proofpoint

BERICHT

VIERTEL-JÄHRLICHER BEDROHUNGS-BERICHT

3. QUARTAL 2017

proofpoint.com

Der *vierteljährliche Proofpoint-Bedrohungsbericht* stellt die Bedrohungen, Trends und wichtigsten Fakten vor, die wir bei unserem weltweiten Kundenstamm 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 Mobilgeräte. 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: Zurück in die Zukunft **4**

E-Mails 4

Exploit-Kits und webbasierte Angriffe 4

Domänen 5

Social Media 5

Trends bei E-Mail-basierten Bedrohungen **5**

Bank-Trojaner: Neue Trends für alte Bekannte 7

Ransomware: Doppelter Einsatz bei Locky, während destruktive Ransomware zunimmt 8

Seitenleiste: Coinminer – die neue Schürfer-Malware *10*

E-Mail-Betrug nimmt aufgrund der wachsenden Raffinesse der Angreifer zu *10*

Exploit-Kits: Auf dem Rückzug, aber noch nicht am Ende **11**

Trends bei Domänen **12**

Trends bei Social Media **13**

Empfehlungen **14**

DIE WICHTIGSTEN PUNKTE: ZURÜCK IN DIE ZUKUNFT

In den letzten Jahren erwies sich das 3. Quartal stets von besonderem Interesse für Bedrohungsforscher, da in dieser Zeit ein erhöhtes Nachrichtenaufkommen registriert und ein erster Ausblick auf die Tools und Techniken möglich wurde, die in den kommenden Monaten für Angriffe benutzt wurden. Auch in diesem Jahr folgte das 3. Quartal diesem Muster.

Die Zahl der E-Mail-Angriffe mit schädlichen URLs ist förmlich explodiert und stellt seit mehr als zwei Jahren den größten Anteil bei E-Mail Angriffen dar (im Vergleich zu denen mit schädlichen Anhängen). Ransomware und Bank-Trojaner bleiben auch weiterhin die am häufigsten genutzten Angriffsformen.

Währenddessen fand eine Weiterentwicklung bei Social-Engineering- und Targeting-Techniken für E-Mail-Betrug sowie bei Angriffen in sozialen Medien statt.

In unserem ersten veröffentlichten Bericht zu Doppelgänger-Domänen, die für verschiedenste Angriffsformen und Betrugsversuche verwendet werden, schienen die Angreifer den Wettlauf um Domänenregistrierungen zu gewinnen. Für jede präventive „Schutzregistrierung" von Unternehmen fanden wir 20 verdächtige Doppelgänger-Registrierungen durch Dritte.

Im Folgenden stellen wir die wichtigsten Erkenntnisse des Quartals vor.

E-MAILS

Das Aufkommen schädlicher E-Mails stieg aufgrund der rasanten Zunahme gefährlicher URL-Angriffe im Vergleich zum vorherigen Quartal um 85 %.

Das Aufkommen von E-Mails mit schädlichen URLs, die auf gehostete Malware verlinken, explodierte förmlich um 600 % im Vergleich zum vorherigen Quartal sowie um mehr als 2.200 % im Vergleich zum Vorjahresquartal. Die Zunahme ist Zeichen einer Entwicklung, die wir in der ersten Jahreshälfte von 2017 beobachten konnten: Die Zahlen markierten den höchsten Stand bei E-Mails mit URLs (im Vergleich zu E-Mails mit Anhängen) seit 2014. Doch auch große Kampagnen, die auf schädliche Anhänge setzen – in diesem Fall Malware, die in komprimierten Dateiarchiven verborgen ist –, trugen ihren Teil zu diesem Anstieg bei.

Ransomware stellte auch weiterhin die größte Malware-Kategorie dar.

Bei unserem weltweiten Kundenstamm machte Ransomware fast 64 % aller E-Mail-basierten Malware-Angriffsversuche aus. Täglich tauchten neue Ransomware-Varianten auf, doch Locky behielt die Spitzenposition. Die Malware machte fast 55 % des gesamten Nachrichten- und mehr als 86 % des gesamten Ransomware-Aufkommens aus. Gleichzeitig entwickelten sich die Ableger Philadelphia und GlobeImposter aufgrund einiger weniger großmaßstäblicher Kampagnen eines einzelnen Angreifers von kleinen und regional beschränkten Varianten zu weltweiten Bedrohungen.

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.

ETERNALBLUE

EternalBlue ist ein leistungsstarkes Hacker-Tool, das Fehler in einer Dateifreigabe-Komponente von Windows ausnutzt. Dieses Tool wurde von der US-amerikanischen NSA (National Security Agency) gestohlen und Anfang 2017 veröffentlicht.

EXPLOIT-KITS (EKS)

Exploit-Kits (EKs) werden über das Web ausgeführt. Sie erkennen und missbrauchen Schwachstellen auf Computern, die über das Internet auf sie zugreifen. Dadurch können sie PCs problemlos bei „Drive-by"-Downloads mit Malware infizieren. Exploit-Kits werden von Angreifern häufig als Service verkauft.

BANK-TROJANER machten 24 % des gesamten schädlichen E-Mail-Aufkommens aus, wobei die Variante The Trick ganze 70 % dieses Anteils ausmacht.

Aufgrund massiver Kampagnen durch einen einzigen Angreifer löste The Trick die Variante Dridex als häufigster Bank-Trojaner ab. (Nach einer Flaute, die fast das gesamte 1. Quartal andauerte, tauchte Dridex im 2. Quartal bei großen Kampagnen wieder auf.) Dridex kam neben Ursnif, Bancos und Zloader weiterhin in regional beschränkten Kampagnen zum Einsatz. Auch eine neue Version von Retefe wurde gesichtet. Zur Verbreitung dieser Malware über interne Netzwerke nutzten die Angreifer einen geleakten Exploit der US-amerikanischen NSA (National Security Agency), der als **ETERNALBLUE** bezeichnet wird.

E-Mail-Betrug nahm im Vergleich zum vorherigen Quartal um 29 % zu.

Die Angriffe wurden auch häufiger: Die Zahl der E-Mail-Betrugsversuche pro angegriffenem Unternehmen stieg verglichen mit dem vorherigen Quartal um 12 % und um 32 % im Vergleich zum Vorjahresquartal. Obwohl sich E-Mail-Betrug nicht nach der Unternehmensgröße richtet, zählen Unternehmen mit komplexeren Lieferketten zu den häufigeren Zielen.

EXPLOIT-KITS UND WEBBASIERTE ANGRIFFE

Datenverkehr von EXPLOIT-KITS (EKS) blieben in etwa konstant – allerding bei lediglich 10 % der Höchstwerte von 2016.

Das Exploit-Kit RIG war für 76 % aller EK-Aktivitäten verantwortlich. Angreifer binden Social-Engineering-Taktiken in ihre EK-Kampagnen ein. Der Trend weist darauf hin, dass sie nicht mehr ausschließlich auf Exploits setzen, da diese immer schwerer zu entdecken und zu kaufen sind.

SCHUTZREGISTRIERUNGEN
Bezeichnet die empfohlene Praxis, präventiv Internet-Domänen zu kaufen, die mit Ihren Domänen leicht verwechselt werden können. Solche Doppelgänger-Domänen werden gern von Betrügern missbraucht, die Kunden und Partner mit gefälschten Websites und betrügerischen E-Mails täuschen und davon überzeugen wollen, 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 Anmeldedaten anzugeben.

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

DOMÄNEN

Die Zahl verdächtiger Domänenregistrierungen überstieg SCHUTZREGISTRIERUNGEN um den Faktor 20 zu 1.

Einige Unternehmen sind eifrig dabei, zur Abwehr von Typosquattern und Domänenbetrug neue Domänen zu registrieren. Diese Methode ist jedoch nur wenig verbreitet. Die Schutzregistrierung von Markendomänen ging im Vergleich zum Vorjahreszeitraum um 20 % zurück. Die Zahl der verdächtigen Domänenregistrierungen stieg dagegen um 20 %.

SOCIAL MEDIA

Die Zahl betrügerischer Kundendienst-Konten, die für so genanntes ANGLER-PHISHING verwendet werden, verdoppelte sich im Vergleich zum Vorjahresquartal.

Sie stieg verglichen mit dem vorherigen Quartal um 5 %, während das Aufkommen bei Phishing-Links zu Marken-Kanälen in sozialen Medien um 10 % zunahm.

TRENDS BEI E-MAIL-BASIERTEN BEDROHUNGEN

Wichtigste Statistik: Die Anzahl URL-basierter Malware-Kampagnen wuchs um beinahe 600 % im Vergleich zum vorherigen Quartal und um mehr als 2.200 % verglichen mit dem Vorjahresquartal.

Das Aufkommen betrügerischer E-Mails, die mithilfe schädlicher URLs Malware verbreiten, ist enorm angestiegen. Einer der größten Faktoren ist **TA505**, ein äußerst raffinierter Akteur, der für seine massiven Locky-Kampagnen bekannt ist und für die Verbreitung der Ransomware von Anhängen zu URLs wechselte. TA505 verteilte auch die Ransomware Philadelphia und GlobeImposter sowie den Bank-Trojaner The Trick in so großen Mengen, dass sich das auf die Gesamtzahl auswirkte.

Dieser Anstieg ließ das Gesamtaufkommen schädlicher E-Mails im Vergleich zum vorherigen Quartal um 85 % wachsen – und das, obwohl wir bei E-Mails mit schädlichen E-Mail-Anhängen einen 74-prozentigen Rückgang registrierten.

Dennoch spielen schädliche E-Mail-Anhänge auch weiterhin eine wichtige Rolle. Angreifer starteten einige wenige Kampagnen mit schädlichen Anhängen sowie einige besonders große Kampagnen, bei denen Schadcode in komprimierten Dateiarchiven versteckt wurde. Bei diesen Kampagnen kommen RAR- und 7-Zip-Archive zum Einsatz, die meist schädlichen JavaScript- oder VBScript-Code enthalten. Bei ihrer Ausführung laden diese Skripts die Ransomware **LOCKY** herunter.

Die Abbildungen 1 und 2 zeigen, dass E-Mails mit schädlichen URLs beim gesamten Nachrichtenaufkommen einen Anteil von 64 % erreicht haben. Eine solche Menge haben wir seit dem Jahr 2014 nicht mehr erlebt, als E-Mails mit schädlichen URLs den Großteil der gefährlichen Kampagnennachrichten ausmachten. Letztendlich hatten beide Ansätze ähnliche Ziele: Ganz gleich, ob die Schaddaten per URL oder als Anhänge verbreitet wurden, kam bei einem Großteil dieser hochvolumigen Kampagnen die Ransomware Locky zum Einsatz.

Täglich erfasste böswillige Nachrichten nach Angriffstyp (seit Jahresbeginn 2017)

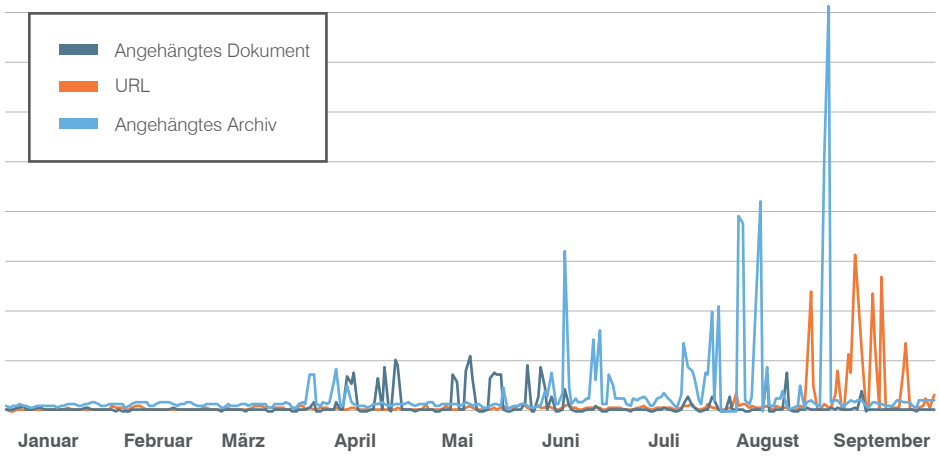

Abb. 1: Trend bei erfassten Angriffstypen, Januar 2017 bis September 2017 (273 Tage)

Vergleich der täglich erfassten böswilligen Nachrichten nach Angriffstyp (3. Quartal 2017)

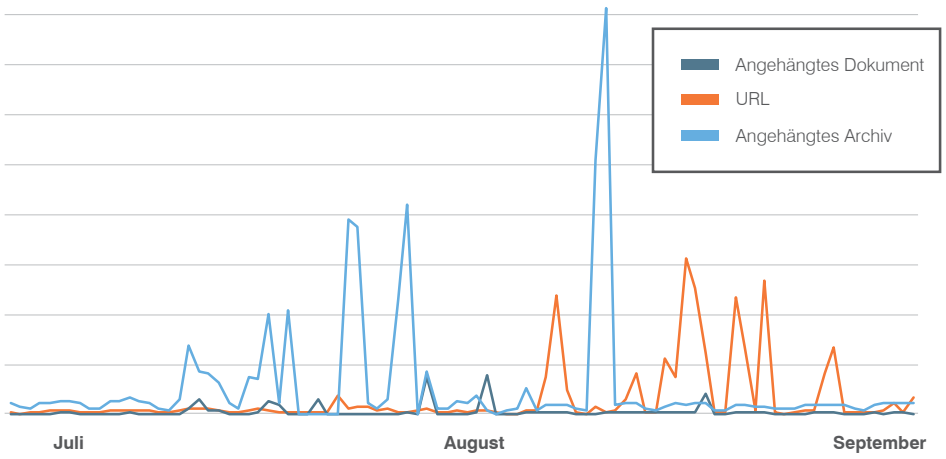

Abb. 2: Trend bei erfassten Angriffstypen, Juli 2017 bis September 2017 (92 Tage)

Abbildung 3 zeigt, wie groß der Anteil von Ransomware wie Locky auch weiterhin ist. Eine Reihe großer Kampagnen, bei denen der Bank-Trojaner **THE TRICK** verteilt wurde, verursachte einige Spitzen gegen Ende des Quartals.

THE TRICK
Der Bank-Trojaner The Trick (auch als Trickbot bekannt) ist eng mit Dyre verwandt. Die Betreiber von Dyre wurden 2015 von russischen Behörden verhaftet, die Malware tauchte jedoch 2017 wieder auf.

Ransomware, Bank-Trojaner und andere Malware im Vergleich

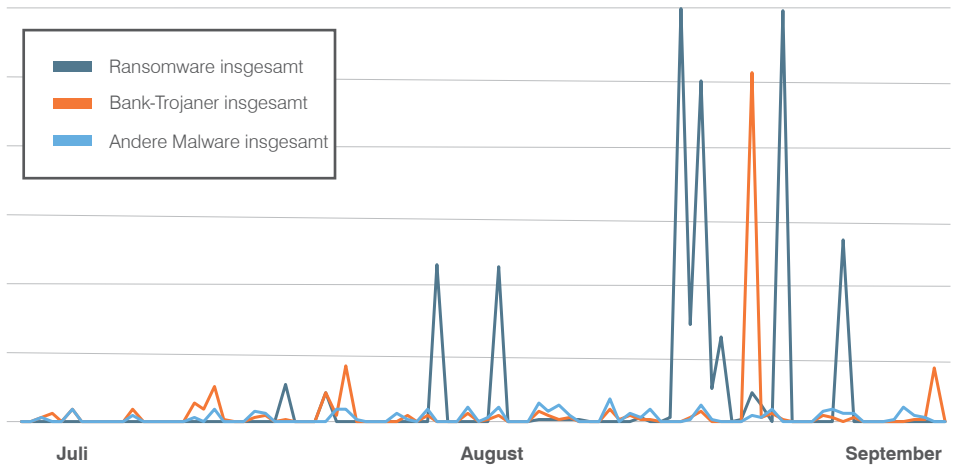

Abb. 3: Juli 2017 bis September 2017 (92 Tage)

BANK-TROJANER: NEUE TRENDS FÜR ALTE BEKANNTE

Wichtigste Statistik: The Trick machte 70 % aller E-Mails aus, die Bank-Trojaner versendeten. Der größte Teil dieser Malware wurde von TA505 verbreitet, dem Bedrohungsakteur hinter den massiven E-Mail-Kampagnen mit der Ransomware Locky und dem Bank-Trojaner Dridex.

Der **DRIDEX**-Datenverkehr ging rapide zurück, als TA505 zu The Trick wechselte. Gleichzeitig blieben die Aktivitäten von **ZLOADER** im Quartalsverlauf größtenteils konstant, wenngleich auf einem geringeren Niveau als im 2. Quartal. Währenddessen tauchten Zeus Panda, Emotet und URLZone in großen und regional beschränkten Kampagnen auf.

Im Rahmen einer potenziell größeren Entwicklung werden Bank-Trojaner wie **RETEFE** und The Trick mit dem EternalBlue-Exploit kombiniert. Dadurch können sich die Trojaner nach der ursprünglichen E-Mail-Infektion ohne weiteres Zutun innerhalb interner Netzwerke ausbreiten. Retefe, das in erster Linie gegen Schweizer Banken gerichtet war und deutschsprachige Köder verwendete, erreichte zu keinem Zeitpunkt das Aufkommen oder die Verbreitung von Dridex oder Zeus. Dennoch weisen die Verwerfungen der **WANNACRY**-Ausbrüche vom Anfang dieses Sommers, bei denen ebenfalls EternalBlue zum Einsatz kam, auf einen potenziellen Trend für 2018 hin: Die Sicherheitsschwachstellen, die von WannaCry und NotPetya aufgedeckt wurden, werden von immer mehr Angreifern ausgenutzt.

Abbildung 4 zeigt das tägliche Aufkommen von Bank-Trojanern. Spitzen beim Datenverkehr von The Trick tauchen immer wieder im Quartal auf und übertreffen die kleineren Anstiege durch Zloader und Panda Banker deutlich.

DRIDEX
Der beliebte Bank-Trojaner Dridex wird über verschiedene Vektoren verbreitet, meist jedoch per E-Mail. Er infiziert die Opfer-Systeme und stiehlt Bank-Anmeldedaten.

ZLOADER
Der Downloader Zloader (auch als Terdot bekannt) wird häufig zusammen mit dem Bank-Trojaner Zbot sowie anderen Malware-Varianten eingesetzt.

RETEFE
Dieser Bank-Trojaner greift vor allem Ziele in Europa an. Statt wie viele andere Bank-Trojaner gefälschte Anmeldeformulare in legitime Bank-Websites einzuschleusen und so Anmeldedaten zu stehlen, leitet Retefe den Benutzer über mehrere Proxy-Server zu einer gefälschten Version der Bank-Website.

WANNACRY
Diese Ransomware infizierte im Mai zehntausende Systeme in mehr als 150 Ländern und gehört damit zu den bisher größten Cyberangriffen. Sie verbreitete sich über einen Fehler in einer Dateifreigabe-Komponente von Microsoft Windows.

Trend bei häufigsten Bank-Trojanern nach täglichem Nachrichtenaufkommen, 3. Quartal 2017

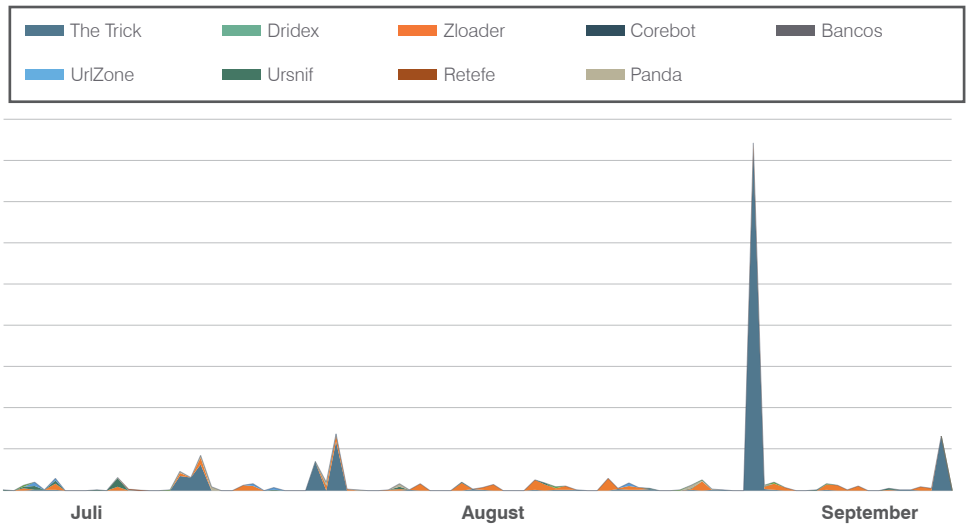

Abb. 4: Täglich erfasste Nachrichten nach häufigsten Bank-Trojanern, Juli bis September 2017

RANSOMWARE: DOPPELTER EINSATZ BEI LOCKY, WÄHREND DESTRUKTIVE RANSOMWARE ZUNIMMT

Wichtigste Statistik: Ransomware-Angriffe machten bei unserem weltweiten Kundenstamm fast 64 % des Gesamtaufkommens schädlicher Nachrichten aus.

Ransomware spielte weiterhin eine dominierende Rolle in der Bedrohungslandschaft. Täglich tauchten neue Varianten auf, die Entwicklung destruktiver Ransomware schritt weiterhin mit vollem Tempo voraus, und die gezielten Angriffe nahmen zu.

Malware nach Kategorie, 3. Quartal

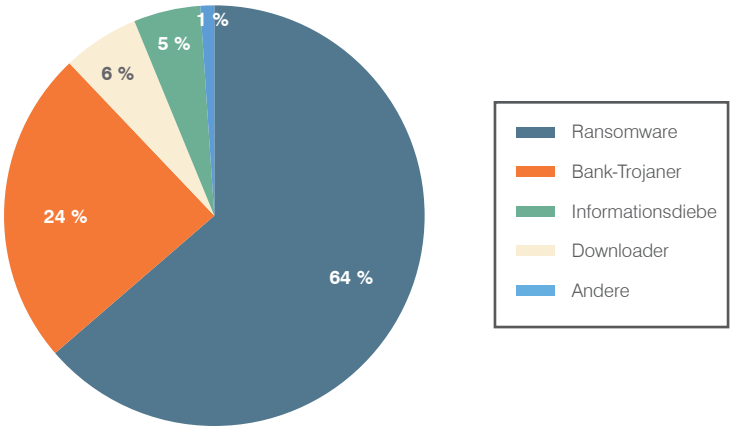

Abb. 5: Vergleich des Gesamtnachrichtenaufkommens im Quartal

Die meisten Ransomware-Varianten tauchten in sehr großen Locky-Kampagnen von TA505 auf. Doch dieser Akteur verbreitete auch die Ransomware-Varianten GlobeImposter und Philadelphia. Bemerkenswert ist, dass eine dieser Varianten eine Offline-Version von Locky enthielt, die keine zentrale C&C-Infrastruktur (Command and Control) benötigte, um die Dateien des Opfers zu verschlüsseln.

Andere Angreifer wechselten von wahllosen massenhaften Kampagnen zu gezielteren Angriffen. Einer setzte im August die Ransomware-Variante Defray für kleine Kampagnen ein, die gegen Ziele im Gesundheitswesen sowie im Bildungsbereich gerichtet waren. Andere Angreifer nahmen sich dies zum Vorbild. Mehrere neue Locky-**AFFILIATE-IDS**, die in Kampagnen registriert wurden, nahmen vorrangig das höhere Bildungswesen sowie das Gesundheitswesen ins Visier. Mindestens eine von ihnen (Affid=36) verteilte die Offline-Version von Locky.

Im Fahrwasser der WannaCry- and Petya-ähnlichen Angriffe in der Ukraine Ende des 2. Quartals tauchten weitere Ableger auf. Hell (im Juli entdeckt) und IsraByte (im August entdeckt) erreichten jedoch nicht den gleichen Verbreitungs- oder Bekanntheitsgrad. Doch ebenso wie **NOTPETYA** und WannaCry schienen sie mehr auf Zerstörung als auf finanzielle Vorteile abzuzielen.

Abbildung 6 zeigt, dass sich Angreifer mit hochvolumigen Kampagnen im 3. Quartal auf eine kleine Zahl von Ransomware-Varianten beschränkten, obwohl neue Ableger und Nutzungsmöglichkeiten verfügbar wurden. Aufgrund der massiven Kampagnen von TA505 dominierten Locky, GlobeImposter und Philadelphia, wobei die neuen Locky-Verbreiter diese Zahlen nur noch verstärkten. Varianten wie SAGE und TorrentLocker sind praktisch ausgestorben.

AFFILIATE-IDS
Malware-Autoren bezahlen häufig Partner dafür, ihre Malware zu verbreiten. Die Affiliate-ID ist in Malware-Versionen festkodiert, womit sichergestellt werden soll, dass die richtigen Partner für die Infektion belohnt werden.

NOTPETYA
Die Malware-Variante tarnte sich als Ransomware Petya, scheint jedoch ein staatlich unterstütztes Tool zu sein, das eher Chaos stiften soll, als Lösegeld zu erpressen.

Trend bei Ransomware-Varianten nach täglichem Nachrichtenaufkommen, 3. Quartal 2017

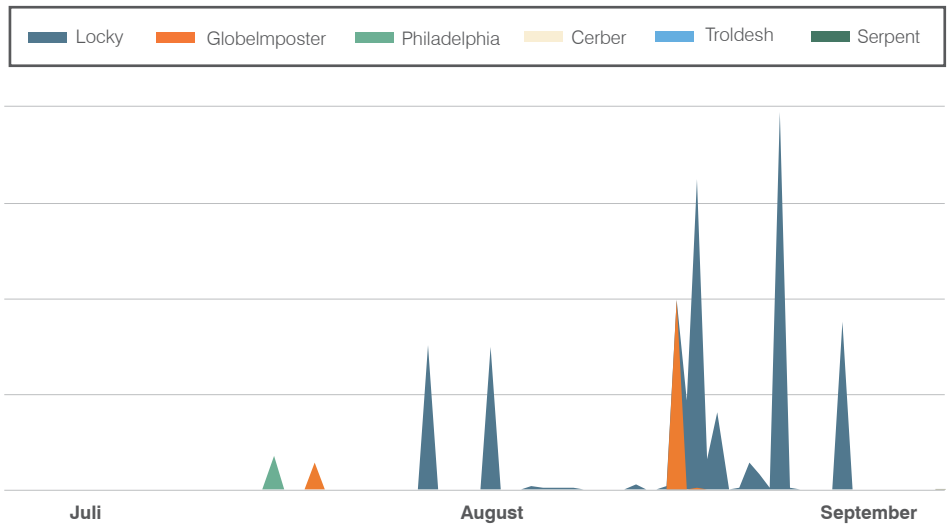

Abb. 6: Täglich erfasste Nachrichten nach häufigsten Ransomware-Varianten, Juli bis September 2017

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

Das exponentielle Wachstum der neuen **RANSOMWARE**-Varianten im vergangenen Jahr scheint sich allmählich etwas zu verlangsamen. Der Grund dafür ist jedoch nicht etwa eine verringerte Bedrohung.

Im Durchschnitt tauchten täglich 1,4 neue Ransomware-Varianten auf, während es im vorherigen Quartal noch 1,8 pro Tag waren. Der Rückgang ist eher durch die sinkende Zahl von Ransomware-Varianten begründet, die als kleines Projekt gestartet werden, als Proof-of-Concept dienen, experimentell sind oder von „Skriptkiddies" eingesetzt werden und frühere Gesamtzahlen aufbauschten.

Mit anderen Worten: Dieser Rückgang geht nicht mit einer geringeren Gefahr durch Ransomware einher. Stattdessen weist er darauf hin, dass die Angreifer sich auf weniger, aber dafür effektivere Varianten konzentrieren, neue Methoden zur Nutzung von Ransomware ausprobieren und dabei immer raffinierter werden (Abbildung 7).

Neu gemeldete Varianten

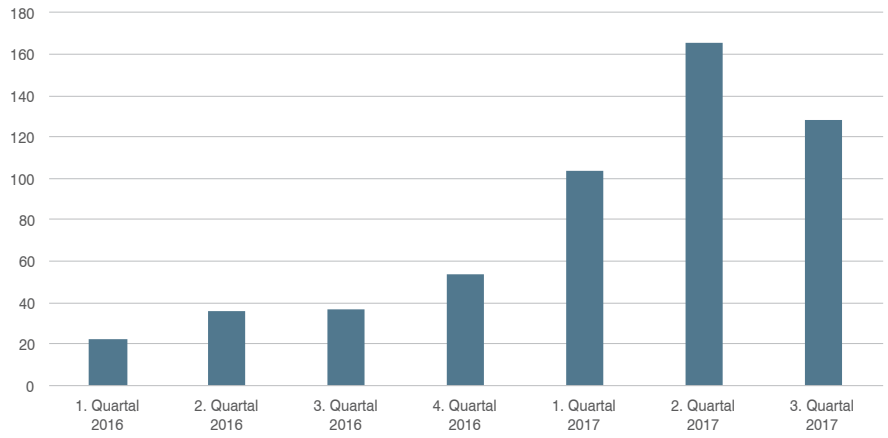

Abb. 7: Neu gemeldete Ransomware-Varianten nach Quartal, 2016 und seit Jahresbeginn 2017

COINMINER – DIE NEUE SCHÜRFER-MALWARE

Miner für **KRYPTOWÄHRUNGEN** (sogenannte „Coinminer“) sind Malware-Varianten, die Systemressourcen infizierter Maschinen zur Generierung elektronischer Währung für Bedrohungsakteure nutzen. Kryptowährungen wie Bitcoin und Litecoin verfügen über integrierte Mechanismen, die die Seltenheit und den Wert der Währungen gewährleisten sollen. Daher werden die Berechnungen zum „Minen“ (Schürfen) neuer Währungseinheiten immer schwieriger. Für die am weitesten verbreitete Kryptowährung Bitcoin sind zum Beispiel inzwischen fast Supercomputer-Rechenleistungen erforderlich. Andere Kryptowährungen wie Litecoin und Monero können jedoch weiterhin mit Desktop-Computern generiert werden – oder dadurch, dass die Rechenleistung zahlreicher Client-Systeme gestohlen wird.

Deshalb verbreitet sich Coinmining-Malware für diese Währungen immer weiter. Für die Verbreitung kommen Exploit-Kits, Social-Engineering-Taktiken und sogar NSA-Exploits wie EternalBlue zum Einsatz. The Pirate Bay gelangte kürzlich in die Schlagzeilen, da hier die Rechenleistung der Besucher zum Schürfen der Währung Monero verwendet wurde.

Die Bedrohung ist äußerst vielseitig. Einige Angriffe zielen auf serverseitige Webschwachstellen ab und integrieren Skripts, damit Coinminer CPU-Ressourcen der Browser von Besuchern nutzen können. Andere Angriffe verwenden Phishing zum Stehlen der Anmeldedaten der Kryptowährungs-Geldbörsen von Benutzern. Dieser Trend verbreitet sich gerade mit hohem Tempo. Andere Malware-Varianten verwandeln die PCs der Opfer in Coinminer.

Unabhängig von der verwendeten Methode werden Bedrohungsakteure wahrscheinlich neue Möglichkeiten finden, die PCs der Opfer zum Schürfen zu missbrauchen. Bis die kleineren Währungen den Sättigungsgrad von Bitcoin erreichen, sind die Erfolgsaussichten sehr groß. Bedrohungsakteure haben immer wieder bewiesen, dass sie bereit sind, „dem Geld zu folgen“.

KRYPTOWÄHRUNG
Eine Form digitalen Geldes, die als sicher und anonym gilt. Die Währung – mit der Waren erworben und verkauft werden können und die sich in Landeswährung umtauschen lässt – wird über einen als „Mining“ (Schürfen) bezeichneten Prozess generiert, der Computerleistung zur Lösung komplexer mathematischer Probleme nutzt.

DOMÄNEN-SPOOFING
Beim Domänen-Spoofing wird versucht, vertrauenswürdige Kollegen oder Kontakte zu imitieren, indem die E-Mail so gestaltet wird, als ob sie von einer legitimen oder erwarteten Adresse stammt. Einige Domänen-Spoofing-Varianten nutzen Namen von Doppelgänger-Domänen, die den echten täuschend ähnlich sind.

E-MAIL-BETRUG NIMMT AUFGRUND DER WACHSENDEN RAFFINESSE DER ANGREIFER ZU

Wichtigste Statistik: E-Mail-Betrugsversuche nahmen bei unserem weltweiten Kundenstamm im Vergleich zum vorherigen Quartal um 29 % zu.

Mit zunehmender Anzahl von E-Mail-Betrugsversuchen nahm auch die Häufigkeit von gezielten Angriffen auf Unternehmen zu: Die Zahl der E-Mail-Betrugsversuche stieg im Vergleich zum vorherigen Quartal um 12 % und im Vergleich zum Vorjahresquartal um 32 %.

DOMÄNEN-SPOOFING, eine häufig verwendete E-Mail-Betrugstechnik, nahm ebenfalls deutlich zu. Diese Angriffsart kann dank E-Mail-Authentifizierung vollständig abgewehrt werden. Dennoch erlebten 89 % aller Unternehmen in diesem Quartal mindestens einen Domänen-Spoofing-Angriff.

Angriffe auf die Branchen

Alle Branchen werden auch weiterhin mit E-Mail-Betrugsversuchen angegriffen. Doch ebenso wie in den vorherigen Quartalen schienen sich die Angreifer auf Unternehmen mit komplexeren Lieferketten zu konzentrieren. Fertigungsunternehmen werden beispielsweise häufiger angegriffen als andere Branchen. Abbildung 8 zeigt die relative Häufigkeit von Angriffen nach Branche. Sie vergleicht das 2. und 3. Quartal 2017 sowie das Vorjahresquartal, die jeweils ähnliche Beziehungen aufzeigten.

Angegriffene Branchen – 3. Quartal 2017, 2. Quartal 2017 und 3. Quartal 2016 im Vergleich

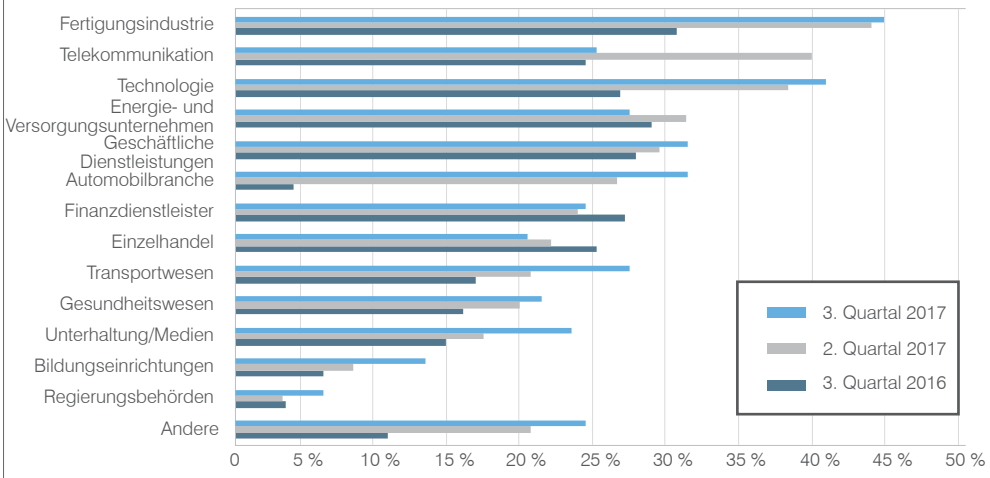

Abb. 8: Durchschnittliche Anzahl betrügerischer E-Mail-Angriffe pro Unternehmen nach Branche, 3. Quartal 2017, 2. Quartal 2017 und 3. Quartal 2016 im Vergleich

E-MAIL-BETRUG
Bei Angriffen mit betrügerischen E-Mails wird der Empfänger in einer E-Mail, die angeblich von einem leitenden Angestellten stammt, zur Überweisung von Geld oder zur Weitergabe vertraulicher Informationen aufgefordert. Da bei dieser Betrugsform weder Dateianhänge noch URLs verwendet werden, ist sie unter Umständen schwer zu erkennen und zu stoppen.

Unsere Analyse des **E-MAIL-BETRUGS** fand keine Korrelation zwischen der Unternehmensgröße und der Häufigkeit von E-Mail-Betrugsversuchen. Zwar registrierten wir im 2. Quartal einige Anzeichen dafür, dass sich Cyberkriminelle auf größere Unternehmen konzentrieren, jedoch nicht mit einem statistisch relevanten Wert. In diesem Quartal gab es überhaupt keinen offensichtlichen Zusammenhang mehr. Stattdessen wurden Unternehmen aller Größen gleichermaßen angegriffen.

Individuelles Targeting beweist Raffinesse

E-Mail-Betrug wird von Natur aus höchst gezielt eingesetzt. Diese Tatsache zeigte sich deutlicher als je zuvor, da die Angreifer mehr Identitäten fälschten und mehr Mitarbeiter pro Unternehmen angriffen. Bei beinahe drei Viertel der angegriffenen Unternehmen wurde mehr als eine Identität gefälscht und mehr als ein Mitarbeiter ins Visier genommen. So genanntes „Whaling“, also Angriffe, bei denen die gefälschte E-Mail einer Führungskraft der obersten Ebene an eine andere Führungskraft gerichtet wird, sind immer noch häufig. (Dieser Angriffstyp wird in Abbildung 9 als „Einer-zu-Einer“-Angriff bezeichnet.) Doch Cyberkriminelle erweitern ihren Aktionsradius und greifen immer mehr Mitarbeiter in jedem Unternehmen an.

Gefälschte Identitäten nach Anzahl der angegriffenen Mitarbeiter, 3. Quartal 2017, 2. Quartal 2017 und 3. Quartal 2016

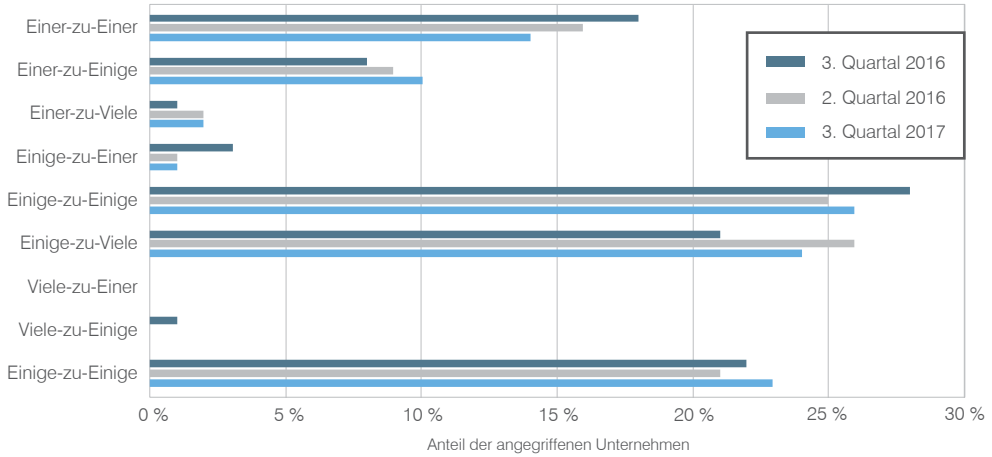

Abb. 9: Angriffstyp nach Anzahl der gefälschten Führungskräfteidentitäten und die Anzahl der angegriffenen Personen im Vergleich. Wenn zum Beispiel ein Unternehmen E-Mail-Angriffe mit betrügerischen Nachrichten beobachtet, wobei die Identitäten von vier Führungskräften gefälscht und zehn Mitarbeiter der Finanzabteilung angegriffen wurden, wird dies als „Einige-zu-Viele“ eingestuft.

Zudem nutzen die Angreifer auch gefälschte E-Mail-Ketten, um ihre E-Mails noch überzeugender wirken zu lassen. Bei etwa 10 % aller betrügerischen E-Mails wurde im 3. Quartal diese Vorgehensweise genutzt.

EXPLOIT-KITS: AUF DEM RÜCKZUG, ABER NOCH NICHT AM ENDE

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

Wichtigste Statistik: Bei 73 % aller Exploit-Aktivitäten des 3. Quartals war das EXPLOIT-KIT RIG involviert.
Exploit-Kits (EK) erlebten nach einem Höchstwert Anfang 2016 einen erheblichen, öffentlichkeitswirksamen Rückgang. Auch wenn die Aktivitäten lediglich 10 % des Niveaus von 2016 ausmachen, bleiben Exploit-Kits weiterhin eine wichtige Bedrohung. Das gilt besonders in den Regionen, in denen Patches aufgrund von Softwarepiraterie selten installiert werden.

Da die Angreifer zur Verbreitung ihrer Exploit-Kits auf neue Social-Engineering-Taktiken setzen, erreichen sie auch ohne die neuesten Exploit-Varianten ihr Ziel. Gleichzeitig nehmen Aktivitäten mit sogenannten „Traffers“ zu. Hierbei handelt es sich um Netzwerke, die Datenverkehr auf EK-Landing-Pages lenken sollen. Diese Veränderung deutet darauf hin, dass die EK-Aktivitäten in den nächsten Monaten wieder zunehmen könnten.

Derzeit ist jedoch das Exploit-Kit RIG dominant und für 73 % des gesamten in diesem Quartal von uns erfassten EK-Datenverkehrs verantwortlich. Bis Ende des Quartals war der bereits vorher schwache Datenverkehr des Exploit-Kits Angler praktisch verschwunden. Selbst Neutrino, das in diesem Quartal zeitweise mit RIG um die Spitzenposition kämpfte, hatte gegenüber RIG letztlich keine Chance. In Abbildung 10 wird der Datenverkehr der häufigsten Exploit-Kits dargestellt.

Exploit-Kit-Aktivitäten nach Anteil der im 3. Quartal 2017 erfassten Varianten

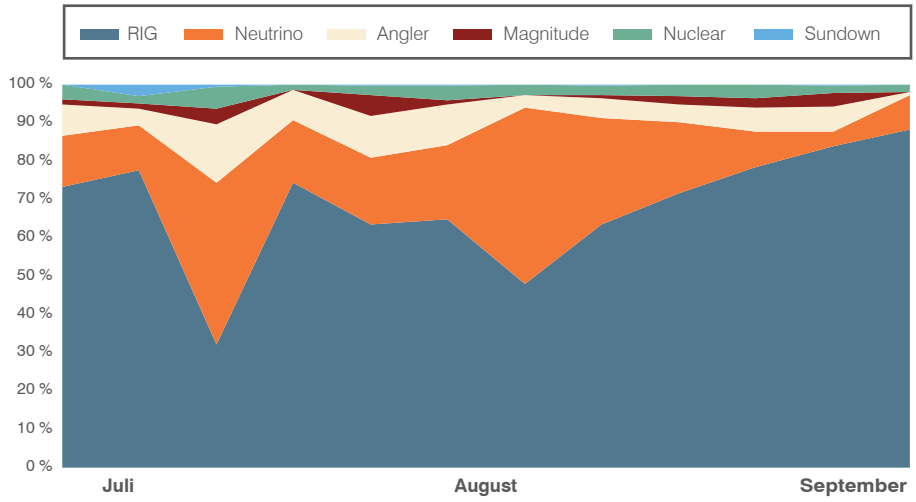

Abb. 10: Datenverkehr der häufigsten Exploit-Kits nach Anteil am Gesamtaufkommen, April bis Mai 2017

TRENDS BEI DOMÄNEN

Wichtigste Statistik: Die Zahl verdächtiger Domänenregistrierungen überstieg die Schutzregistrierungen um das 20-fache. Damit wächst die Lücke zwischen den Unternehmen, die ihre Marke schützen möchten, und den Angreifern, die Marken ausnutzen wollen, noch weiter.

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.

Im 3. Quartal weiteten wir unsere Untersuchungen aus und analysierten die Registrierungen „verdächtiger Domänen" der Fortune 50. Bei verdächtigen Domänen handelt es sich um solche Domänen, die sich besonders für **TYPOSQUATTING** und Spoofing eignen.

Seit Anfang 2015 bis Ende August 2017 sank die Zahl der Domänen, die Unternehmen zum Schutz der eigenen Marke registriert hatten, während die Zahl verdächtiger Domänen, die nicht vom Markeninhaber registriert wurden, stieg (Abbildung 11). Von Januar bis August 2017 wuchs die Zahl der registrierten verdächtigen Domänen um 20 %, während die Zahl der Schutzregistrierungen von Markendomänen im Vergleich zum Vorjahr um 20 % zurückging.

Trotz der vorhandenen Schutzregistrierungen haben verdächtige Domänen in der Vergangenheit die Zahl der Schutzregistrierungen von Markendomänen weit hinter sich gelassen. Für jede Schutzregistrierung im Jahr 2016 fanden wir zehn verdächtige Doppelgänger-Registrierungen durch Dritte. In diesem Jahr lag das Zahlenverhältnis bei 20:1 – zugunsten der verdächtigen Registrierungen.

Zudem sind starke Zunahmen bei Schutzregistrierungen meist mit großen markenbezogenen Ereignissen (z. B. der Veröffentlichung einer Produktneuheit) statt mit kontinuierlichen Sicherheitsüberlegungen verbunden.

Verdächtige Domänenregistrierungen und Schutzregistrierungen von Markendomänen im Vergleich (seit Jahresbeginn 2017)

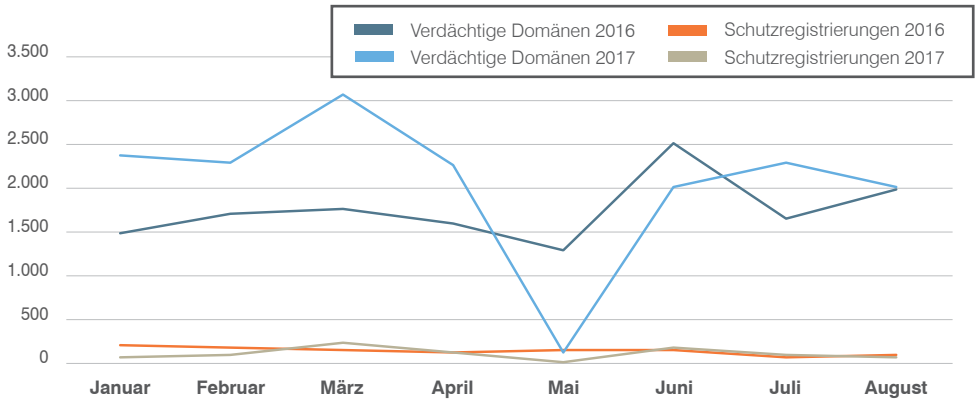

Abb. 11: Jahresvergleich (jeweils 1. bis 3. Quartal 2016 und 2017) der verdächtigen Domänenregistrierungen und der Schutzregistrierungen für Domänen durch Unternehmen bei Fortune 50-Unternehmen

TRENDS BEI SOCIAL MEDIA

Wichtigste Statistik: Die Zahl betrügerischer Kundendienst-Konten hat sich im Vergleich zum Vorjahresquartal verdoppelt.

Es gibt eine hohe Anzahl und große Vielfalt bei Social-Media-Bedrohungen, die von Malware-Verbreitung bis zu Betrug reichen. Wir gliedern die Vorkommen in zwei Hauptkategorien:

- Betrügerische Kundendienst-Konten für sogenannte Angler-Phishing-Angriffe
- Herkömmliche Phishing-Links, die Benutzer auf Seiten leiten, die Anmeldedaten und persönliche Informationen stehlen sollen

Die Zahl der gefälschten Kundendienst-Konten stieg im Vergleich zum vorherigen Quartal um 5 % und verdoppelte sich gegenüber dem Vorjahr. Phishing-Links zu markeneigenen Social-Media-Konten nahmen im Vergleich zum vorherigen Quartal um 10 % zu (Abbildung 12), ihre Zahl blieb jedoch gegenüber dem Vorjahreszeitraum relativ konstant.

Beide Entwicklungen zusammengenommen deuten auf einen erheblichen Wandel bei Social-Media-Angriffen hin. Während Angreifer mit konventionellem Phishing auf Ereignisse oder saisonale Trends reagieren, konzentrieren sie sich insgesamt mehr auf lukrativeres Angler-Phishing.

Standardmäßiges Anmeldedaten-Phishing per Social Media mag einfacher sein, doch bei gezieltem Angler-Phishing ist die Erfolgswahrscheinlichkeit größer, denn der Angriff fühlt sich für das Opfer legitim an – und erheblich natürlicher als zufällige Links in Kommentaren auf Social-Media-Seiten von Unternehmen.

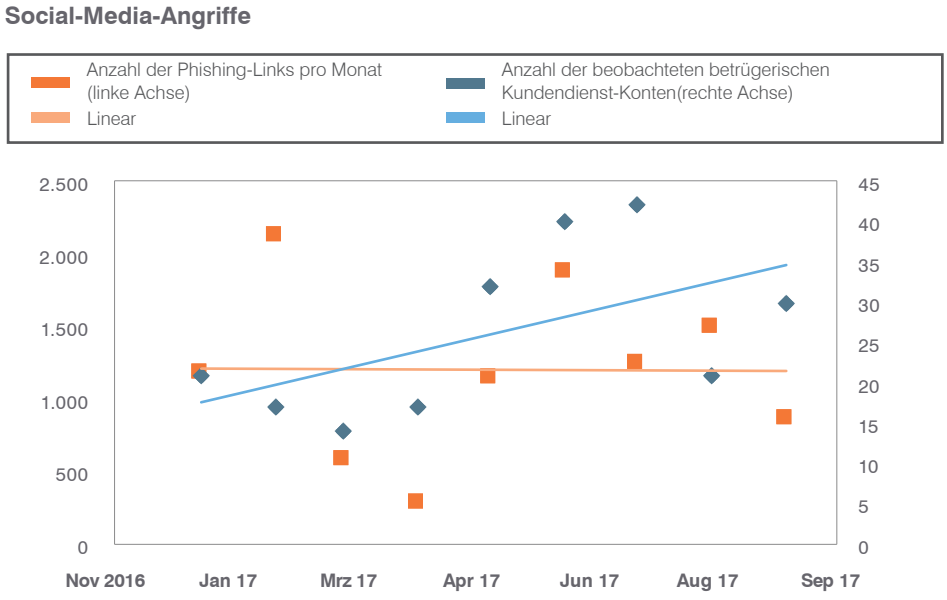

Abb. 12: Relative Aktivitäten im Monat – Vergleich der Trends bei der Verbreitung von Phishing-Links über Social Media und betrügerische Kundendienst-Konten

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 Daten, Ihre Mitarbeiter, Ihre Marke und Ihr Unternehmen in den nächsten Monaten schützen.

Verhindern Sie Typosquatting im Web.
Die Schutzregistrierung von Markendomänen ist eine einfache und kostengünstige Taktik, um Angreifer an der Erstellung von Doppelgänger-Domänen für E-Mail-Betrug und Anmeldedaten-Phishing zu hindern. Arbeiten Sie mit Ihrer Unternehmensführung zusammen, um eine Liste potenzieller Doppelgänger-Domänen für die Registrierung zusammenzustellen. Schließen Sie dabei häufig attackierte Websites zu Konferenz- und Marketing-Kampagnen ein.

Implementieren Sie E-Mail-Authentifizierung, um häufig bei E-Mail-Betrug eingesetzte Domänen-Spoofing-Techniken zu stoppen.
Mit Protokollen wie DMARC (Domain-based Message Authentication, Reporting & Conformance) können Sie Betrüger daran hindern, Ihre E-Mail-Domäne zu missbrauchen. Bei E-Mail-Angriffen mit Doppelgänger-Domänen sollte Ihre Lösung in der Lage sein, Domänen zu finden, die fälschlicherweise als Ihre wahrgenommen werden könnten. Zudem sollten Sie mit externen Dienstleistern zusammenarbeiten, um diese Domänen stillzulegen.

Schützen Sie Ihre Benutzer vor allen Arten von E-Mail-Angriffen.
Ihre E-Mail-Abwehr sollte möglichst alle E-Mail-Bedrohungen abdecken, einschließlich Malware-Anhänge, schädliche URLs oder E-Mail-Betrug per Social Engineering. Zuverlässiger Schutz umfasst zuverlässige Analysefunktionen zur präventiven Identifizierung und Sandbox-Analyse verdächtiger URLs sowie Anhänge. Diese Sandbox-Analyse sollte mehrstufig erfolgen, um schädliche Anhänge sowie URLs zum Zeitpunkt der Übertragung oder beim Klicken zu identifizieren. Ebenso sollte sie Bedrohungen identifizieren und blockieren können, die keine Malware-Komponenten enthalten. Dazu gehören zum Beispiel E-Mails, die Mitarbeiter zum Überweisen von Geldbeträgen oder Preisgeben sensibler Informationen an Betrüger verleiten sollen.

Arbeiten Sie mit einem Anbieter für Bedrohungsdaten zusammen.
Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Nutzen Sie eine Lösung, die Analyse- und Bedrohungsdaten kombiniert und mithilfe statischer sowie dynamischer Techniken Angriffs-Tools, -Taktiken und -Ziele aufdeckt und daraus Erkenntnisse zieht. Durch die Korrelation der Analyseergebnisse mit Bedrohungsdaten-Feeds können diese schwer zu entdeckenden E-Mails identifiziert werden, bevor die Benutzer darauf klicken können.

Schützen Sie Ihre Marke in sozialen Netzwerken vor Betrügern.
Entscheiden Sie sich für eine Sicherheitslösung, die Sie benachrichtigt, sobald Doppelgänger-Konten auf Social-Media-Websites entdeckt werden. Hierbei sollte der Fokus auf betrügerischen „Kundendienst"-Angeboten liegen. Die Lösung sollte nicht nur betrügerische Konten erkennen, sondern auch mit Dienstleistern zum Stilllegen von Domänen zusammenarbeiten, damit Sie Ihre Kunden und Partner vor Betrug schützen können.

Aktuellste Bedrohungsdaten und Erkenntnisse finden Sie im Proofpoint Threat Insight-Blog 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

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern.
Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.