELOCK
	DCRY	VINDOWSCARE	RDW	ABCLOCKER
	INVISCARE	SPONGESCARE	STORM	GRYPHON
	FILEREKT	SIFRELI	DEMON	FCPSCARE
Aug	TPSCARE	DAYSCARE	PASTMONTH	WANNAPAY
	SHELLSKULL	NODEAD	CRYPSTAHL	GOLANG
	CONHOOD	JCODER	LOCKBOX	EBWALL
	ISRABYE	LOCKERPAY	PEYDAY	HELLSCRYPT
	CRYPZABLO	TOOLCRYP	BITPAYMER	SHREKLOCK
	SHINIGAMI	INFINITETEAR	LOCKCRYPT	CRYPTWELVE
	SYNCRYPT	CLICOCRYP	DYNAMITE	BRANGG
	WOODLOCK	CYRON	DZSPLITTER	FLATTENWARE
	ERROR	PASIEM	MINDSYS	STRAWHAT
	WOOLY	SURERAN	CYBER	AKIRA
	HAZE			

Sep	CATLOCKER	HACKBIT	APOLLO	HAKKED
	DILMALOCKER	FAKELOCKY	HAPPYCRYPTER	LOCKED
	BLACKHAT	MYSTIC	MATROSKA	INFINITYLOCK
	ENTREPED	PENDOR	CRYPGG	DEKFOS
	CRYPMOD	CRYPROTO	BUD	SAPNUPUAS.A
	SOLDIERSCARE	CLONE	DEATHMSG	REDBOOT
	MBRLOCKER	ZONE	LOCKSCARE	CYPHERPY
	BLACKMIST	LASERLOCK		
Okt	POLSKY	ENDER	CRYPTROTCOD	AESBAT
	ALLCRY	BADRABBIT	LOSERS	WANNAHAPPY
	XIAOBA	XRANSOM	RYZERLO	
Nov	KRISTINA	SAD	WAFFLE	HSDFSDCRYPT
	FOXY	SIGMA	XMAS	CYBERPOLICE
	JCANDY	LOCKON	RASTAKHIZ	WANNASMILE
	WANADIE	KATAFRACK	SCRAM	NETCRYPT
	HCSIX	WPEACE		
Dez	MAURI	WMONEY	HANDSOMEWARE	BLIND
	HALLOWARE	PAYMENT	MRCYBER	XSCAREWARE
	PURGEN	ETERNITY	FILESPIDER	NOBLIS
	NOWAY	DYNACRYPT	CYCLONE	SITER
	PULPY	ROZLOK	MADBIT	

Tabelle 2. Mehr als 300 tauchten auf: Neue Ransomware-Familien 2017

Im letzten Jahr war das gesamte Exploit Kit-Ökosystem rückläufig, denn Cyberkriminelle nahmen Abstand davon wegen zu geringer Infektionsraten. Stattdessen wandten sie sich anderen verlässlicheren Taktiken zu wie Spam, Phishing und Anvisieren von spezifischen, einzelnen Schwachstellen.

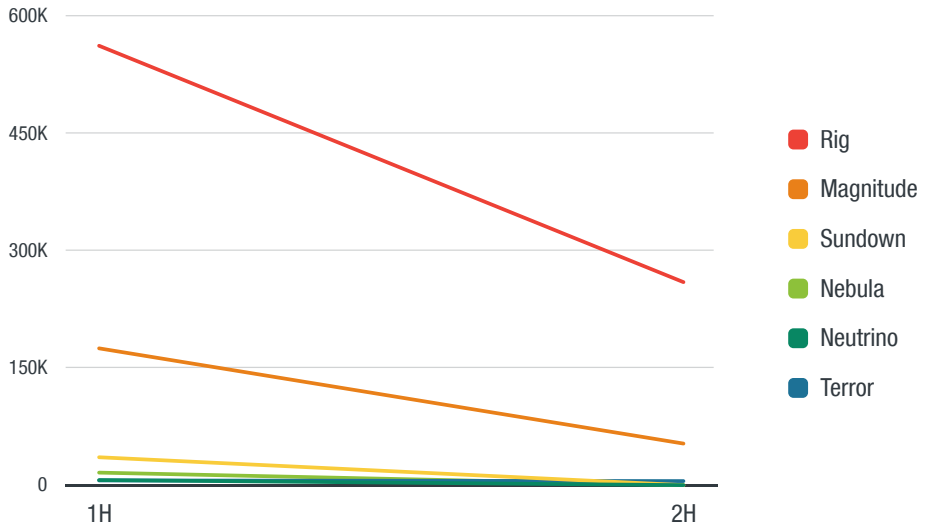


Bild 19. Rückgang im Exploit Kit-Ökosystem: Rückläufige Zahl der Exploit Kit-Angriffe von H1 2017 zu H2

An der mobilen Front zeigen die Daten von Trend Micros Mobile App Reputation Service (MARS), dass 2017 mehr einzigartige Ransomware-Familien mobile Geräte missbrauchten als im Jahr zuvor. Die Slocker mobile Ransomware-Familie ist mit 499.634 Sample führend, während an letzter Stelle mit nur 16 LeakerLocker steht.

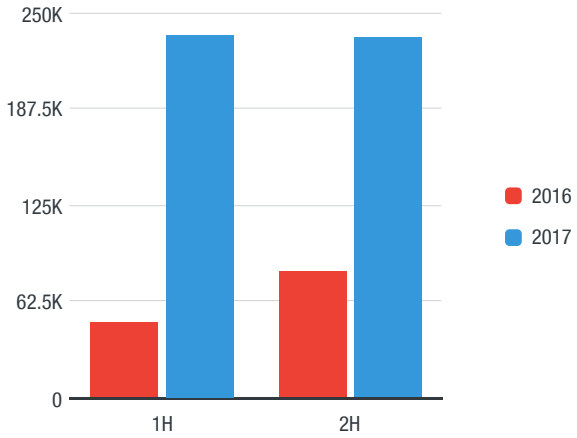


Bild 20. Eine hoher Anstieg bei mobiler Ransomware 2017: Vergleich zwischen einzigartiger mobiler Ransomware, die von MARS entdeckt oder hinzugefügt wurde, 2016 vs. 2017

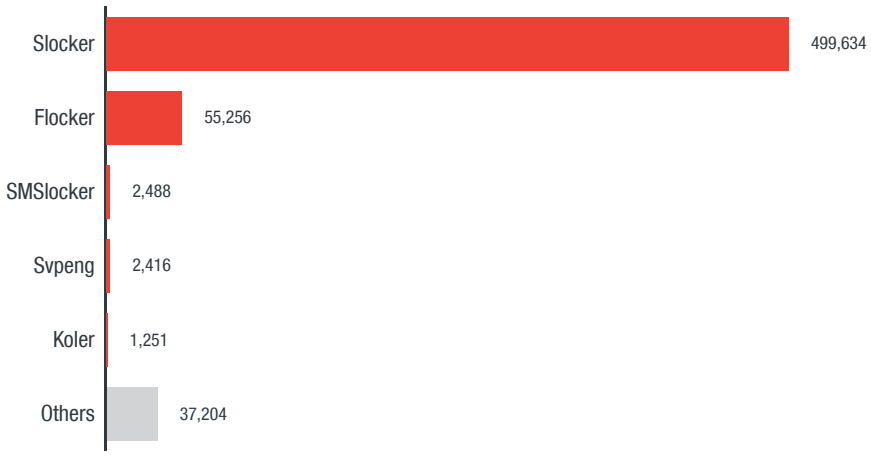


Bild 21. Slocker führt die Liste der mobilen Ransomware an:
Mobile Ransomware-Familien und Zahl der Samples aus MARS 2017

References

1. Trend Micro. (11 September 2017). *Trend Micro*. "2017 Midyear Security Roundup: The Cost of Compromise." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

2. Trend Micro. (6 December 2016). *Trend Micro*. "Security Predictions: The Next Tier." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017.

3. Steve Morgan. (17 May 2017). *Cybersecurity Ventures*. "Global ransomware damage costs predicted to exceed $5 billion in 2017, up from $325 million in 2015." Last accessed on 15 January 2018 at https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.

4. Ryan Delany. (18 May 2017). *Trend Micro Simply Security*. "Protecting Your Small Business From WannaCry." Last accessed on 30 January 2018 https://blog.trendmicro.com/protecting-small-business-wannacry/.

5. Trend Micro. (21 May 2017). *Trend Micro Business Support*. "Preventing WannaCry (WCRY) ransomware attacks using Trend Micro products." Last accessed on 30 January 2018 at https://success.trendmicro.com/solution/1117391-updates-on-the-latestwcry-wannacry-ransomware-attack-and-trend-micro-protection.

6. CBS News. (16 May 2017). *CBS News*. "North Korean hackers behind global cyberattack?" Last accessed on 30 January 2018 at http://www.cbsnews.com/news/cyberattack-wannacry-ransomware-north-korea-hackers-lazarus-group/.

7. Mayra Rosario Fuentes. (10 October 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "WannaCry Ransomware Sold in the Middle Eastern and North African Underground." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/wannacry-ransomware-middle-eastern-north-african-underground/.

8. Mayra Rosario Fuentes. (10 October 2017). *Trend Micro*. "Digital Souks: A Glimpse into the Middle Eastern and North African Underground." Last accessed on 7 February 2018 at https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf.

9. Trend Micro. (29 August 2017). *Trend Micro Simply Security*. "Petya expands its scope: A global ransomware threat." Last accessed on 30 January 2018 at https://blog.trendmicro.com/petya-expands-its-scope-a-global-ransomware-threat/.

10. Nicole Perlroth, Mark Scott, and Sheera Frenkel. (27 June 2017). *The New York Times*. "Cyberattack Hits Ukraine Then Spreads Internationally." Last accessed on 30 January 2018 at https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

11. Trend Micro. (29 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Petya expands its scope: A global ransomware threat." Last accessed on 30 January 2018 at https://blog.trendmicro.com/petya-expands-its-scope-a-global-ransomware-threat/.

12. Trend Micro. (25 October 2017). *Trend Micro*. "Protecting Yourself from Bad Rabbit Ransomware." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/protecting-yourself-from-bad-rabbit-ransomware.

13. Trend Micro. (3 November 2017). *Trend Micro*. "Ransomware Recap: The Short-Lived Spread of Bad Rabbit Ransomware." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/ransomware-recap-the-short-lived-spread-of-bad-rabbit-ransomware.

14. Trend Micro. (25 October 2017). *Trend Micro*. "Protecting Yourself from Bad Rabbit Ransomware." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/protecting-yourself-from-bad-rabbit-ransomware.

15. Trend Micro. (19 June 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Erebus Resurfaces as Linux Ransomware." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/.

16. Trend Micro. (6 December 2016). *Trend Micro*. "Security Predictions: The Next Tier." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017.

17. Gilbert Sison. (2 May 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Cerber Version 6 Shows How Far the Ransomware Has Come (and How Far it'll Go)." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/.

18. Glibert Sison. (28 March 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Cerber Starts Evading Machine Learning." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/.

19. Gilbert Sison and Janus Agcaoili. (3 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Cerber Ransomware Evolves Again, Now Steals From Bitcoin Wallets." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolves-now-steals-bitcoin-wallets/.

20. Max Metger. (13 April 2017). *SC Magazine UK*. "The King is dead, long live the King: Cerber wins in ransomware wars." Last accessed on 18 January 2018 at https://www.scmagazineuk.com/the-king-is-dead-long-live-the-king-cerber-wins-in-ransomware-wars/article/650255/.

21. Trend Micro. (21 August 2017). *Trend Micro*. "Voice Message Malspam Arrives With Locky Ransomware." Last accessed on 18 January 2018 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/671/voice-message-malspam-arrives-with-locky-ransomware.

22. Trend Micro. (9 September 2017). *Trend Micro*. "Fake invoice email with Html attachment spreads Locky ransomware." Last accessed on 18 January 2018 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3621/fake-invoice-email-with-html-attachment-spreads-locky-ransomware.

23. Brooks Li. (29 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Locky Ransomware Now Downloaded as Encrypted DLLs." Last accessed on 17 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/locky-ransomware-now-downloaded-encrypted-dlls/.

24. Trend Micro. (18 September 2017). *Trend Micro*. "Locky Ransomware Pushed Alongside FakeGlobe in Upgraded Spam Campaigns." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/locky-ransomware-pushed-alongside-fakeglobe-upgraded-spam-campaigns/.

25. Trend Micro. (4 September 2017). *Trend Micro*. "New Locky Variant Lukitus Distributed in 23 Million Emails" Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-locky-variant-lukitus-distributed-in-23-million-emails.

26. Buddy Tancio. (15 June 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Analyzing the Fileless, Code-injecting SOREBRECT Ransomware." Last accessed on 23 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/.

27. Veo Zhang. (6 December 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "New Flavor of Dirty COW Attack Discovered, Patched." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-flavor-dirty-cow-attack-discovered-patched/.

28. Mobile Threat Response Team. (25 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "ZNIU: First Android Malware to Exploit Dirty COW Vulnerability." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/.

29. Mobile Threat Response Team. (25 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "ZNIU: First Android Malware to Exploit Dirty COW Vulnerability." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/.

30. Darre Pauli. (23 January 2017). *The Register*. "It's 2017 and 200,000 services still have unpatched Heartbleeds." Last accessed on 18 January 2018 at https://www.theregister.co.uk/2017/01/23/heartbleed_2017/.

31. Trend Micro. (7 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "CONFICKER/ DOWNAD 9 Years After: Examining its Impact on Legacy Systems." Last accessed on 19 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/conficker-downad-9-years-examining-impact-legacy-systems/.

32. Trend Micro. (6 December 2016). *Trend Micro*. "Security Predictions: The Next Tier." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017.

33. FBI IC3. (04 May 2017). *FBI IC3*. "Business E-mail Compromise, Email Account Compromise: The 5 Billion Dollar Scam." Last accessed on 18 January 2018 at https://www.ic3.gov/media/2017/170504.aspx.

34. Trend Micro. (16 June 2016). *Trend Micro*. "BEC Scams Amount to $3 billion According to Latest FBI PSA." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scams-amount-to-3-billion-according-to-latest-fbi-psa.

35. Samuel Gibb. (28 April 2017). *The Guardian*. "Facebook and Google were conned out of $100m in phishing scheme." Last accessed on 30 January 2018 at https://www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme.

36. Reuters. (10 July 2017). *Reuters*. "German Firms Lost Millions of Euros in 'CEO Fraud' Scam: BSI." Last accessed on 18 January 2018 at https://www.usnews.com/news/technology/articles/2017-07-10/german-firms-lost-millions-of-euros-in-ceo-fraud-scam-bsi.

37. Kelli B. Grant. (19 October 2017). *CNBC*. "Scammers are conning homebuyers out of their down payment." Last accessed on 6 February 2018 at https://www.cnbc.com/2017/10/19/scammers-are-conning-home-buyers-out-of-their-down-payment.html.

38. BBC News. (2 November 2017). *BBC News*. "Art galleries targeted by cyber-thieves." Last accessed on 18 January 2018 at http://www.bbc.com/news/technology-41845965.

39. Japan Times. (21 December 2017). *Japan Times*. "Japan Airlines Falls Victim to Email Fraud, Paying Out ¥384 Million to Hong Kong Accounts." Last accessed on 30 January 2018 at https://www.japantimes.co.jp/news/2017/12/21/business/japan-airlines-bilked-%C2%A5384-million-getting-bogus-emails-seeking-lease-fees/#.WnA6N66WaM8.

40. Stan Higgins. (29 December 2017). *CoinDesk*. "From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited." Last accessed on 19 January 2017 at https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/.

41. BBC News. (29 August 2017). *BBC News*. "Burger King launches WhopperCoin crypto-cash in Russia." Last accessed on 6 February 2018 at http://www.bbc.com/news/technology-41082388.

42. Gerrit De Vynck. (25 May 2017). *Bloomberg*. "Kik App Debuts Digital Currency Amid Bitcoin Boom." Last accessed on 6 February 2018 at https://www.bloomberg.com/news/articles/2017-05-25/kik-messenger-app-debuts-own-digital-currency-amid-bitcoin-boom.

43. Chris Cooper and Kiyotaka Matsuda. (22 May 2017). *Bloomberg*. "Peach Becomes Japan's First Airline to Accept Payment in Bitcoin." Last accessed on 6 February 2018 at https://www.bloomberg.com/news/articles/2017-05-22/peach-becomes-japan-s-first-airline-to-accept-payment-in-bitcoin.

44. Dom Galeon. (2 October 2017). *Business Insider*. "Dubai just got its first official cryptocurrency." Last accessed on 6 February 2018 at http://www.businessinsider.com/dubai-official-cryptocurrency-blockchain-emcash-2017-10.

45. Thomson Reuters. (25 October 2017). *Thomson Reuters*. "Cryptocurrencies by country." Last accessed on 6 February 2018 at https://blogs.thomsonreuters.com/answerson/world-cryptocurrencies-country/.

46. BBC News. (19 December 2017). *BBC News*. "Bitcoin exchange Youbit shuts after second hack attack." Last accessed on 2 February 2018 at http://www.bbc.com/news/technology-42409815.

47. Mobile Threat Response Team. (30 October 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Coin Miner Mobile Malware Returns, Hits Google Play." Last accessed on 19 January 2017 at https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/.

48. Trend Micro. (21 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Digmine Cryptocurrency Miner Spreading via Facebook Messenger." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/.

49. Trend Micro Cyber Safety Solutions Team. (20 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "New RETADUP Variants Hit South America, Turn To Cryptocurrency Mining." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-retadup-variants-hit-south-america-turn-cryptocurrency-mining/.

50. Trend Micro. (15 November 2017). *Trend Micro*. "Coinhive Miner Emerges as the 6th Most Common Malware." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coinhive-miner-the-6th-most-common-malware.

51. Joseph Chen. (22 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "ElTest Campaign Uses Tech Support Scams to Deliver Coinhive's Monero Miner." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/eitest-campaign-uses-tech-support-scams-deliver-coinhives-monero-miner/.

52. Statista. (November 2016). *Statista*. "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)." Last accessed on 23 January 2017 at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

53. Trend Micro. (31 January 2017). *Trend Micro*. "Securing Your Routers Against Mirai and Other Home Network Attacks." Last accessed on 30 January 2018 at http://www.trendmicro.com.my/vinfo/my/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks.

54. Trend Micro. (14 December 2016). *TrendLabs Security Intelligence Blog*. "Home Routers: Mitigating Attacks that can Turn them to Zombies." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/home-routers-mitigating-attacks-that-turn-them-to-zombies/.

55. Trend Micro. (1 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "New Mirai Attack Attempts Detected in South America and North African Countries." Last accessed on 30 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-attack-attempts-detected-south-america-north-african-countries/.

56. Stephen Hilt. (27 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "The Need for Better Built-in Security in IoT Devices." Last accessed on 26 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/iot-devices-need-better-builtin-security/.

57. Federico Maggi. (16 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard." Last accessed on 26 January 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/connected-car-hack/.

58. William Malik. (24 October 2017). *Trend Micro Simply Security*. "Accelerating Security for Intelligent Transportation Systems: A New Trend Micro Report." Last accessed on 31 January 2018 at https://blog.trendmicro.com/accelerating-security-intelligent-transportation-systems-new-trend-micro-report/.

59. Trend Micro. (24 October 2017). *Trend Micro*. "High-Tech Highways." Last accessed on 31 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/high-tech-highways-securing-the-future-of-transportation.

60. Trend Micro. (4 October 2017). *Trend Micro*. "Yahoo!: All Three Billion User Accounts Affected in 2013 Data Breach." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/yahoo-all-three-billion-user-accounts-affected-in-2013-data-breach.

61. Trend Micro. (18 September 2017). *Trend Micro*. "The Equifax Breach: What to Do Now and What to Watch Out For." Last accessed on 17 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/equifax-breach-what-to-do-and-what-to-watch-out-for.

62. Mark Nunnikhoven. (22 November 2017). *Trend Micro Simply Security*. "Uber: How Not To Handle A Breach." Last accessed on 30 January 2018 at https://blog.trendmicro.com/uber-how-not-to-handle-a-breach/.

63. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches.

64. Trend Micro. *Trend Micro*. "EU General Data Protection Regulation (GDPR)." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/ph/security/definition/eu-general-data-protection-regulation-gdpr.

65. Sophia Yan. (31 May 2017). *CNBC*. "China's New Cybersecurity Law Takes Effect Today, And Many are Confused." Last accessed on 30 January 2018 at https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.

66. Kevin Kwang. (13 November 2017). *Channel News Asia*. "Singapore's Draft Cybersecurity Bill Tweaked to Include Public Feedback." Last accessed on 30 January 2018 at https://www.channelnewsasia.com/news/singapore/singapore-s-draft-cybersecurity-bill-tweaked-to-include-public-9399378.

67. James E. Lee. (9 May 2017). *Infosecurity Magazine*. "Will New Cybersecurity Legislation Offer Better Protection for Consumers?" Last accessed on 30 January 2018 at https://www.infosecurity-magazine.com/opinions/will-new-cybersecurity-legislation/.

68. Trend Micro. (28 February 2017). *Trend Micro*. "A Record Year for Enterprise Threats." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2016-roundup-record-year-enterprise-threats.

69. Privacy Rights Clearinghouse. *Privacy Rights Clearinghouse*. "Data Breaches by Breach Type." Last accessed on 30 January 2018 at https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2434.

70. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches?title=yahoo.

71. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches?title=equifax.

72. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches?title=uber.

73. Brian Krebs. (26 September 2017). *Krebs on Security*. "Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards." Last accessed on 18 January 2018 at https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/.

74. Mariella Moon. (20 April 2017). *Engadget*. "Over 1,000 Intercontinental hotels hit by a data breach." Last accessed on 30 January 2018 at https://www.engadget.com/2017/04/20/intercontinental-data-breach/.

75. Mark Wycislik-Wilson. (6 March 2017). *BetaNews*. "Huge database leak reveals 1.37 billion email addresses and exposes illegal spam operation." Last accessed on 2 February 2018 at https://betanews.com/2017/03/06/river-city-media-spam-database-leak/.

76. Trend Micro. (15 December 2017). *Trend Micro*. "Year in Review: Notable Data Breaches for 2017." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017.

77. Trend Micro. (15 December 2017). *Trend Micro*. "Year in Review: Notable Data Breaches for 2017." Last accessed on 30 January 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017.

78. Trend Micro. *Trend Micro*. "Smart Protection Network – Global Threat Intelligence." Trend Micro. Last accessed on 30 January 2018 at https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.

Über Trend Micro
Als einer der weltweit führenden IT-Sicherheitsanbieter verfolgt Trend Micro das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Die innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten mehrschichtigen Schutz für Rechenzentren, Cloud-Umgebungen, Netzwerke und Endpunkte.
Die Lösungen von Trend Micro sind für führende Umgebungen wie Amazon Web Services, Microsoft® und VMware® optimiert. Mit ihnen können Organisationen den Schutz ihrer wertvollen Daten vor aktuellen Bedrohungen automatisieren. Die miteinander kommunizierenden Produkte bilden einen vernetzten Schutzmechanismus, der durch zentrale Transparenz und Kontrolle eine schnellere und bessere Absicherung ermöglicht.
Zu den Kunden von Trend Micro zählen 45 der Top-50-Unternehmen der Fortune® Global 500 sowie alle der zehn jeweils führenden Unternehmen in den Branchen Automotive, Bankenwesen, Telekommunikation und Erdöl.
Mit nahezu 6.000 Mitarbeitern in über 50 Ländern und der fortschrittlichsten Analyse globaler Cyberbedrohungen schützt Trend Micro zuverlässig vernetzte Unternehmen.
Die deutsche Niederlassung von Trend Micro befindet sich in Hallbergmoos bei München. In der Schweiz kümmert sich die Niederlassung in Wallisellen bei Zürich um die Belange des deutschsprachigen Landesteils, der französischsprachige Teil wird von Lausanne aus betreut; Sitz der österreichischen Vertretung ist Wien.
Weitere Informationen zum Unternehmen und seinen Lösungen sind unter **www.trendmicro.de** verfügbar, zu aktuellen Bedrohungen unter **blog.trendmicro.de** sowie **blog.trendmicro.ch**. Anwender können sich auch unter **@TrendMicroDE** informieren.

TREND MICRO™ Securing Your Connected World

TREND MICRO Deutschland GmbH
Zeppelinstrasse 1 • 85399 Hallbergmoos
Germany
Tel. +49 (0) 811 88990-700
Fax +49 (0) 811 88990-799

TREND MICRO Schweiz GmbH
Schaffhauserstrasse 104 • 8152 Glattbrugg
Switzerland
Tel. +41 (0) 44 82860-80
Fax +41 (0) 44 82860-81

TREND MICRO (SUISSE) SÀRL
World Trade Center • Avenue Gratta-Paille 2
1018 Lausanne
Switzerland

www.trendmicro.com