BERICHT

proofpoint.

VIERTEL-JÄHRLICHER BEDROHUNGS-BERICHT

4. QUARTAL 2017

proofpoint.com/de

Der *vierteljährliche Proofpoint-Bedrohungsbericht* stellt die Trends und wichtigsten Fakten von Angriffen vor, die wir bei unserer großen Kundenbasis und in der Bedrohungslandschaft insgesamt beobachten.

Jeden Tag analysieren wir mehr als 1 Milliarde E-Mails, hunderte Millionen Social-Media-Posts und mehr als 150 Millionen Malware-Exemplare. Besondere Berücksichtigung erhalten dabei die drei wichtigsten Vektoren für hochentwickelte Bedrohungen: E-Mails, Social Media und Cloud-Anwendungen. Dadurch erhalten wir einen hervorragenden Überblick und können die Taktiken, Tools sowie Ziele heutiger Cyberangriffe aufdecken und analysieren.

Dieser Bericht soll Ihnen umsetzbare Informationen geben, mit denen Sie aktuelle Angriffe besser abwehren, sich auf neue Bedrohungen vorbereiten und Ihre Sicherheitslage verbessern können. Neben diesen Erkenntnissen empfiehlt der Bericht Schritte, mit denen Sie Ihre Mitarbeiter, Daten und Marken schützen können.

INHALT

DIE WICHTIGSTEN PUNKTE: COIN-MINER UND RANSOMWARE STEHEN IM MITTELPUNKT

Im Folgenden stellen wir die wichtigsten Erkenntnisse des vierten Quartals 2017 vor.

E-MAILS

Das Aufkommen an E-Mail-Nachrichten mit schädlichen Dokumentanhängen nahm sprunghaft um 300 % zu.
Ein Großteil dieses Datenverkehrs stammt von massiven Angriffskampagnen, die das Microsoft DYNAMIC DATA EXCHANGE-Protokoll missbrauchten und Social Engineering nutzten.

RANSOMWARE ist auch weiterhin der am häufigsten von schädlichen E-Mails verbreitete Schadcode.
Dieser Angriffstyp macht 57 % des Gesamtaufkommens aller schädlichen Nachrichten aus.

Die Zahl der Ransomware-Zahlungsforderungen, die in Bitcoin geleistet werden sollten, fiel um 73 %. Gleichzeitig erlebte die KRYPTOWÄHRUNG enorme Wechselkursschwankungen.
Die Angreifer fordern das Lösegeld immer häufiger in US-Dollar oder der jeweiligen Landeswährung (obwohl die Zahlung selbst meist in Kryptowährung erfolgt).

THE TRICK war der am häufigsten genutzte Bank-Trojaner.
Er machte 84 % aller schädlichen Spam-Nachrichten aus, die einen Bank-Trojaner enthielten.

Doppelgänger- und TYPOSQUATTING-Domänen kamen bei verschiedensten Angriffen zum Einsatz.
Meist wurden Buchstaben ausgetauscht, um Domänen zu erzeugen, die etablierten Marken oder Unternehmen zum Verwechseln ähnlich sahen.

EXPLOIT-KITS UND WEBBASIERTE ANGRIFFE

Die Zahl von Social-Engineering-Techniken nahm bei bekannt gewordenen webbasierten Angriffskampagnen zu, während Browser-Exploits zurückgingen.
EXPLOIT-KIT (EK)-Datenverkehr ging im Vergleich zum vorherigen Quartal um 31 % zurück. Das Exploit-Kit RIG wurde am häufigsten eingesetzt.

SOCIAL MEDIA

Die Zahl betrügerischer Kundendienst-Konten in sozialen Netzwerken stieg um 30 %.
Gleichzeitig wuchs die Zahl von Phishing-Links in sozialen Netzwerken um 70 % im Vergleich zum vorherigen Quartal.

DYNAMIC DATA EXCHANGE
Dynamic Data Exchange (DDE, dynamischer Datenaustausch) ist ein 20 Jahre altes Kommunikationsprotokoll in Microsoft Windows, das das Abrufen von Dokumenten aus anderen Dokumenten erlaubt. Die Technik wurde größtenteils durch neuere Protokolle ersetzt, wird jedoch weiterhin in Windows unterstützt.

RANSOMWARE
Diese Malware-Form sperrt die Daten der Opfer per Verschlüsselung und fordert ein Lösegeld (englisch „ransom“) für den Entschlüsselungsschlüssel.

KRYPTOWÄHRUNG
Eine Form digitalen Geldes, die als sicher und anonym gilt und daher gut geeignet ist, eine Verfolgung von Ransomware-Zahlungen bis zum Angreifer zu verhindern.

THE TRICK
Der Bank-Trojaner The Trick (auch als Trickbot bekannt) ist eng mit Dyre verwandt, deren Betreiber 2015 von russischen Behörden verhaftet wurde, 2017 jedoch wieder auftauchte.

TYPOSQUATTING
Betrüger registrieren Domänen mit Fehlschreibungen oder typographisch falsche Versionen legitimer Domänen, um Benutzer zu täuschen, die die URL falsch eingeben oder nicht genau auf den E-Mail-Header achten.

EXPLOIT-KIT
Exploit-Kits (EKs) werden über das Web ausgeführt. Sie erkennen und missbrauchen Schwachstellen auf Computern, die über das Internet auf kompromittierte Websites, schädliche Werbung und von Hackern gesteuerte Landing Pages zugreifen. Dadurch können sie PCs problemlos bei „Drive-by“-Downloads mit Malware infizieren. Exploit-Kits werden von Angreifern häufig als Service verkauft und zunehmend verwendet, um Social-Engineering-Angriffe zu ermöglichen, die nicht auf aktiven Exploits basieren.

TA505
Dieser finanziell motivierte Bedrohungsakteur hat einige der bisher umfangreichsten E-Mail-Angriffskampagnen gestartet. Dazu gehören unter anderem Kampagnen, die die Bank-Trojaner Dridex und The Trick oder die Ransomware-Varianten Locky und Jaff verbreiteten.

LOCKY
Locky ist die derzeit häufigste Ransomware-Variante in schädlichen E-Mails und verschlüsselt die Daten der Opfer, um sie in „Geiselhaft" zu nehmen, bis das Lösegeld gezahlt wurde. Über den größten Teil des Jahres 2016 und über mehrere Monate des Jahres 2017 war Locky für den meisten Datenverkehr mit schädlichen E-Mails verantwortlich.

GLOBEIMPOSTER
Diese auch als Fake Globe bekannt Ransomware-Variante imitiert die frühere Ransomware-Variante Globe und ist auch danach benannt. GlobeImposter wurde ursprünglich nur in regionalen Kampagnen verwendet, entwickelte sich jedoch zu einer globalen Bedrohung, als der aktive Bedrohungsakteur TA505 sie in umfassenderen Kampagnen einsetzte.

E-MAILS: SCHÄDLICHE DOKUMENTE ZIEHEN AN URLS VORBEI

Wichtigste Statistik: Das Aufkommen an E-Mail-Nachrichten mit schädlichen Dokumentanhängen nahm im Vergleich zum vorherigen Quartal sprunghaft um 300 % zu.

Das weltweite Aufkommen an Nachrichten mit schädlichen Anhängen machte einen enormen Sprung nach vorn und legte im Vergleich zum vorherigen Quartal 300 % zu. Getrieben von hochvolumigen Kampagnen des Bedrohungsakteurs **TA505** verteilten diese E-Mails den Bank-Trojaner The Trick oder eine bunte Mischung an Ransomware-Varianten, zum Beispiel **LOCKY** und **GLOBEIMPOSTER**.

Mehrere Angreifer nutzten die Bekanntgabe einer Technik für den Missbrauch von Microsoft Dynamic Data Exchange (DDE) zur Verbreitung von Malware in großen und kleinen Kampagnen.

Zum Ende Oktober hatten die Angreifer diese Technik weitgehend aufgegeben und sich wieder ihren üblichen Methoden zugewandt – der Ausnutzung schädlicher Makros und andere Formen von eingebettetem Code. Einzelne Kampagnen nutzen jedoch auch im November und Dezember weiterhin die DDE-Technik, da sie in das Arsenal der Tools der Bedrohungsakteure aufgenommen wurde.

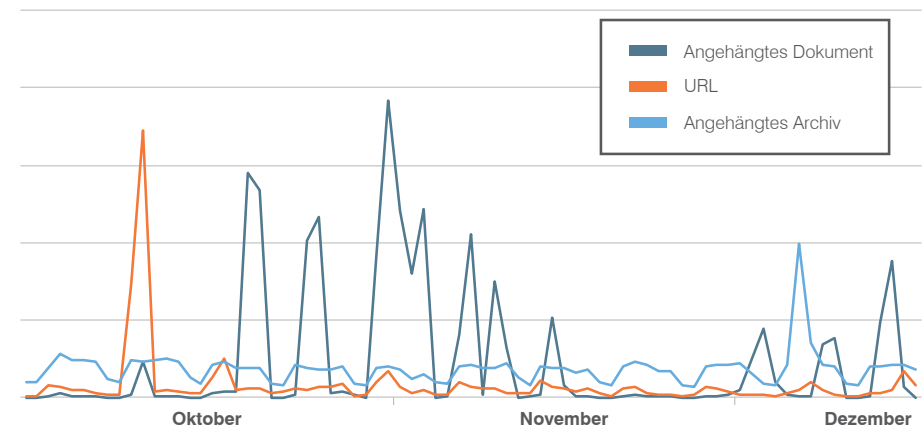

Abb. 1: Trend bei erfassten Angriffstypen, Oktober 2017 bis Dezember 2017 (77 Tage)

Im Gegensatz dazu ging die Nutzung schädlicher URLs erheblich zurück: Die außergewöhnlich hohen Zahlen des dritten Quartals erwiesen sich als Ausnahme. Dennoch sind alle Angriffstypen bei den verschiedensten Bedrohungsakteuren im Einsatz.

Abb. 1 zeigt die erheblichen Schwankungen beim Aufkommen schädlicher E-Mails, die schädliche URLs, Dokumentanhänge und Archivdateien (z. B. ZIP oder 7-Zip) nutzen. Diese beständigen Wechsel verdeutlichen, wie flexibel die Angreifer vorgehen. Sie variieren ständig ihre Angriffstypen, Schaddaten und Infektionstechniken, um effektiver vorzugehen und maximale Profite zu erzielen.

BANK-TROJANER
Dieser Malware-Typ stiehlt die Online-Banking-Anmeldedaten von Kunden. Dies erfolgt meist dadurch, dass der Browser des Opfers auf eine gefälschte Version der Bank-Website umgeleitet oder ein gefälschtes Anmeldeformular in die echte Website injiziert wird.

ZEUS PANDA
Dieser Bank-Trojaner ist auch als Panda Banker bekannt und mit Zeus, einem der frühesten Bank-Trojaner, verwandt.

COIN MINER
Kryptowährung wird mit einem als „Mining" (Schürfen) bezeichneten Prozess generiert, der die Rechenleistung des Computers zur Lösung komplexer mathematischer Probleme verwendet. Die Malware-Variante Coin Miner übernimmt infizierte Systeme, um mit deren Hilfe Kryptowährung für den Bedrohungsakteur zu generieren, der hinter der Malware steht.

WEBINJEKTION
Diese Technik manipuliert die Anzeige von Webseiten für die Benutzer und wird eingesetzt, um unsichere Formulare in scheinbar sichere Webseiten einzubinden. Wenn Benutzer diese Formulare ausfüllen (z. B. mit ihren Online-Banking-Zugangsdaten), werden diese Informationen nicht an die Bank, sondern an den Angreifer gesendet.

BANK-TROJANER: NICHT NUR FÜR BANKEN EINE GEFAHR

Wichtigste Statistik: E-Mails, die The Trick verteilten, machten 84 % aller Nachrichten mit BANK-TROJANERN aus.

The Trick ist – gemessen am Anteil des weltweiten E-Mail-Aufkommens – auch weiterhin der am häufigsten genutzte Bank-Trojaner. Er wurde sechsmal so häufig gefunden wie alle anderen erfassten Bank-Trojaner zusammen. Daran war im Jahr 2016 noch nicht zu denken, als Dridex und Vawtrak die Spitzenplätze einnahmen und The Trick vornehmlich auf kleine und regionale Kampagnen beschränkt war.

Neben The Trick wurden im vierten Quartal auch **ZEUS PANDA** (auch bekannt als Panda Banker) und Emotet häufig in Kampagnen registriert. Zudem wechselten mehrere regelmäßig aktive Angreifer schnell zum neuen Trojaner IcedID.

Einige Bank-Trojaner – der bekannteste davon The Trick – integrierten Module oder Bots zum Schürfen von Kryptowährung. Andere Banker-Kampagnen integrierten solche auch als **COIN MINER** bekannten Funktionen als nachrangige Schaddaten und folgten damit einem Trend, von dem wir bereits im 3. Quartal berichteten.

In den vergangenen Jahren erlebte die Herbstzeit eine größere Vielfalt bei den Zielen von Bank-Trojanern. Das vierte Quartal des Jahres 2017 war da keine Ausnahme. Bei Zeus Panda-Kampagnen wurden die üblichen Online-Banking-**WEBINJEKTIONEN** ergänzt durch Injektionen bei Online-Shopping-Websites zahlreicher beliebter stationärer Einzelhändler.

Diese Veränderungen erinnern auf unangenehme Weise daran, dass Bank-Trojaner keineswegs darauf beschränkt sind, Kunden von Finanzdienstleistern anzugreifen. Online-Kunden *aller* Unternehmen oder Services sind potenzielle Ziele.

RANSOMWARE BITCOIN-KURSSCHWANKUNGEN ERSCHÜTTERN DIE BRANCHE

Wichtigste Statistik: Die Nutzung von Bitcoin zur Zahlung von Ransomware-Lösegeld ging um 73 % zurück.

Trotz eines Anstiegs beim Aufkommen von Bank-Trojaner-E-Mails – was in erster Linie auf einen einzigen Angreifer zurückzuführen ist, der The Trick verwendet – blieb Ransomware der häufigste Schadcode, der in E-Mail-Kampagnen zum Einsatz kommt. Wie Abb. 2 zeigt, macht diese Angriffsform mehr als 57 % aller schädlichen E-Mails aus.

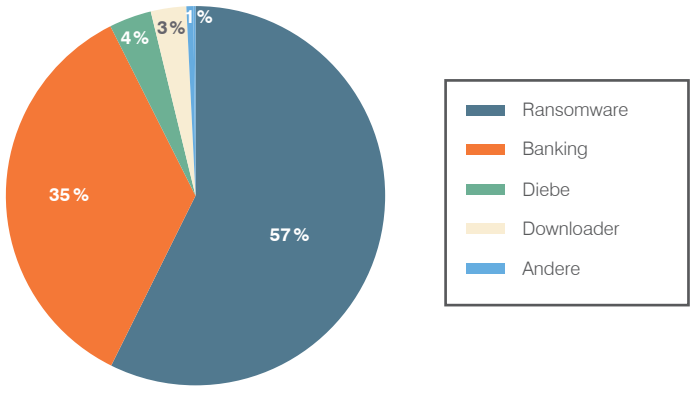

Abb. 2: Anteil des weltweiten Aufkommens schädlicher Nachrichten nach Malware-Familie, 4. Quartal 2017

In den letzten zwei Jahren wurde ein Großteil des Lösegeldes in Bitcoin verlangt. Die geforderte Summe wurde als ganze Bitcoin oder als Teilmenge (z. B. 0,5 oder 0,15) angegeben.

Rapide steigende Kryptowährungskurse sind für Bitcoin-Besitzer ein Geschenk. Für alle, die ihre Produkte oder Services in dieser Währung auspreisen, sind sie jedoch ein Problem. Bedrohungsakteure bilden da keine Ausnahme.

Im vierten Quartal trugen neue Ransomware-Varianten dieser Tatsache offensichtlich Rechnung. Die Ransomware Sigma tauchte erstmals Mitte November auf und verlangte die Lösegeldzahlung in US-Dollar.

Für Angreifer hat die Zahlung in einer Landeswährung – selbst wenn die eigentliche Überweisung in Bitcoin erfolgt – zwei große Vorteile. Einerseits kann der Bedrohungsakteur auf diese Weise Preisstabilität gewährleisten und die Lösegeldzahlung immer noch anonym entgegennehmen. Andererseits erfreut sich die Kryptowährung im Moment großer Beliebtheit.

Eine Analyse von Lösegeldforderungen der letzten 90 Tagen bis Mitte Dezember zeigt, dass der Währungswechsel Teil eines allgemeinen Trends bei vielen Angriffsformen ist (Abb. 3).

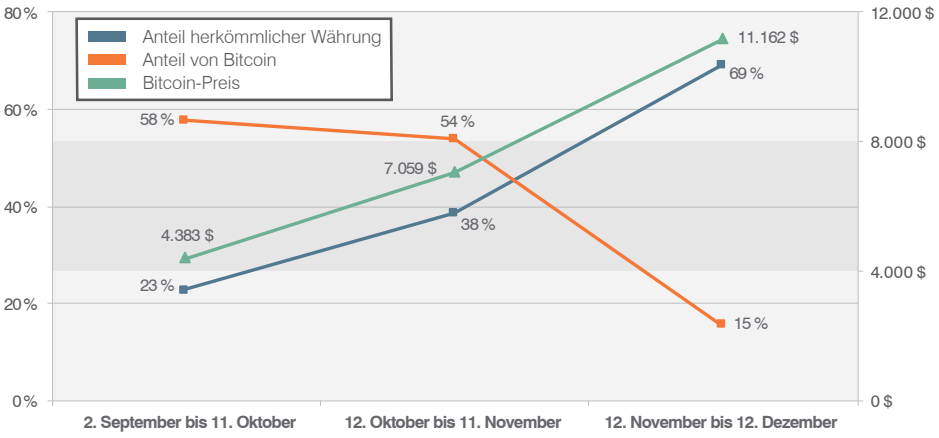

Abb. 3: Ransomware-Lösegeldforderungen: Bitcoin und herkömmliche Währung im Vergleich, 90-Tage-Trend

Die Forderung von Lösegeld in herkömmlicher Währung anstatt oder zusätzlich zu Bitcoin zeigt eindeutige Parallelen zum Anstieg des Bitcoin-Kurses. Ökonomen würden darauf hinweisen, dass das Letztere eine Folge des Ersteren ist.

Dieser Trend kann sich umkehren, wenn die Bitcoin-Preise in den Keller gehen. Doch unabhängig von den eigentlichen Geschehnissen ist die Korrelation ein weiterer Beweis für die Profitorientierung moderner Cyberkrimineller. Sie setzen auf die Tools und Techniken, die ihnen den leichtesten Zugang zum Geld anderer Leute gewähren.

GEZIELT AGIERENDE BEDROHUNGSAKTEURE HEBEN SICH VON DER MASSE AB

Viele der von unseren Forschern im 4. Quartal beobachteten Kampagnen verbreiteten standardmäßige Malware-Schaddaten. Wir analysierten und dokumentierten jedoch auch Aktivitäten verschiedener gezielt agierender Bedrohungsakteure (z. B. Lazarus Group, APT28) sowie eines neuen Bedrohungsakteurs, den wir Leviathan nennen.

Die in diesen Angriffen eingesetzten E-Mails und Dokumente waren häufig personalisiert und an die Interessen sowie Geschäfte der angegriffenen Ziele angepasst. Hierfür verwendeten sie gestohlene öffentliche und mit Markenangaben ergänzte Dokumente. Zudem nutzten sie Typosquatting- oder Doppelgänger-Domänen, um die Benutzer zum Anklicken der Links oder Herunterladen der Dateien zu verleiten.

E-MAIL-BETRUG: ANALYSE DER BENENNUNGSMETHODEN BEI BETRÜGERISCHEN DOMÄNEN

Wichtigste Statistik: Der Durchschnitt bei SCHUTZREGISTRIERUNGEN VON MARKENDOMÄNEN liegt bei 300. Bei großen Unternehmen kann die Zahl verdächtiger registrierter Domänen im Vergleich zu den vom Unternehmen selbst registrierten das Verhältnis von 20 zu 1 erreichen.

SCHUTZREGISTRIERUNG VON MARKENDOMÄNEN
Bezeichnet die empfohlene Praxis, präventiv Internet-Domänen zu kaufen, die mit den eigenen legitimen Domänen leicht verwechselt werden können. Solche Doppelgänger-Domänen werden gern missbraucht, um Kunden und Partner mit gefälschten Websites und betrügerischen E-Mails zu täuschen und davon zu überzeugen, dass diese Websites und E-Mails von Ihrem Unternehmen stammen.

ANGLER-PHISHING
Beim Angler-Phishing erstellen Angreifer gefälschte Kundendienst-Konten für soziale Netzwerke, um Hilfe suchende Benutzer dazu zu verleiten, eine Phishing-Website aufzurufen oder Anmeldeinformationen anzugeben.

Unsere Untersuchungen zeigen, dass Bedrohungsakteure die Marken bei der Registrierung verdächtiger Domänen gegenüber Schutzregistrierungen erheblich überflügeln. Dieser große Abstand führt zu Schutzlücken von Marken bei der Abwehr von Betrug, Phishing, Spoofing und weiteren Angriffsmethoden.

Unternehmen müssen jedoch nicht jede einzelne denkbare Variante ihrer Domäne(n) registrieren, um sich zu schützen. Stattdessen können sie die häufigsten Änderungen und Ersetzungen analysieren, um ihre Schutzregistrierungen zu priorisieren, und auf diese Weise einen Großteil in Frage kommender Typosquatting-Domänen unter ihre Kontrolle bringen.

Doppelgänger-Domänen kommen insgesamt bei etwas mehr als 3 % aller E-Mail-Betrugsversuche zum Einsatz. Anders sieht es jedoch bei E-Mail-Betrug, Phishing, **ANGLER-PHISHING** und anderen Angriffen aus, wo sie überdurchschnittlich häufig vertreten sind.

Obwohl einige Beobachter in erster Linie betrügerische Registrierungen bei neuen oder ungewöhnlichen TLDs (Top-Level Domains) im Blick haben, macht die bekannte „.com“-TLD immer noch den Großteil der verdächtigen Registrierungen aus.

Während fast 82 % dieser Registrierungen „.com“ verwenden, nutzen fast 90 % aller verdächtigen Registrierungen die gleiche TLD nutzen wie die angegriffene Marke. E-Mail-Betrüger setzen häufig auf einfache Variationen legitimer Domänennamen innerhalb der TLD der Marke.

Abb. 4 zeigt häufige Muster von Schreibweisen bei der Registrierung verdächtiger Domänen.

Typ der Doppelgänger-Domäne	Unterschiedliche TLD	Gleiche TLD	Insgesamt
Einzelnes ersetztes Zeichen	3,49 %	37,60 %	41,09 %
Zusätzlich eingefügtes Zeichen	0,97 %	31,15 %	32,12 %
Hinzugefügte oder entfernte erste/letzte Zeichen	0,73 %	12,51 %	13,25 %
Entferntes Zeichen	0,41 %	5,10 %	5,51 %
Gleicher Name mit Bindestrich	1,23 %	3,40 %	4,63 %
Gleicher Name	3,40 %	0,00 %	3,40 %
Insgesamt	**10,23 %**	**89,77 %**	**100,00 %**

Abb. 4: Typosquatting-Techniken

Die häufigste Typosquatting-Technik ist der Austausch einzelner Zeichen eines Markennamens innerhalb derselben TLD. Abb. 5 zeigt die häufigsten Zeichenersetzungen.

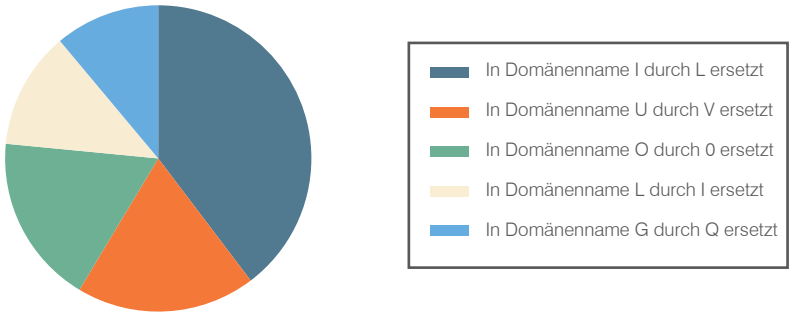

Abb. 5: Muster bei Zeichenersetzungen bei verdächtigen Typosquatting-Domänen für Unternehmen

WEBBASIERTE ANGRIFFE: KONSOLIDIERUNG UND SOCIAL ENGINEERING

Wichtigste Statistik: Der beobachtete Exploit-Kit-Datenverkehr ging seit dem 3. Quartal um 31 % zurück.

EXPLOIT-KIT RIG
Nach dem Verschwinden von Angler im Zusammenhang mit der Verhaftung seiner Betreiber im Juni 2016 wurde RIG zum am weitesten verbreiteten Exploit-Kit.

Der bereits verhaltene Exploit-Kit-Datenverkehr, der schon seit mehreren Quartalen konstant bei etwa 10 % seines Höchstaufkommens von 2016 lag, ging im 4. Quartal noch weiter zurück. Das **EXPLOIT-KIT RIG** war für fast 98 % des beobachteten Exploit-Kit-Datenverkehrs im 4. Quartal 2017 verantwortlich. Doch dessen Anteil am gesamten Datenverkehr sank gegen Ende des Quartals aufgrund des letzten Ausbruchs des Exploit-Kits Magnitude (Abb. 6).

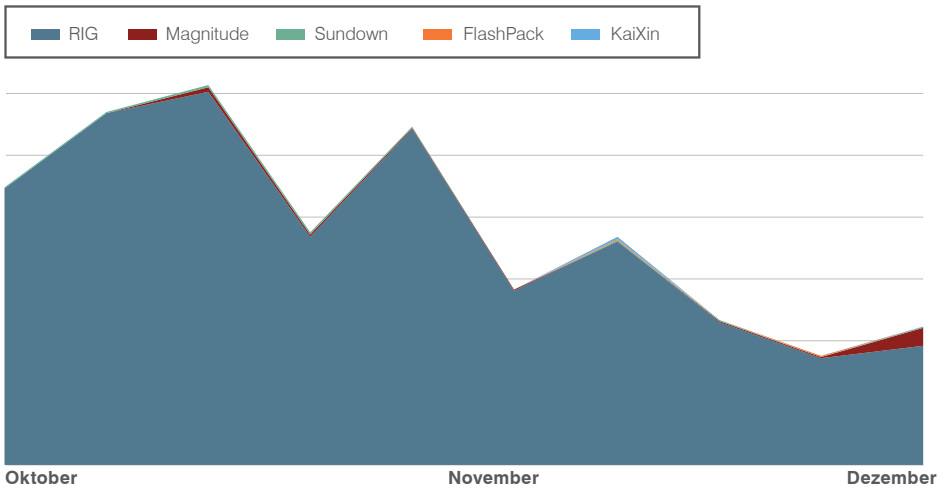

Abb. 6: Datenverkehr der häufigsten Exploit-Kits nach Anteil am Gesamtaufkommen, Oktober bis Dezember 2017

BAD RABBIT
Diese Ransomware-Variante tauchte erstmals im Oktober auf und griff Benutzer in Russland und der Ukraine an. Sie ist der Ransomware-Variante NotPetya ähnlich und tarnt sich als Adobe Flash-Update, das die Systeme über Drive-by-Downloads infiziert. Sie benötigt jedoch einen Benutzer, der das vermeintliche Update startet.

Die große Meldung war die Entdeckung einer großen, ausgeklügelten Kampagne, die auf Benutzer einer beliebten Video-Website für Erwachsene abzielte. Statt technische Fehler in den Webbrowsern der Benutzer auszunutzen, verleiteten die Angriffe ihre Opfer zur Installation der Malware. Die Angreifer nutzen raffinierte Filtertechniken für gezielte Attacken auf bestimmte geografische Regionen und Internetanbieter. Dabei wurde eine Webseite angezeigt, die zum Herunterladen eines Adobe Flash-Updates auffordert. Anstelle des Updates erhalten die Benutzer die Werbebetrugs-Malware Kovter, die beim Ausbruch der Ransomware **BAD RABBIT** zum Einsatz kam.

Angreifern stehen kaum noch ausnutzbare Webbrowser-Exploits zur Verfügung, wozu erschwerend noch die allgemeinen Beschränkungen der Exploits als Infektionstechnik kommen. Wie bereits Ende 2016 in einigen Fällen gezeigt, setzen sie stattdessen auf Social-Engineering-basierte Angriffe, die den früheren E-Mail-Angriffen ähnlich sind. Und dabei waren sie häufig sehr erfolgreich.

KASSENTERMINAL-MALWARE ERLEBT HÖHEN UND TIEFEN

Im Jahr 2016 stellten wir während des Black Friday-Wochenendes fest, dass sich Kassenterminal-Malware vervierfacht hatte. Im Jahr 2017 fielen die Höchstwerte nicht so deutlich aus. Zu verschiedenen Zeiten im Jahr war ein Mix häufiger Kassenterminal-Malware-Varianten aktiv – und das nicht nur am Black Friday (siehe Abb. 7).

So war zum Beispiel FindPOS im März aktiv, ruhte in den Sommermonaten und nahm Ende Oktober seine Aktivitäten wieder auf. Etwa um diese Zeit gingen die Aktivitäten von MagikPOS zurück, was darauf hindeutete, dass ein Akteur das Tool gewechselt hat. Andererseits blieb der Datenverkehr durch NewPosThings – abgesehen von einem Höhepunkt im Juni – über das gesamte Jahr hinweg konstant auf geringem Niveau.

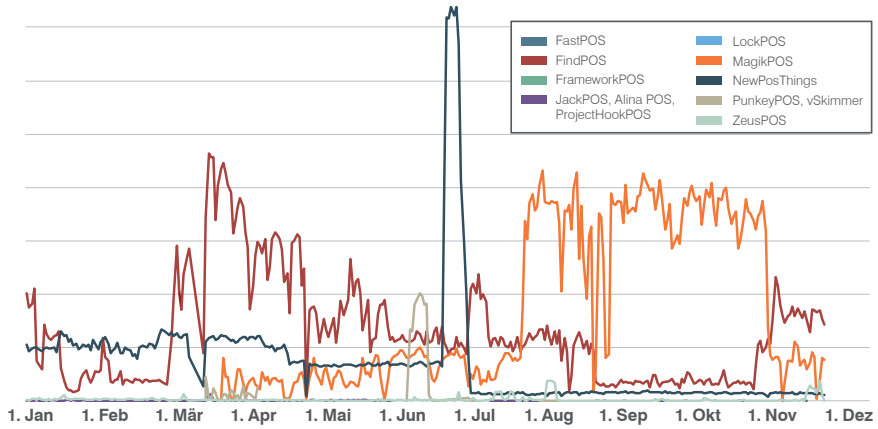

Abb. 7: Datenverkehr bei Kassenterminal-Malware, Januar bis November 2017

Welche Erkenntnisse können wir daraus ziehen? Wir können darüber spekulieren, dass breitere Chip-und-PIN-Implementierungen den Erfolg von Kassenterminal-Malware und damit das Erfolgspotenzial saisonaler Kampagnen verringern, die zu Spitzenwerten im Datenverkehr führen. Dennoch müssen wir die zyklischen Trends bei Kassenterminal-Malware analysieren, um festzustellen, wie bzw. ob sich die Bedrohungslage durch neue und bestehende Varianten verändern wird.

SOCIAL-MEDIA-BEDROHUNGEN STARTEN STARK INS JAHR 2018

Wichtigste Statistik: Die Zahl betrügerischer Kundendienst-Konten in sozialen Netzwerken nahm gegenüber dem vorherigen Quartal und Vorjahr um 30 % zu.

Die Social-Media-Bedrohungen bekamen im vergangenen Quartal Aufwind. Die Zahl der gefälschten Kundendienst-Konten stieg im Vergleich zum vorherigen Quartal und zum gleichen Zeitraum im Jahr 2016 um 30 %.

Nachdem die Zahl der Phishing-Links in sozialen Netzwerken fast das gesamte Jahr 2017 über konstant blieb, stieg sie im 4. Quartal stark an – um fast 70 % gegenüber dem 3. Quartal (Abb. 8).

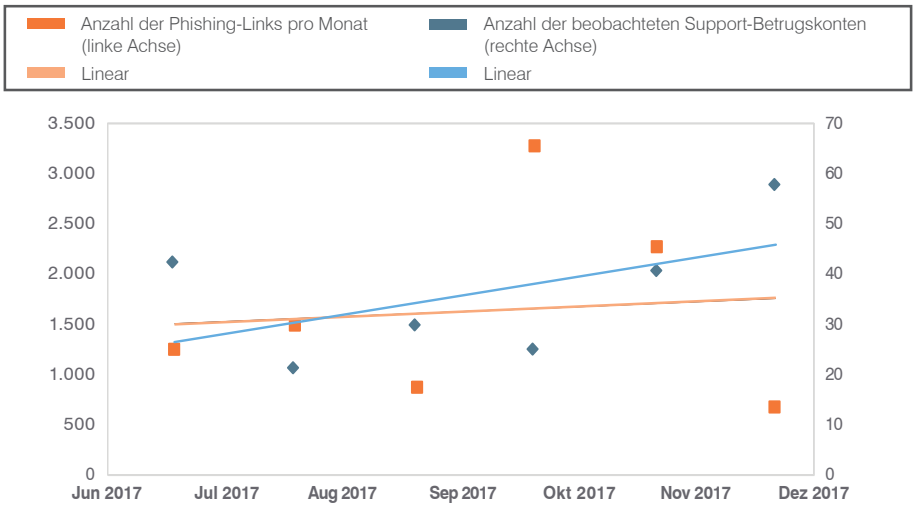

Abb. 8: Relative Aktivitäten im Monat – Vergleich der Trends bei der Verbreitung von Phishing-Links über soziale Netzwerke und betrügerische Support-Konten

EMPFEHLUNGEN

In diesem Bericht erhalten Sie Einblick in die sich verändernde Bedrohungslandschaft, damit Sie Ihre Cybersicherheitsstrategie anpassen können. Mit den folgenden Empfehlungen können Sie Ihre Marke und Ihr Unternehmen in den nächsten Monaten schützen.

Gehen Sie davon aus, dass Benutzer leichtfertig handeln. Social Engineering wird bei E-Mail-Angriffen immer beliebter, und Kriminelle finden immer neue Wege, den Faktor Mensch auszunutzen. Setzen Sie eine Lösung ein, die Ihre Mitarbeiter vor eingehenden sowie Ihre Kunden vor ausgehenden E-Mail-Angriffen schützt und gefährliche E-Mails erkennt sowie isoliert, bevor sie den Posteingang erreichen.

Errichten Sie eine zuverlässige Abwehr zum Schutz vor E-Mail-Betrug. Bei äußerst gezieltem und selten eingesetztem E-Mail-Betrug kommen häufig keine Schaddaten zum Einsatz, sodass er nur schwer zu erkennen ist. Investieren Sie in eine Lösung mit dynamischen Klassifizierungsfunktionen und der Möglichkeit, Quarantäne- und Blockierungsrichtlinien zu erstellen.

Schützen Sie den Ruf Ihrer Marke und Ihre Kunden. Wehren Sie Angriffe auf Ihre Kunden über soziale Netzwerke, E-Mails und Mobilgeräte ab, insbesondere solche mit betrügerischen Konten, die Ihre Marke imitieren. Suchen Sie nach einer umfassenden Lösung zum Schutz vor Social-Media-Angriffen, die alle sozialen Netzwerke überprüft und betrügerische Aktivitäten meldet.

Arbeiten Sie mit einem Anbieter für Bedrohungsdaten zusammen. Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Implementieren Sie eine Lösung, die mithilfe von statischen und dynamischen Techniken Angriffs-Tools, -Taktiken und -Ziele sowie die sich kontinuierlich ändernden Bedrohungen aufdeckt und daraus Erkenntnisse zieht.

Weitere Informationen zu neuesten Ergebnissen der Bedrohungsforschung sowie Hinweise zum Umgang mit aktuellen hochentwickelten Bedrohungen und digitalen Risiken finden Sie unter **proofpoint.com/de/threat-insight**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.

proofpoint.

www.proofpoint.com/de

1217-033