proofpoint™

JULI – SEPT 2016

3. QUARTAL 2016

In der vierteljährlichen Zusammenfassung der Bedrohungen von Proofpoint werden Trends und Veränderungen erfasst, die wir bei unseren Kunden und im breiteren Sicherheitsmarkt beobachten. Tagtäglich analysieren wir mehr als 1 Milliarde E-Mail-Nachrichten, Hunderte von Millionen Social-Media-Beiträge und über 150 Millionen Malwarebeispiele, um Organisationen vor komplexen Bedrohungen zu schützen. Dies bietet uns einen einzigartigen Blickwinkel, von dem aus wir Daten und Trends über die ganze Bedrohungslandschaft hinaus erkennen können.

Wir analysieren die Veränderungen dieser Bedrohungen von Vierteljahr zu Vierteljahr, was uns dabei hilft, größere Trends zu identifizieren und Unternehmen mit umsetzbaren Informationen und Ratschlägen zur Verwaltung ihrer Sicherheitsinfrastrukur zu rüsten. Wir beobachten weiterhin hochentwickelte Bedrohungen über drei primäre Vektoren hinweg: E-Mail, Social Media und Mobilgeräte.

WICHTIGE SCHLUSSFOLGERUNGEN: DER STURM NACH DER RUHE

Cyber-Bedrohungen haben sich im dritten Quartal dramatisch geändert, nachdem die relative Ruhe im zweiten Quartal zu einer explosionsartigen Zunahme der Menge der Kampagnen wie auch der Vielfalt der Bedrohungen führte. Angreifer erweiterten ihre Fähigkeiten, Attacken zielgerichtet auszuführen und herkömmliche Cyberabwehren zu umgehen. Spitzenvolumen und neue Formen der Ransomware verbreiteten sich wie Lauffeuer. Gleichzeitig vermehrte sich die Malware, die für den Diebstahl von Bankkontenangaben entwickelt wurde, rasant und führte maßgeschneiderte Angriffskampagnen aus.

Während Benutzer weiterhin in Scharen zu den Social Media und Mobilgeräten strömten, folgten ihnen die Angreifer – und verwenden oft beide Technologien zusammen. Cyberverbrecher stützten sich auf populäre Marken und Apps, um Personen dazu zu verleiten, Malware herunterzuladen und Anmeldeinformationen offenzulegen.

Nachstehend finden Sie einige Schlussfolgerungen des Quartals.

E-MAIL- UND EXPLOIT-KITS

- **Der Umfang der schädlichen E-Mails, die JavaScript-Anhänge verwendeten, stieg gegenüber dem 2. Quartal um 69 % auf ihr bisher höchstes Niveau an.** Neue Kampagnen mit unterschiedlichen Anhangstypen brachen alle Rekorde des 2. Quartals mit einer Spitze von Hunderten von Millionen Nachrichten pro Tag. Weiterhin führten JavaScript-Anhänge diese extrem umfangreichen E-Mail-Kampagnen an, wobei Locky-Ransomware-Akteure auch neue Arten von Dateianhängen einführten – aller Wahrscheinlichkeit nach, um die herkömmlichen Sicherheitsvorkehrungen zu umgehen. JavaScript-Anhänge, häufig als andere Anhangtypen getarnt, können Benutzer verwirren und sind deshalb speziell wirksam in E-Mail-Angriffen.

- **Die meisten E-Mails mit schädlichen Dokumentenanhängen enthielten den Ransomware-Stamm Locky.** Unter den Milliarden von Nachrichten, die schädliche Dokumentenanhänge verwendeten, enthielten 97 % Locky-Ransomware. Das ist ein Anstieg von 28 % gegenüber dem 2. Quartal und 64 % gegenüber dem 1. Quartal, als Locky entdeckt wurde. Wie andere Varianten von Ransomware verschlüsselt Locky die Daten des Opfers und verlangt eine Zahlung, um sie zu entsperren.

- **Eine Vielfalt neuer Ransomware-Varianten vermehrte sich im 4. Quartal 2015 um das Zehnfache.** Die Auswahl an Ramsonware stieg weiterhin an, vor allem die Varianten, die mit Exploit-Kits (EK) geliefert wurden. Unter diesen mit EK verteilten Varianten sowie in kleineren E-Mail-Kampagnen blieb CryptXXX die dominante Ransomware-Nutzlast, die selbst in Spam-Kampagnen auftrat. Ransomware kann störend und teuer sein, vor allem, weil die neuen Varianten die Erkennung erschweren.

- **Cyberkriminelle verfeinern ihre Methoden in BEC(Business Email Compromise)-Angriffen ständig.** Die Betrüger geben sich in BEC-Angriffen als hochrangige Führungskräfte aus, um die Mitarbeiter dazu zu bringen, Geld zu überweisen. „Beantworten"-Manipulationen haben sich seit Jahresbeginn 2016 ungefähr um 30 % vermindert, während „Anzeigename"-Manipulationen anstiegen und ca. ein Drittel aller BEC-Angriffe ausmachten.[1]Die Verschiebung zeigt, dass die Angreifer ihre Methoden weiter ausbauen und anpassen. Keine davon haben jedoch das „übliche" Phishing ersetzt, das auch immer raffinierter wird. BEC und viele Phishing-Angriffe verwenden keine bösartigen Anhänge, verlassen sich stattdessen auf Social Engineering, was die Entdeckung mit herkömmlichen Sicherheitstools besonders schwierig macht.

1 Bei der Manipulation der Antwortadresse sind der Name im „Von"-Feld, die Adresse und der Name im Antwortfeld legitim, die Antwortadresse hingegen ist die des Betrügers. Opfer, die die Abweichung nicht bemerken, denken, dass sie der richtigen Person eine E-Mail senden. Die Manipulation des Anzeigenamens beruht auf einer ähnlichen Unaufmerksamkeit: der Name im „Von"-Feld ist legitim, aber die Adresse im „Von"-Feld ist die des Betrügers.

- **Banking-Trojaner wurden abwechslungsreicher und personalisierter.** Nach einer Periode relativer Ruhe tauchte der populäre Banking-Trojaner Dridex wieder in größeren Kampagnen auf. Dridex war in kleineren und gezielten Kampagnen im 2. Quartal aufgetreten. Andere Banking-Trojaner, wie z. B. Ursnif, traten in stark personalisierten Kampagnen ebenfalls auf und beliefen sich auf Hunderte von Tausenden von Nachrichten, ein Trend, der im 2. Quartal begann und sich bis ins 3. Quartal fortsetzte. Gleichzeitig wurden auch vielfältige Banking-Trojaner in Malvertising – bösartiger in Online-Anzeigen eingebetteter Code – verwendet oder von EKs in anderen browserbasierten Angriffen abgelegt. Diese großen, aber sehr zielgerichteten Kampagnen sind ohne intelligenten Schutz schwer zu ermitteln.
- **Die Exploit-Kit-Aktivität ist zwar stabil, bleibt jedoch weit unter den Spitzen von 2015.** Die insgesamt beobachtete EK-Aktivität fiel im 3. Quartal um 65 % im Vergleich zum 2. Quartal und seit ihrem Hoch im Januar 2016 um 93 %, doch der Abrutsch scheint sich ausgeglichen zu haben. Da nun der einst populäre Angler verschwunden ist, wich Neutrino im Verlauf des 3. Quartals RIG als dominantem EK. Die Veränderung deutet auf eine größere Anzahl und Vielfalt von Exploit-Kits hin, was eine Herausforderung für die Cybersicherheitstools bedeuten könnte.

MOBILE

- **Pokémon GO-bezogene Malware brachte bösartige Fälschungen hervor.** Malware in Form von schädlichen „Side-Loaded“ Klon-Apps, gefährlichen Add-ons und anderen riskanten Apps ist nicht mehr so populär. Benutzer können Apps von überall herunterladen und selbst die großen App-Stores bieten nur begrenztes Screening von Apps und Aktualisierungen an. Das bedeutet, dass viele Benutzer keine Ahnung haben, ob die Apps, die sie herunterladen, wirklich sicher sind.
- **Mobile Exploit-Kits und Zero-Day-Angriffe attackierten iOS und Android.** Die meisten Mobilgeräte haben heute 10 – 20 nutzbare Zero-Days. Ungefähr 30 % davon sind schwerwiegend und könnten Angreifern gestatten, schädlichen Code auf infizierten Geräten auszuführen. Da viele Geräte am Arbeitsplatz den Mitarbeitern gehören, haben die meisten Unternehmen wenig Einblick in die mobilen Bedrohungen in ihrer Umgebung.

SOCIAL MEDIA

- **Negativer Inhalt hat sich vermehrt.** Negative bzw. potenziell schädliche Inhalte wie Spam, obszöne Ausdrücke und Pornografie sind im 2. Quartal um 50 % angestiegen. Wenn diese Art von Inhalt auf dem Social-Media-Konto einer Marke erscheint oder von einem Schwindler eingerichtet wurde, dann ziehen die Kunden ab.
- **Social-Phishing hat sich seit dem 2. Quartal verdoppelt.** Social Media sind die Brutstätte für Daten- und Finanz-Phishing, wobei Angreifer die Benutzer sozialer Medien dazu verleiten, ihre Anmeldedaten zu übermitteln. Betrügerische Konten, die für Angriffe verwendet wurden, die wir Angler-Phishing nennen, waren die Vorreiter. Da diese Angriffe auf Social-Media-Netzwerken stattfinden, weit außerhalb der Netzwerkparameter und nicht auf Konten, die dem Unternehmen gehören, können herkömmliche Sicherheitstools sie nicht sehen.
- **Die Kreuzung zwischen mobilen und Social-Media-Bedrohungen ist im Kommen.** Phänomene mit hohem Stellenwert wie die Olympischen Spiele in Rio und Pokémon GO schufen Möglichkeiten, mobile Malware zu verbreiten, einschließlich Zero-Day-Exploits über Social Media. Herkömmliche Sicherheitstools haben wenig Einblick weder in den einen noch den anderen Kanal.

SPITZENBEDROHUNGEN UND TRENDS, JULI – SEPTEMBER 2016

Einige der Trends, die wir im zweiten Quartal hervorgehoben haben, haben sich im dritten Quartal forgesetzt, mit einigen beachtenswerten Ergänzungen. Das Volumen der großen E-Mail-Kampagnen, vor allem jene, die Locky verteilen, stieg weiterhin an. Gleichzeitig setzte sich die explosionsartige Ausbreitung der neuen Arten von Ransomware fort. Bösartige Anhänge blieben der dominante Vektor für E-Mail-basierte Bedrohungen. Wir begannen das erneute Auftauchen der großen URL-basierten Kampagnen, die direkt auf gehostete Malware zeigen, festzustellen. Die Exploit-Kit-Aktivität blieb in der Nähe des Niveaus vom Juni. RIG war nun der hauptsächliche EK-Akteur.

Tägliche massive Kampagnen und viel beachtete Ransomware-Infektionen dominierten die Schlagzeilen in der ganzen ersten Hälfte des Jahres. Bedrohungsakteure verwendeten auch weiterhin E-Mail, um Beachheads für Advanced Persistent Threats (APTs) einzurichten und zielgerichtete Angriffe auszuführen. Sobald Malware über E-Mail bereitgestellt wird, öffnet sie großen Paydays und weiteren Angriffen die Tür.

Volumentrends: Locky-Kampagnen machen das 3. Quartal zum Mount Everest von 2016 ... bis jetzt jedenfalls

Zwar hat sich das Volumen Ende 3. Quartal verringert, aber Locky bleibt ein lukrativer und erfolgreicher Malwarestamm. Es ist daher kein Wunder, dass er weiterhin von mehreren Angreifern weltweit über E-Mail verteilt wird. Das massive Volumen der Nachrichten und sich ändernde Anhangtypen sind große Hürden für jemanden, der zu verhindern versucht, dass sie die Benutzer erreichen.

Wichtige Statistiken: Nachrichten, die Locky verteilten, machten 97 % der bösartigen Nachrichten im 3. Quartal aus.

Analyse: Die Locky-Ransomware dominierte die bösartigen Nachrichten-Nutzlasten im 3. Quartal vollständig. Sie erschien in 97 % der Nachrichten. Nur im August allein betrugen die Locky verbreitenden Nachrichten wie auch die Menge der allgemeinen bösartigen Nachrichten 63 % des ganzen Quartals. Nachrichten, die Malware über schädliche Dokumentenanhänge verbreiteten, stiegen um 184 % im Vergleich mit dem 2. Quartal, machten jedoch nur 25 % der gesamten Menge der bösartigen Nachrichten aus. Stattdessen verbreiteten immer mehr Nachrichten Locky über gezippte JavaScript-Dateien (ein Trend, den wir auch im 2. Quartal beobachteten) sowie über angehängte .hta (ausführbare HTML-Dateien) und .wsf (Windows-Skriptdateien).

Im September verringerte sich die Menge an Nachrichten bedeutend. Wie in Abbildung 1 zu sehen ist, begann der Monat stark. Angriffskampagnen gehörten zu den größten, die wir je beobachtet hatten, mit einer Spitze von Hunderten von Millionen Nachrichten an einem einzigen Tag. Aufgrund eines nachfolgenden Rückgangs blieb das Gesamtvolumen des Monats unter den Spitzen im August. Zusätzlich zu den Änderungen in der Verteilungsmethode erlebte auch Locky mehrere Aktualisierungen, einschließlich neuer Erweiterungen für verschlüsselte Dateien.

Indiziertes Volumen schädlicher Angriffe nach Angriffstyp, 2016 seit Jahresbeginn

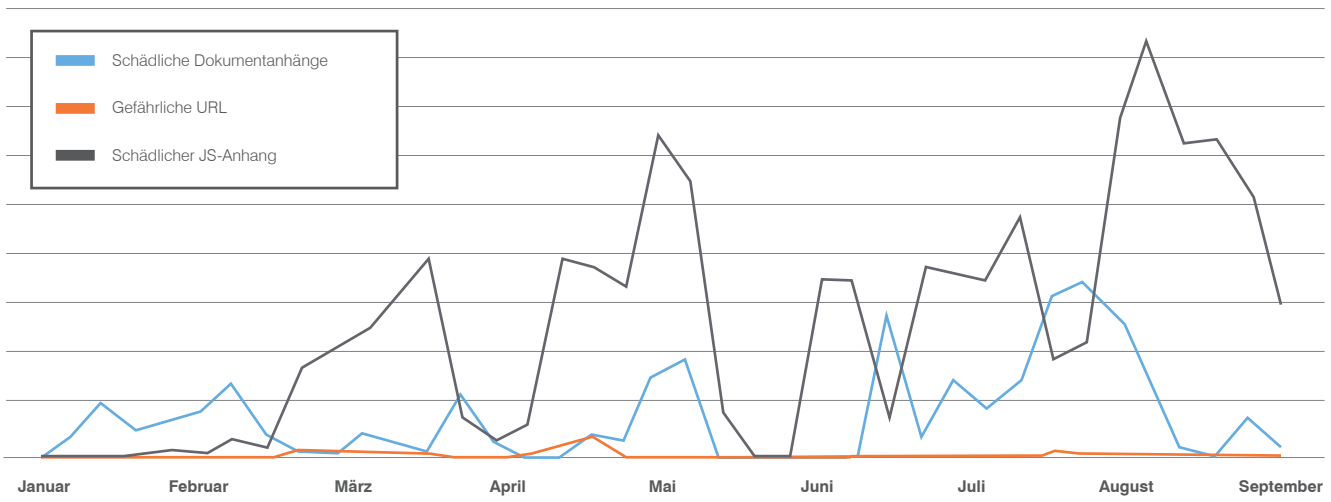

Abbildung 1: Wöchentliche schädliche Nachrichten nach Angriffstyp seit Jahresbeginn

Während Locky alle anderen Arten der per E-Mail verteilten Malware in den Schatten stellte, war es der einzige Ransomware-Stamm in den obersten fünf Malwaretypen, wie in Abbildung 2 angezeigt. Die restlichen vier sind alles Banking-Trojaner, oder, im Falle von Pony, Zwischenladeprogramme, die mit den Banking-Trojanern verbunden sind.

Die schädlichsten Malware-Nutzlasten in Prozenten des gesamten Nachrichtenvolumens, Juli bis September 2016

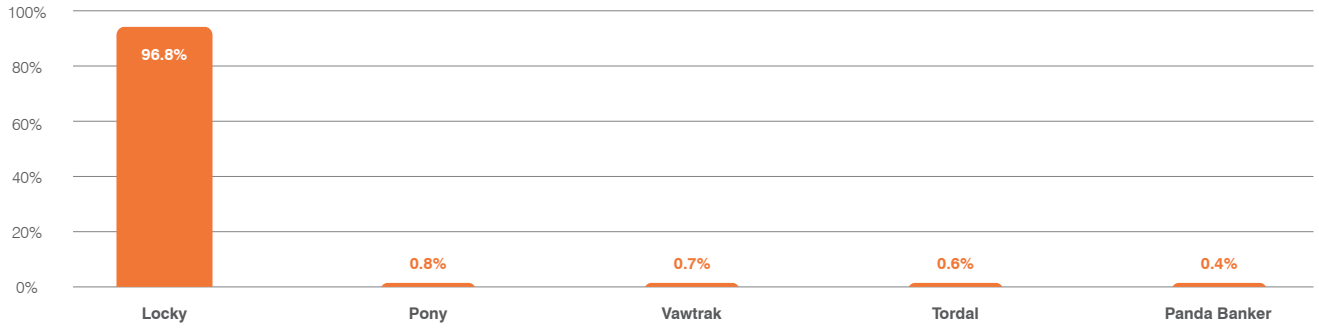

Abbildung 2: Die schädlichsten Malware-Nutzlasten, die im 3. Quartal über E-Mail verbreitet wurden

Ransomware: Entweder alles oder gar nichts

Ransomware kann teuer sein. Das FBI meldete, dass Kriminelle im ersten Quartal von 2016 209 Millionen US-Dollar an Ransomware-Zahlungen einnahmen, wobei geschätzt wird, dass die Zahlungen bis Ende Jahr 1 Milliarde US-Dollar betragen werden. Die unmittelbaren Kosten der hohen Lösegelder, um Daten wiederherzustellen, können bedeutend sein. Noch größere indirekte Verluste stammen oft von der Systemausfallzeit und den verlorenen Geschäften, selbst wenn ein robustes Backupsystem vorhanden ist, mit dem Daten ohne Bezahlung eines Lösegeldes wiederhergestellt werden können.

Wichtige Statistiken: Beobachtete Ransomware-Familien nahmen im 3. Quartal im Vergleich mit dem 2. Quartal um 53 % zu und wuchsen um das Zehnfache seit 2015.

Analyse: Im Verlauf des 3. Quartals blieb Ransomware eine dynamische Bedrohung. Mehrere neue Ransomware-Familien traten auf und das Volumen wuchs weiterhin. Andere Familien verschwanden gänzlich. Noch andere blieben erfolglos. Schließlich waren Locky und CryptXXX die zwei dominanten Ransomware-Familien. Die Verbreitung von Locky geschah hauptsächlich mit E-Mail und diejenige von CryptXXX über EKs.

Die Störung des Necurs Botnet im Juni brachte die Nachrichtenmenge im 2. Quartal zum Austrocknen. Locky tauchte jedoch im 3. Quartal wieder im großen Stil auf und führte zu einem um 370 % größeren Nachrichtenvolumen im Vergleich mit dem 2. Quartal und erschien in mehreren groß angelegten Kampagnen.

Im 3. Quartal setzte sich der Trend der Überlieferung von Locky mittels JavaScript-Anhängen fort. Die Menge schädlicher JavaScript-Anhängen wuchs um 69 % von Quartal zu Quartal. Drei Bedrohungsakteure begannen Instanzen von Locky zu versenden, die auch „offline“ funktionierten. Diese Varianten verschlüsselten infizierte Geräte, ohne dass sie zuerst in einen C&C(Command-and-Control)-Server übertragen wurden.

Locky war die am meisten verbreitete E-Mail-Bedrohung. Andere Ransomware-Varianten erschienen ebenfalls in groß angelegten Kampagnen, unter anderem CryptFile2, MarsJoke und Cerber. MarsJoke war für die Verwendung von schädlichen online gehosteten Dokumenten bekannt – sie wurde über URLs anstelle von direkten E-Mail-Anhängen übermittelt. Diese Änderung schien ein wachsender Trend zu sein. Petya Ransomware tauchte Ende des Quartals ebenfalls wieder auf. Dies ist eine der wenigen Varianten, die Datenträgerstrukturen auf einer niederen Ebene angreift und dabei den Master Boot Record (MBR) des Systems anstelle der einzelnen Dateien verschlüsselt. Außerdem wurde die Fähigkeit, Netzwerklaufwerke zu entdecken und zu verschlüsseln, die Standardfunktion vieler Ransomware-Varianten, was die Bedrohung für Opfer zusätzlich vergrößerte.

Abbildung 3 zeigt das rapide Wachstum der Ransomware-Varianten seit Ende 2015 – eine beinahe zehnfache Steigerung. Obwohl wir glauben, dass die Hälfte der Ransomware-Familien inaktiv sind, weist der Wachstumstrend darauf hin, dass die alten Familien kontinuierlich durch neue Varianten ersetzt werden. Es ist verlockend zu glauben, dass diese älteren Varianten, die sich nicht länger bemerkbar machen, entweder deaktiviert oder ausgeschieden sind. Die Erfahrung zeigt jedoch, dass Angreifer leicht „alte“ Malware reaktivieren, manchmal mit kleineren oder sogar ohne Updates, oder Code in neuen Varianten wiederverwenden können.

Wachstum der Ransomware-Varianten seit Dezember 2015

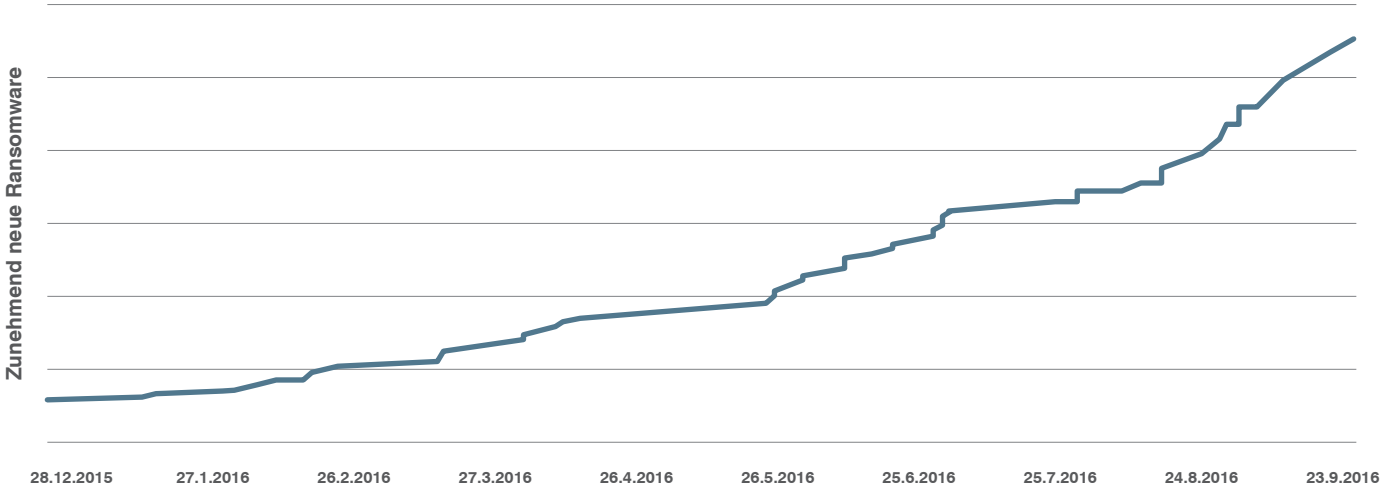

Abbildung 3: Indiziertes Wachstum der Ransomware-Familien seit Dezember 2015

BEC passt die Taktiken an, während generisches Phishing ebenfalls cleverer wird.

Die Herausforderungen der massiven Nachrichtenmenge werden noch verstärkt duch die sich schnell verändernden Bedrohungen und durch erweiterte Methoden, die über Malware hinausgehen. Ein typisches Beispiel: BEC. Diese sorgfältig geplanten, per Social Engineering ausgeführten Angriffe richten sich auf einzelne große Payouts. Manuelle Sicherheitsvorkehrungen und regelmäßige Updates genügen nicht, um diese dynamischen, schwer identifizierbaren Bedrohungen anzugehen. Stattdessen erfordern sie skalierbare, automatisierte Verteidigung gegen BEC und andere fortgeschrittene E-Mail-Bedrohungen. Groß angelegte Anmeldeinformationen-Phishing-Kampagnen entwickeln sich ebenfalls. Ohne automatisierte Abwehr sind sie schwierig zu erkennen. Die Zeit der schwerfälligen „419"-Schemen ist vorbei. Die heutigen Phishing-Attacken sind hochentwickelte, durch Social Engineering ausgeführte Anschläge.

Wichtige Statistiken: Die Manipulationen des Anzeigenamens sind angestiegen und betreffen nun beinahe 1 in 3 BEC-Nachrichten.

Analyse: Manipulation der Antwortadresse – in der das „Von"-Feld legitim ist, aber die „Antwort"-Adresse dem Angreifer gehört – wurde mehr als 2-mal so oft verwendet wie die Manipulation des Anzeigenamens. Dies stellt eine leichte Veränderung von dem 3:1-Verhältnis dar, das wir im Bericht Der Faktor Mensch 2016 bekanntgaben. Die Manipulation des Anzeigenamens erscheint inzwischen in beinahe einer von drei BEC-Nachrichten. Diese Verschiebung deutet darauf hin, dass BEC-Betrüger ihre Taktik ändern, weil Personen und Unternehmen solche Angriffe schneller erkennen.

Die Betreffzeile, die am meisten in BEC-Angriffen verwendet wurde, war erneut „Anfrage". Die wichtigsten fünf Betreffzeilen machen mehr als 20 % aller beobachteten BEC-Betreffzeilen aus. Zwar haben Angreifer einige klare Favoriten, sie verwenden jedoch eine Vielfalt von Betreffzeilen. Abbildung 4 zeigt die relative Anzahl der Top-Betreffzeilen im Zusammenhang mit BEC-Phishing-Versuchen vom Juli bis September 2016.

Top 10 BEC-Betreffzeilen in Prozenten der Gesamtmenge

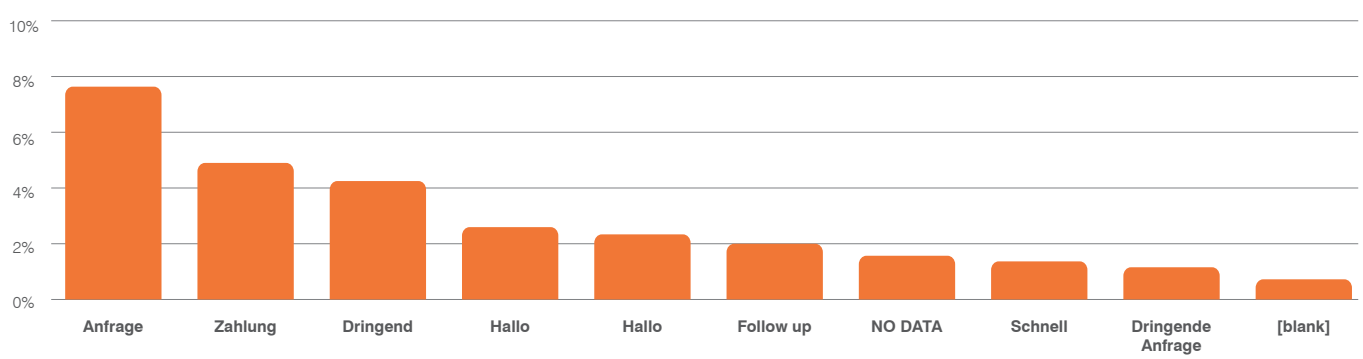

Abbildung 4: Top 10 BEC-Betreffzeilen in Prozenten der gesamten beobachteten Vorfälle, Juli bis September 2016

BEC und ähnliche Instanzen des E-Mail-Betrugs erscheinen aufgrund des Ausmaßes der Verluste in den Schlagzeilen und führen zu Warnungen des FBI. Das herkömmliche Phishing wird jedoch immer raffinierter und ist noch immer weit verbreitet. Wir beobachten regelmäßig Kampagnen, die Social Engineering und sorgfältig gestaltete Seiten kombinieren, die Websites der Banken, Online-Dienste, Social-Media-Anmeldedaten und mehr nachahmen. Die meisten sind dazu bestimmt, Anmeldeinformationen zu erfassen. Andere stehlen womöglich detailliertere Bank- oder Kontoinformationen. Ob BEC oder allgemeineres, weniger zielgerichtetes Phishing, der potenzielle Schaden für Einzelpersonen und Unternehmen reicht von Identitätsdiebstahl bis hin zu bedeutenden direkten finanziellen Verlusten.

Banking-Trojaner diversifizieren

Die Menge der Banking-Trojaner-Kampagnen ist geschrumpft mit dem Wechsel zu groß angelegten Ransomware-Kampagnen im E-Mail-Bereich. Banking-Trojaner sind jedoch weiterhin eine ernsthafte Bedrohung und verursachen Verluste von Milliarden US-Dollar. Mit verbesserten Ziel- und Umgehungsmethoden und besseren Fähigkeiten, Informationen zu stehlen, könnten sie für Unternehmen mit fehlendem intelligenten Schutz eine ernsthafte Gefahr bedeuten.

Wichtige Statistiken: Banking-Trojaner machten in diesem Quartal nur ungefähr 3 % aller E-Mail-basierten Bedrohungen nach Nachrichtenvolumen aus. Diese Arten von Malware waren jedoch zunehmend zielgerichtet und wurden mit personalisierten Methoden und evasiven Makros versandt.

Analyse: Da groß angelegte bösartige E-Mail-Kampagnen ihren Schwerpunkt auf die Verteilung von Ransomware verlegten, tauchten die einst allgegenwärtigen Banking-Trojaner in kleineren Mengen und zunehmend personalisierten Kampagnen auf, ein Trend, den wir zuerst im 2. Quartal beobachteten. Diese Trojaner wurden auch gemäß unseren Beobachtungen sehr häufig in massiven Malvertising-Verfahren verwendet und in Exploit-Kits und mit differenzierter Zielausrichtung bereitgestellt.

Ohne die einseitige Dominanz von Dridex, die wir 2015 und im ersten Quartal von 2016 beobachteten, zeigten Banking-Trojaner ebenfalls eine größere Vielfalt. Dridex stieg in verschiedenen personalisierten Kampagnen sprunghaft an. Gleichzeitig beobachteten wir auch Ursnif, Panda Banker, Zeus, Gootkit, Cthonic und mehrere andere Banking-Trojaner in regionalen Angriffen. Zwei Trends ergaben sich aus diesen Kampagnen.

Erstens fügen Trojaner selbst mehr Funktionen hinzu. Dazu gehören:

- Die Fähigkeit, zusätzliche Anmeldeinformationen und andere Angaben zu stehlen
- Kommunikation mit C&C-Infrastruktur über das Tor-Netzwerk, wodurch sie möglicherweise noch schwieriger zu erkennen sind

Zweitens verwenden Bedrohungsakteure, die die Banking-Trojaner verbreiten, ausgefeiltere Methoden. Hier einige Beispiele:

- Verwendung von Verteilungsmethoden, die nicht erkannt werden
- Einbauen der Ausweichtechniken in Makros
- Verwendung von unauffälligen Exploits und Stenografien
- Kooptierung von vertrauenwürdigen Drittanbietern wie PayPal
- Verbessern der Zielausrichtung

Angesichts der Tatsache, dass ihre „Web-Injektionen“ für spezifische Banken konfiguriert werden müssen, erfordern Banking-Trojaner immer ein gewisses Maß an regionaler Zielausrichtung. In letzter Zeit haben wir jedoch eine noch stärkere Regionalisierung festgestellt. Ursnif ist zum Beispiel stark auf Australien ausgerichtet und Gootkit verbreitet sich vor allem in Zentral- und Südeuropa (Deutschland, Italien, Frankreich).

Exploit-Kits: Wo sind sie alle geblieben?

Unternehmen sollten in der Lage sein, Bedrohungen von einer größeren Anzahl und Vielfalt von Exploit-Kits zu überwachen. Kleinere, wettbewerbsfähigere Malvertising- und „Drive-By-Download“-Märkte zwingen Angreifer, Neuerungen vorzunehmen und um den Marktanteil zu kämpfen. Gleichzeitig sollten Unternehmen in Asien aufgrund der Malvertising-Kampagnen, die besonders auf Opfer in asiatischen Ländern ausgerichtet sind, ihre Abwehrmaßnahmen prüfen, um sicherzustellen, dass sie für den neuen geografischen Fokus gerüstet sind. Sie müssen vor allem in der Lage sein, den Verkehr für neue auf Asien bezogene Exploit-Kit-Varianten erkennen zu können.

Wichtige Statistiken: Die gesamte Exploit-Kit-Aktivität fiel im 3. Quartal um 65 % im Vergleich mit dem 2. Quartal und um 93 % von Januar (dem aktivsten Monat im Jahr 2016) bis September.

Analyse: Nachdem das Neutrino EK scheinbar im Begriff war, an die Stelle von Angler zu treten, verblasste es im 3. Quartal. RIG dagegen eroberte sich einen weiteren Platz auf dem Markt und wuchs von 5 % bis auf 50 % des beobachteten Exploit-Kit-Verkehrs. Diese Veränderungen finden jedoch vor dem Hintergrund eines viel kleineren Gesamtverkehrsvolumens statt. Während sich die Gesamtmenge im 3. Quartal anscheinend stabilisiert hat, ist sie 93 % niedriger als diejenige, die wir in den ersten drei Monaten in 2016 festgestellt haben.

Groß angelegte Malvertising-Kampagnen 2015 und anfangs 2016 – veranschaulicht durch die AdGholas-Kampagne – sind kleineren Kampagnen und einem Wechsel in der geografischen Ausrichtung gewichen. Die weit verbreiteten Malvertising-Kampagnen, die wir beobachten, zielen auf Opfer in den asiatischen Ländern hin. Beispiele sind u. a. Magnitude, GooNky und eine Variante von Neutrino. Dieser regionale Wechsel ist wenigstens teilweise das Ergebnis der Bemühungen, der Entdeckung und Preisgabe auf Online-Werbenetzwerken zu entgehen. In gewissen Fällen enthalten die Kampagnen spezifische Funktionen oder Varianten für Asien.

Das Verschwinden von wichtigen Akteuren und die allgemeine Einschränkung des Raums hat das Feld gestört. Während die restlichen Akteure sich bemühen, den Marktanteil zu behalten, tauchen neue Varianten der wichtigen Exploit-Kits wie RIG und Neutrino auf. Angreifer, die früher andere EKs verwendet haben, bauen nun ebenfalls neue Kits auf.

Gleichzeitig bleiben kleinere EKs wie Sundown aktiv und gewisse ältere und weniger auffällige Kits kommen erneut zum Vorschein. Das Ergebnis: ein stärker wettbewerbsorientiertes Umfeld.

Wichtigste Exploit-Kit-Aktivität in Prozenten der Gesamtmenge, Juni bis September 2016

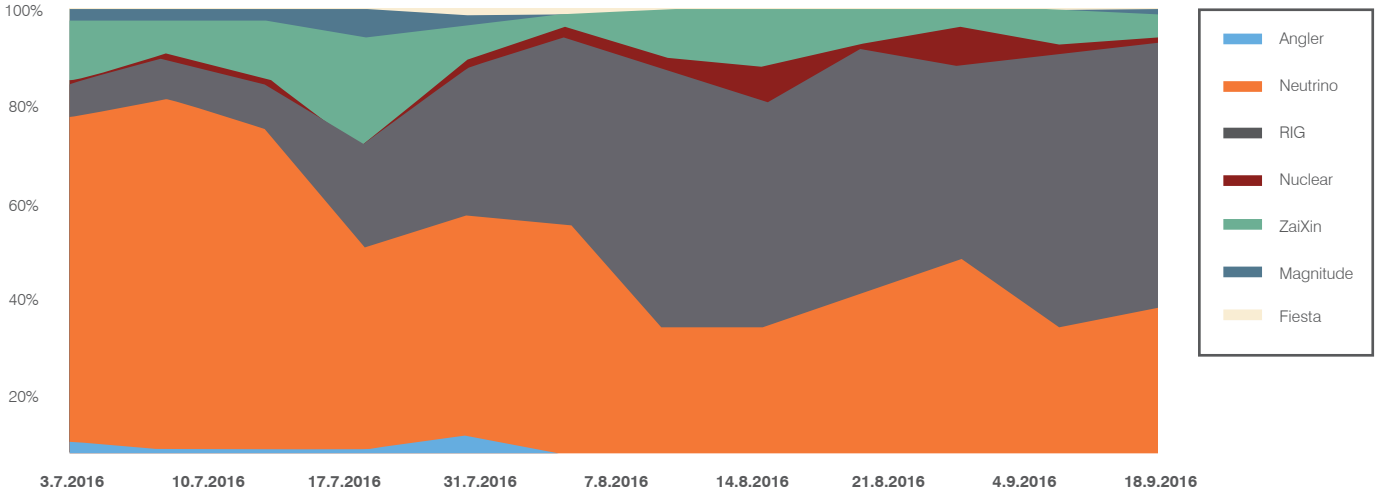

Abbildung 5: Wichtigste Exploit-Kit-Aktivität in Prozenten des gesamten beobachteten EK-Verkehrs, Juli bis September 2016

Indizierter Trend der wichtigsten Exploit-Kit-Aktivitäten, seit Beginn des Jahres 2016

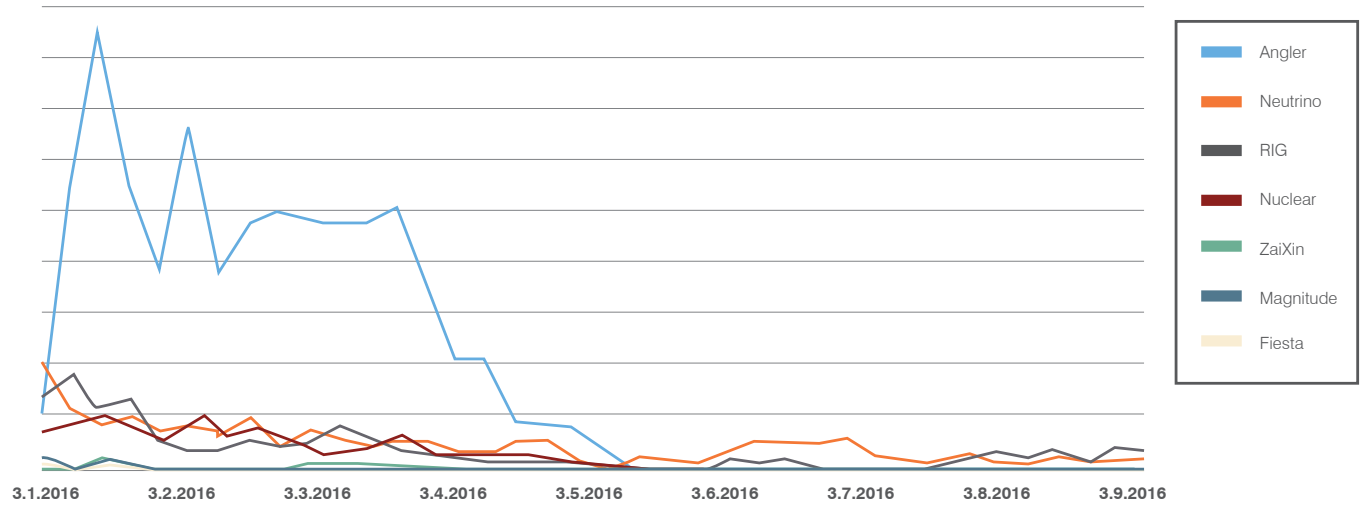

Abbildung 6: Indizierter Trend der wichtigsten beobachteten Exploit-Kit-Aktivitäten, Juli bis September 2016

Mobile-App-Bedrohungen: Kein Spielzeug!

Pokémon GO ist ein spektakuläres Beispiel einer App, deren Beliebtheit ein Ökosystem von mobilen Bedrohungen geschaffen hat. Games wie auch Apps, die mit wichtigen Events verbunden sind, sind Hauptziele. Gewisse Apps sind offenkundig schädlich und andere verursachen Geschäftsrisiken, indem sie übermäßige Berechtigungen verlangen oder Daten schlecht verwalten. Schädliche oder andere riskante Apps folgen Benutzern bis an den Arbeitsplatz, unabhängig davon, ob sie von Mitarbeitern oder ihren Familienmitgliedern heruntergeladen werden.

Wichtige Statistiken: Beinahe 5 % der Mobilgeräte auf Unternehmensnetzwerken führen Pokémon GO aus.

Analyse: Pokémon GO, freigegeben im Juli, wurde unmittelbar zu einer internationalen Sensation. Die gestaffelte internationale Einführung führte bei Benutzern zu einem Nachfragestau und diejenigen, die keinen Zugang zur App über legitime App-Stores hatten, versuchten sie über Drittanbieter und direkte Downloads querzuladen. Innerhalb von drei Tagen nach der Freigabe von Pokémon GO in Australien und Neuseeland, identifizierten wir eine geklonte Version der Android-App in einem Malware-Repository. Die gefälschte Kopie enthielt DroidJack, ein Fernzugriff-Trojaner, der in der Lage war, das Gerät in Besitz zu nehmen und die in Abbildung 7 angegebenen App-Berechtigungen zu modifizieren. Obwohl diese Version von Pokémon GO nicht „in der Wildnis“ beobachtet wurde, zeigte sie doch deutlich, wie leicht Angreifer eine beliebte App modifizieren und eine schädliche Version an Benutzer verteilen können.

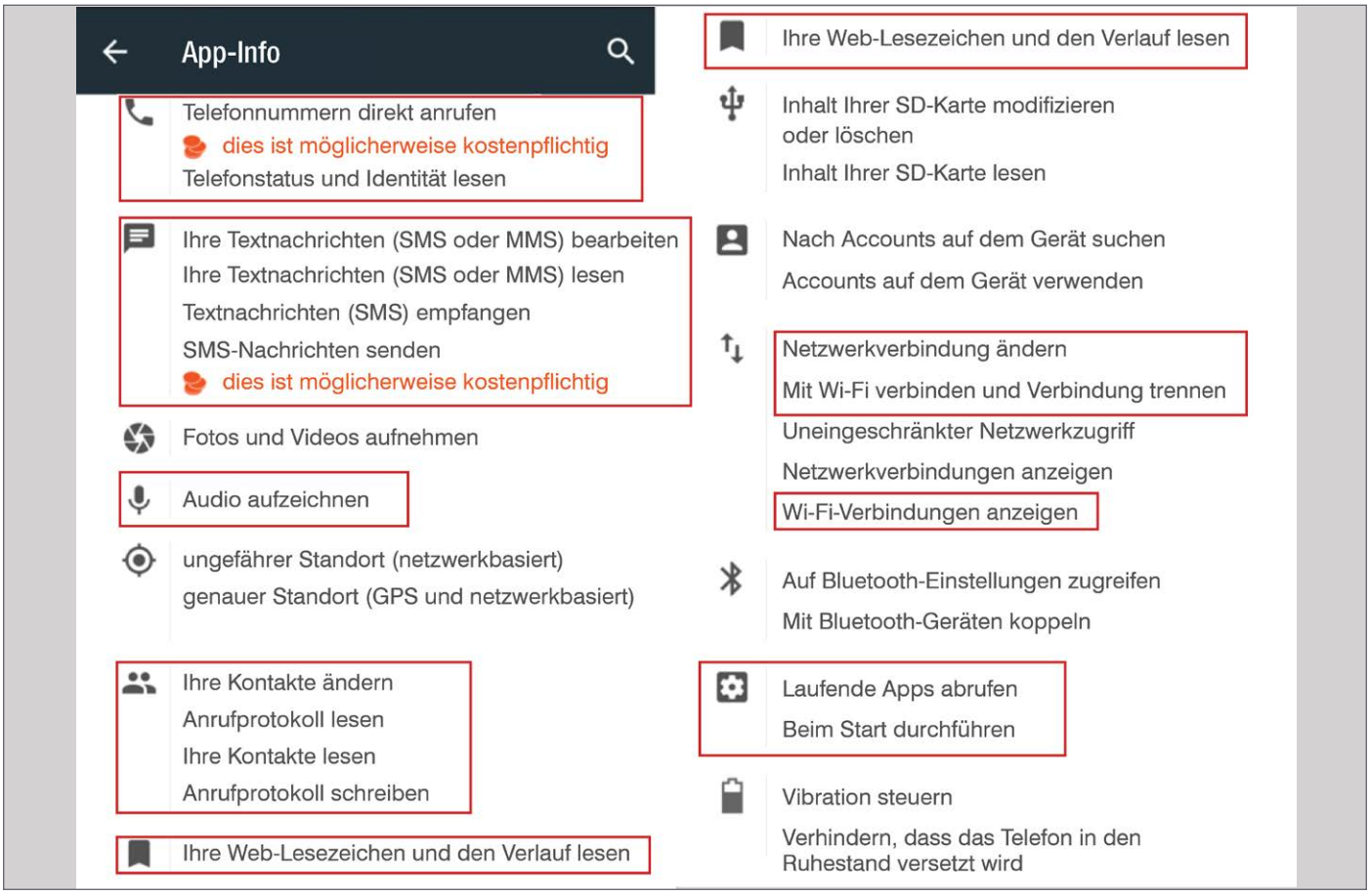

Abbildung 7: Modifizierte App-Zugriffsberechtigungen für betrügerisches Klonen von Pokémon GO

Eine kürzliche Studie hat gezeigt, dass Pokémon GO auf nahezu 5 % aller Mobilgeräte, die Zugriff auf Unternehmensnetzwerke haben, installiert ist. Wie viele populäre Spiele hat Pokémon GO eine Vielzahl von Spielanweisungen, Fälschungen und Add-ons erzeugt. Viele davon sind riskant oder schädlich und können den Angreifern Netzwerkressourcen offenlegen. In diesem Quartal haben wir mindestens drei bösartige Versionen von Pokémon GO zusammen mit mehreren schädlichen Begleit-Apps identifiziert. Sogar unter legitimen Installationen enthielten 4 % der Geräte mit Zugriff auf Unternehmensnetzwerke eine frühe Version des Spiels, die übermäßige Zugriffsberechtigungen gewährte.

Die Olympischen Spiele in Rio zeigten weitere Beispiele, wie Bedrohungsakteure populäre Phänomene für bösartige Zwecke nutzten. Wir identifizierten über 4000 Android-Apps und über 500 iOS-Apps in Verbindung mit der Olympiade, die riskantes oder bösartiges Verhalten zeigten.

Mobile Bedrohungen existieren weiterhin mit Pegasus und anderen Zero-Day-Tools

Die meisten Mobilgeräte enthalten mehrere ernsthafte, ungepatchte Schwachstellen, die die Geräte einer Unzahl von Malware- und Angreifervektoren aussetzen könnten. Dazu gehören Android- wie auch iOS-Geräte. Wenn Mobilgeräte zu den primären Hilfsmitteln der täglichen Arbeit und der Kommunikation werden, können diese Sicherheitslücken ernsthafte Konsequenzen haben. Deshalb benötigen Unternehmen eine dynamische, intelligente Sicherheitsabsicherung und -verwaltung.

Wichtige Statistiken: Das durchschnittliche Mobilgerät hat zwischen 10 bis 20 nutzbare Zero-Day-Schwachstellen.

Analyse: Im August fanden wir heraus, dass das sogenannte „Pegasus Mobile Device Attack Kit" für die Forschungsgemeinschaft, aber auch für die kriminelle Szene verfügbar war. Dieses Kit kann für einen Angriff auf ein beliebiges Gerät mit einer iOS-Version zwischen iOS 7 und iOS 9.3.5. verwendet werden. Obwohl die Malware ursprünglich im Zusammenhang mit einem spektakulären Angriff auf einen politischen Dissidenten in den Vereinigten Arabischen Emiraten auftauchte, kann sie gegen jede Person oder jedes Unternehmen mit einem anfälligen Gerät verwendet werden.

Wie viele andere Arten von Malware für Mobilgeräte und Desktop-Computer kann Pegasus über eine URL mit einem überzeugenden Köder verteilt werden. Da der Link Mobilgeräte anzielt, kann er über SMS, E-Mail, Social Media, bösartige Suchergebnisse oder sogar andere Apps verbreitet werden. Nach der Installation kann Pegasus Schwachstellen in vielen iOS-Versionen ausnutzen. Er versteckt sich im Mobiltelfon und erhält unverschlüsselten Zugriff auf eine Vielzahl von Apps und Kommunikationsfunktionen auf dem Telefon.

Durch die sofortige Bereitstellung eines Updates für iOS von Apple und die erhebliche Aufmerksamkeit, die das Problem in der Öffentlichkeit erregte, konnte das unmittelbare Risiko gemildert werden. Aber Pegasus war nur die bekannteste Art dieser Malware: das durchschnittliche Mobilgerät hat 10 bis 20 nutzbare Zero-Day-Sicherheitslücken, die von mobiler Malware angepeilt werden können. Ungefähr ein Drittel davon sind ernsthafte Fehler, die es Angreifern ermöglichen, bösartigen Code auszuführen. Abbildung 8 zeigt die Anzahl der Sicherheitslücken der mobilen Betriebssysteme, die 2016 bereits geschlossen wurden.

Mobile BS-Sicherheitslücken, die 2016 geschlossen wurden

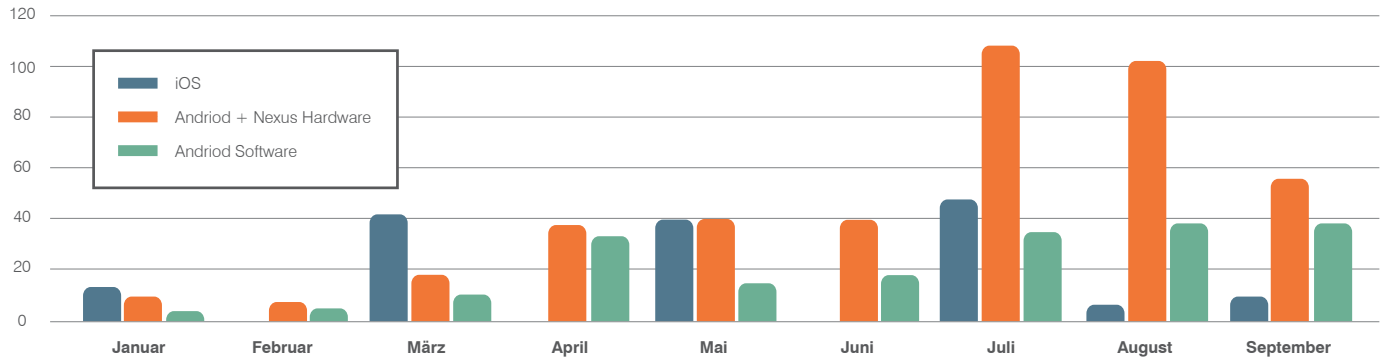

Abbildung 8: Mobile BS-Sicherheitslücken, die 2016 geschlossen wurden

Social Media: Nährboden für Phishing und Malware

Social-Media-Kanäle bieten eine Unmenge von Gelegenheiten für Bedrohungsakteure, um Benutzer, Marken und Unternehmen anzugreifen. Beliebte Trends und Ereignisse leiten den Verkehr zu betrügerischen Webseiten und Konten. Gleichzeitig müssen Unternehmen regelmäßig mit großen Mengen von Spam und bedenklichem Inhalt rechnen. Ungeachtet der zugrunde liegenden Motivation sind die Risiken für Marken wie auch Personen bedeutend und machen sie für Phishing, Malware und für potenzielle Gefahren anfällig.

Wichtige Statistiken: Zwischen dem 2. und 3. Quartal hat sich das soziale Phishing um mehr als 100 % vermehrt

Analyse: Phishing auf Facebook, YouTube, LinkedIn, Twitter und Instagram hat sich im 3. Quartal mehr als verdoppelt im Vergleich zu dem 2. Quartal und hat sich vervierfacht gegenüber dem Jahr zuvor. Dazu gehören sowohl das allgemeine Phishing wie auch das „Angler-Phishing“, bei dem Angreifer falsche Supportkonten verwenden, um Kunden abzufangen, die über ein Social-Media-Konto eines Unternehmens Unterstützung anfordern.

Neben Phishing sind auch Spam, anstößige Sprache und bösartige Links weiterhin ein wichtiger Anteil der sozialen Bedrohungen. Solche Vorfälle haben sich im 3. Quartal um 50 % vermehrt.

Phishing-Versuche in Social Media, Januar bis August 2016

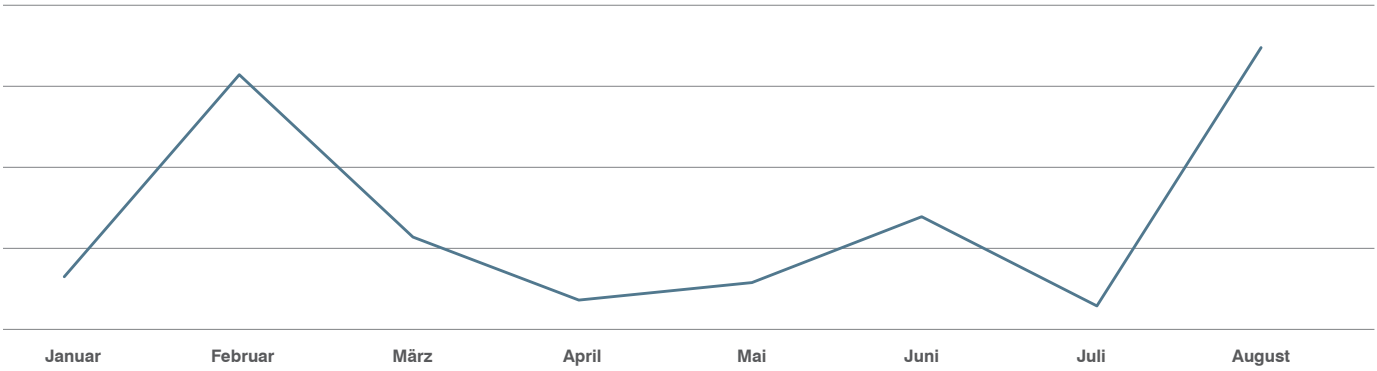

Abbildung 9: Social-Phishing nach Monat

Die Olympischen Spiele in Rio haben sich als Nährboden für Social-Media-Scams und schädlichem Inhalt erwiesen. Neben der Aufmerksamkeit um die Social Media, die Pokémon GO erregte, förderten andere beliebte Trends das Phishing, die Scams und die Verbreitung von Malware über Social-Media-Kanäle. Beispiele:

- Von 1.310 Social-Media-Konten mit Verbindungen zu den Olympischen Spielen und den Marken von Sponsoren waren 15 % betrügerischer Art. Diese Konten hatten 400.000 Abonnenten.
- Von den 543 mit Pokémon GO über Facebook, Twitter und Tumblr verbundenen Social-Media-Konten waren 167 – über 30 % – betrügerischer Art. Viele wurden entweder über Desktop- oder mobile Malware verbreitet.

EMPFEHLUNGEN VON PROOFPOINT

Gestützt auf die Entwicklungen in der Bedrohungslandschaft, die in diesem Bericht ausführlich beschrieben sind, empfehlen wir Folgendes, damit Sie sich vor den neuesten Angriffen schützen können:

- Die Verhinderung der Ransomware-Infizierung bei den E-Mail- und Netzwerkgateways ist noch immer die beste Strategie, um Kosten zu reduzieren und die Geschäftskontinuität zu sichern. Die Ransomware-Varianten, die nicht von der Kommunikation mit C&C-Servern abhängig sind, können netzwerk- und endpunktbasierte Lösungen umgehen, die sich auf die Erkennung von Kommunikationen mit schädlichen IPs konzentrieren. Verwenden Sie Sicherheitslösungen, die Informationen über verschiedene Angriffsvektoren (E-Mail, Netzwerk, Endpunkt usw.) hinweg freigeben können. Konzentrieren Sie sich auf das Abfangen der Bedrohungen, bevor sie in Ihr Netzwerk eindringen und Personen erreichen.

- Ransomware hat auch eine Personen- und Verfahrenskomponente, die mit Technologie allein nicht gelöst werden kann. Aufgrund der großen Menge der von Ransomware dominierten E-Mail-Kampagnen ist es doppelt so wichtig, dass Sie die Daten Ihres Unternehmens regelmäßig sichern. IT und die Sicherheitsabteilungen sollten auch über einen Plan und ein Verfahren verfügen, um Daten im Falle eines Angriffs wiederherzustellen. Mit Ransomware ist die Erstellung von Backups von Daten zugleich Prävention und Wiederherstellung. Ebenfalls wichtig ist Schulung, um die Bedrohungen erkennen und melden zu können.

- Weniger große, personalisierte Kampagnen können schwerer zu ermitteln sein. Investieren Sie in Sicherheitslösungen mit prädiktiven und verhaltensorientierten Erkennungsfunktionen, damit ähnliche Bedrohungen mit unterschiedlichen Hash-Werten erkannt und gestoppt werden können.

- Achten Sie auf gefälschte, schädliche Apps, die auf dem Rücken populärer Apps eingeschleust werden. Laden Sie nie Apps von illegalen Märkten herunter, auch wenn sie echt aussehen. Ihr Mobilgerät kann infiziert werden, auch wenn kein Jailbreak des Betriebssystems stattfindet.

- Sicherheitslücken auf Mobilgeräten kommen häufiger vor, als Sie denken. Das Aktualisieren der Apps auf die neueste Version ist immer empfehlenswert. Dies allein wird Ihnen jedoch nicht sagen, ob Sie bereits eine gefährliche oder bösartige App auf Ihrem Gerät haben. Investieren Sie in mobile Bedrohungsabwehrlösungen, die nach schadhaften Apps auf den Geräten in Ihrer Umgebung suchen und Sie vor einem riskanten oder schädlichen App-Verhalten warnen.

- Achten Sie auf Gefahren für Ihre Marke durch betrügerische Social-Media-Websites, die Angreifer verwenden. Investieren Sie in Tools, die Transparenz für die Social Media Ihres Unternehmens bieten und Sie vor betrügerischer Nutzung Ihrer Marke warnen. Schulen Sie Ihre Mitarbeiter, damit Sie achtsam sind, wenn Sie auf Links auf den Social-Media-Websites klicken, vor allem auf jene, die Downloads empfehlen für ein Angebot, das zu gut klingt, um wahr zu sein, oder die populäre Trends ausnützen. Fordern Sie sie auf, jedes Mal zu prüfen, ob die Website, die sie besuchen, die offizielle Website einer Organisation ist und nicht eine betrügerische Imitation. Halten Sie Ausschau nach Hinweisen wie beispielsweise die Anzahl der Followers, verifizierte Account-Badges und registrierte, in den Weblinks angegebene Domänen.