BERICHT

proofpoint.

DER FAKTOR MENSCH

2017

proofpoint.com/de

Prägend für die Bedrohungslandschaft 2016 sind das explosionsartige Wachstum bei Ransomware sowie die massiven E-Mail-Kampagnen, mit denen diese Malware-Form weltweit an Unternehmen aller Größen verteilt wurde. Diese Angriffe verursachten insgesamt mehrere Milliarden US-Dollar an direkten finanziellen Verlusten.

Cyberkriminelle verließen sich dabei weniger auf automatisierte Angriffe oder Exploits, sondern zunehmend auf Social Engineering, wodurch die Kampagnen effektiver wurden und schwerwiegendere Folgen nach sich zogen. Die Social-Engineering-Angriffe der Cyberkriminellen wurden dabei in großem Maßstab ausgeführt, ganz gleich, ob per E-Mail, als Software-as-a-Service, in sozialen Netzwerken oder mithilfe von Mobilgeräte-Apps. Für die ausgefeilten Angriffe kombinierten sie raffinierte Tricks und attackierten ihre Opfer mit überzeugenden Ködern. Außerdem wurden neue und verbesserte Techniken angewandt.

Diese Taktik ging auf. Die Angreifer verleiteten viele Benutzer zur Installation von Malware, zur Weitergabe von Anmeldedaten oder anderen vertraulichen Informationen sowie zur Überweisung von Geldern.

INHALT

Angriffe zielen auf Menschen und nicht auf den Code.

Cyberkriminelle setzen zunehmend auf Angriffe, bei denen nicht Schwachstellen in Software, sondern das Verhalten der Benutzer ausgenutzt wird. Der Wechsel zu dieser Angriffsform wurde erstmals im Jahr 2015 beobachtet, im vergangenen Jahr kam sie dann massiv zum Einsatz. Im Dezember 2016 setzten mehr als 99% aller Angriffe mit infizierten E-Mail-Anhängen auf Klicks durch Benutzer statt auf automatisierte Exploits. Diese Entwicklung betraf auch Bedrohungen mit gefährlichen URLs: 90% aller Nachrichten führten auf Phishing-Seiten, die keine Exploits verwenden, sondern die Opfer zur Eingabe ihrer Benutzernamen und Kennwörter auffordern.

Empfehlung: Implementieren Sie Lösungen, die Anhänge auf böswillige Makros und anderen eingebetteten Code untersuchen. Stellen Sie zudem Lösungen bereit, die mithilfe von Sandboxes proaktiv und in Echtzeit das Ergebnis von Klicks auf URLs sowie Anhänge analysieren. Dadurch kann böswilliges Verhalten aufgedeckt werden, das von herkömmlichen Schutzmaßnahmen unbemerkt bleibt. Ihre Lösung sollte Webseiten erkennen können, die Anmeldeinformationen stehlen – selbst wenn diese Webseiten nicht als böswillig bekannt sind.

DIE WICHTIGSTEN ERKENNTNISSE

Äußerst personalisierte, gezielte E-Mail-Kampagnen konzentrieren sich weniger auf Technologien als auf die Ausnutzung menschlichen Verhaltens.

Spearphishing-E-Mail-Kampagnen, die nicht wahllos verbreitet werden, sondern auf bestimmte Personen zugeschnitten sind, wurden automatisiert und in großem Umfang betrieben. Trotz der hohen Zahlen wurden häufig mehrere private, speziell auf den beabsichtigten Empfänger zugeschnittene Details verwendet. Bei Social-Engineering-Kampagnen wurden die Empfänger mit Dokumenten, die böswillige Makros und andere Techniken enthielten, zur Installation der Malware verleitet.

Empfehlung: Setzen Sie Lösungen ein, die raffinierte Phishing-Nachrichten erkennen und blockieren, bevor sie ihre Ziele erreichen.

Bedrohung, die auf Mobilgeräte abzielen, verzichteten auf Exploits und setzten stattdessen auf betrügerische Mobilgeräte-Apps sowie SMS-Phishing der nächsten Generation, um Benutzer großer Banken und andere Verbrauchermarken anzugreifen.

Angreifer gaben sich als vertrauenswürdige Marken aus, veröffentlichten Apps mit irreführenden Namen und nutzten weitere Tricks, um Benutzer zum Herunterladen der Malware auf ihre Mobilgeräte zu verleiten. Auf diese Weise installierten die Benutzer bereitwillig betrügerische Apps, die persönliche Informationen stehlen und in einigen Fällen sogar die volle Kontrolle über Mobilgeräte übernehmen. SMS-Phishing, bei dem die Angreifer ihre Opfer per Textnachrichten zur Weitergabe von Anmeldedaten und anderen vertraulichen Informationen verleiten, nahm ebenfalls zu. Dieser Trend spiegelt die wachsenden Bemühungen der Angreifer wieder, die Benutzer auf den von ihnen am meisten genutzten Geräten zu erreichen und so etablierte Netzwerk- und PC-basierte Schutzmaßnahmen zu umgehen.

Empfehlung: Implementieren Sie Lösungen zum Schutz von Mobilgeräten, die in Ihrem Untetnehmen eingesetzte und von Ihren Mitarbeitern genutzte Geräte abdecken. Diese Lösungen sollten in der Lage sein, SMS-Phishing-Angriffe der nächsten Generation zu erkennen und abzuwehren, Benutzerklicks zu erkennen, nachzuverfolgen und zu blockieren sowie das Vorhandensein betrügerischer, riskanter und böswilliger Apps auf Smartphones und Tablets zu erkennen. Gleichzeitig benötigen Banken, Telekommunikationsunternehmen, Einzelhändler und andere Unternehmen Lösungen zur Erkennung von Apps, die ihre Marke missbrauchen, um ihre Kunden zu betrügen, zu bestehlen oder ihnen in anderer Form zu schaden.

Business Email Compromise-Angriffe (BEC) holen im Vergleich mit Banking-Trojanern auf. Angreifer setzen bei dieser Betrugsmasche auf menschliches Fehlverhalten statt auf Software.

Der Anteil von Kompromittierungen geschäftlicher E-Mails (BEC-Angriffe) zur Durchführung von Finanzbetrug ist enorm angestiegen, da die Angreifer weniger auf böswillige Programme setzen, sondern ihre Opfer zunehmend überlisten, damit diese den Angriff selbst durchführen. BEC-Angriffe, bei denen die Opfer durch angebliche Kollegen dazu verleitet werden, Gelder zu überweisen oder vertrauliche Informationen weiterzugeben, machten im Jahr 2015 lediglich 1 % aller Finanzbetrug-E-Mails aus – und damit erheblich weniger als Banking-Trojaner. Ende 2016 lag ihr Anteil bereits bei 42 %. Dieser Anstieg wurde durch technische Fortschritte wie Sub-domänen-Spoofing in großem Maßstab sowie neue Vorgehensweisen beim gezielten Ansprechen von Empfängern und Fälschen von Absendern möglich.

Empfehlung: Verwenden Sie eine Lösung, die E-Mails dynamisch klassifizieren kann, damit auch neue Angriffsmethoden erkannt werden. Erstellen Sie mit dieser Lösung Quarantäne- und Blockierungsrichtlinien zur Abwehr von BEC-Attacken, die Unternehmen sehr individuell und gezielt angreifen sowie häufig keinerlei Schaddaten nutzen, sodass sie umso schwerer zu erkennen sind.

Betrügerischer Social-Media-Support nahm im Jahr 2016 um 150 % zu.

Bei so genannten „Angler-Phishing"-Angriffen wurden Kunden von Banken, sozialen Netzwerken und anderen Diensten mit gezielten Antworten auf Beiträge in den legitimen Social-Media-Kanälen der Marke angegriffen. Mit Angler-Phishing bezeichnen wir Angriffe, bei denen der Angreifer ein Doppelgängerkonto für das soziale Netzwerk erstellt und sich damit als Kundendienstmitarbeiter einer vertrauenswürdigen Marke ausgibt. Wenn sich ein Benutzer per Tweet hilfesuchend an ein Unternehmen wendet, antwortet der Angreifer und verweist das Opfer häufig auf echt wirkende Landing Pages, wo es zur Eingabe seiner Kontozugangsdaten aufgefordert wird.

Empfehlung: 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 zuverlässigen Lösung zum Schutz vor Social-Media-Angriffen, die alle sozialen Netzwerke überprüft und betrügerische Aktivitäten meldet.

Die Hälfte der Klicks auf böswillige URLs erfolgt auf Geräten außerhalb der Desktop-verwaltungsumgebung von Unternehmen.

Etwa 42 % aller Klicks auf böswillige URLs stammen von Mobilgeräten – und damit doppelt so viele wie die bislang üblichen 20 %. Weitere 8% der Klicks erfolgten durch, veraltete Windows Systeme bei denen potentielle Schwachstellen nicht mehr behoben werden.

Empfehlung: Implementieren Sie Lösungen, mit denen Mitarbeiter vor E-Mail-basierten Angriffen geschützt werden – unabhängig davon, wo die Nachrichten gelesen werden. Ihre Lösung sollte Klicks auf böswillige URLs von Smartphones und Tablets sowie E-Mail-Zugriffe über Webseiten am PC erkennen und blockieren. Für Benutzer, die weiterhin an (unternehmenseigenen oder privaten) Windows-PCs arbeiten, müssen Sie sicherstellen, dass Windows-Versionen verwendet werden, die weiterhin mit Sicherheitspatches unterstützt werden. Gewährleisten Sie außerdem, dass alle verfügbaren Patches für das jeweilige Betriebssystem sowie die genutzten Anwendungen installiert sind.

Physische Branchen und Cyberrisiken

Die branchenübergreifende Klickrate von durchschnittlich 4,6 % bedeutet, dass die Benutzer auf fast jede zwanzigste böswillige URL klicken. Die höchsten Klickraten registrierten wir eher in physischen, klassischen Branchen wie Bergbau und Bauindustrie statt in Branchen des digitalen Zeitalters, in denen persönliche, finanzbezogene sowie Gesundheitsdaten verarbeitet werden. Moderne Cyberkriminelle greifen jedoch alle Unternehmen und Branchen an, nicht nur solche mit Bezug zur digitalen Wirtschaft.

Der Donnerstag bringt nicht nur neue Rabattaktionen: Malware-Kampagnen variieren von Tag zu Tag.

Im Laufe der Woche erfolgt der Malware-Versand nach einem relativ festgelegten Muster, wobei erhebliche Unterschiede bei den Malware-Typen und Versandvektoren zu beobachten sind. Kampagnen, die böswillige Anhänge nutzen, treffen zu Bürobeginn ein und gehen nach 4 bis 5 Stunden stark zurück. Im Gegensatz dazu gehen E-Mails mit böswilligen URLs gleichmäßig über den Tag verteilt ein. Bedrohungsakteure versenden ihre E-Mails nach einem festen Zeitplan, um die maximale Wirkung zu erzielen. E-Mails mit dem Ziel Informationen zu stehlen, werden Anfang der Woche verschickt, wenn sie die meisten Informationen erfassen können. Gegen Ende der Woche kommt die Zeit von Ransomware und POS-Trojanern (Point of Sale, Kassensysteme), da die Sicherheitsteams vor dem Wochenende meist weniger Zeit haben, Infektionen zu erkennen und zu beseitigen.

Empfehlung: Unternehmen sollten die Suche nach Malware in ihrer Umgebung in der zweiten Wochenhälfte intensivieren. Zudem sollten sie Lösungen zur automatisierten Reaktion auf Zwischenfälle implementieren, die Sicherheitsvorfälle schnell beheben und Bedrohungen innerhalb von Stunden anstatt von Tagen beseitigen.

Empfehlung: Unternehmen in Branchen, in denen typischerweise viele Mitarbeiter außerhalb der Büros ihrer Arbeit nachgehen, müssen ihre Mitarbeiter ebenso gewissenhaft schützen wie Unternehmen, die in den Bereichen Finanzdienstleistungen, Gesundheitswesen und Technologie tätig sind. Sie benötigen unternehmensweite Lösungen, die auch die neuesten E-Mail-basierten Angriffe stoppen können.

Fast 90 % aller Klicks auf böswillige URLs finden innerhalb der ersten 24 Stunden nach Eingang statt.

Diese Nachrichten sind an dem Tag, an dem sie in den Posteingang gelangen, am wirksamsten: 87 % aller Klicks erfolgen innerhalb der ersten 24 Stunden nach Eingang. Fast die Hälfte aller Klicks findet innerhalb einer Stunde nach Ankunft der Nachricht statt, und ein Viertel aller Klicks sogar innerhalb von nur zehn Minuten. Die mittlere Zeit zwischen E-Mail-Eingang und Klick auf die URL ist während der Bürozeiten (zwischen 8 Uhr und 15 Uhr EDT in den USA und Kanada) mit weniger als einer Stunde am kürzesten. Großbritannien und Europa folgen einem ähnlichen Muster.

Empfehlung: Die schnelle Erkennung zugestellter böswilliger Nachrichten, auf die geklickt wurde, ist für die Minimierung der potenziellen Folgen unerlässlich. Unternehmen sollten Lösungen einsetzen, die proaktiv bereits übermittelte Nachrichten kennzeichnen und angeklickte URLs blockieren, die nach der Übermittlung als böswillig erkannt werden. Je länger sich eine böswillige URL im E-Mail-Posteingang des Empfängers befindet, desto größer ist die Wahrscheinlichkeit, dass sie angeklickt wird. Die ersten 24 Stunden sind besonders wichtig, um das Risiko der Bedrohungsübertragung zu begrenzen.

Mittagszeit für die Benutzer – ein Festmahl für Kriminelle!

Die Angreifer wissen genau, wann die Wahrscheinlichkeit am größten ist, dass die Empfänger auf böswillige Nachrichten klicken, und optimieren ihre Kampagnen entsprechend. Die Aktivitäten steigern sich schnell zu Beginn der Bürozeiten und erreichen etwa vier bis fünf Stunden später ihren Höhepunkt – genau zur Mittagszeit.

Dieses Muster ist in allen Regionen in etwa gleich. Ganz besonders genau wird es in den USA, in Kanada sowie Australien befolgt, während die Klicks in Frankreich gegen 13 Uhr ihren Höhepunkt erreichen. Benutzer in der Schweiz und in Deutschland klicken hingegen noch vor der Mittagszeit – hier wird der Höhepunkt in den ersten Stunden des Bürotages erreicht. Angestellte in Großbritannien verteilen die Klicks gleichmäßig über den gesamten Tag, mit einem deutlichen Rückgang nach 14 Uhr.

Empfehlung: Implementieren Sie Lösungen, die Benutzer unabhängig davon schützen, wo sie böswillige Nachrichten lesen und darauf klicken – ob Vormittags am Arbeitsplatz oder zur Mittagszeit am Smartphone.

DIE GENAUEN ZAHLEN

AUSNUTZUNG MENSCHLICHEN VERHALTENS ÜBERTRUMPFT BINÄRDATEIEN

Im zweiten Halbjahr 2016 war der Wechsel zu Taktiken, die menschliches Verhalten ausnutzten, bereits vollzogen. Ganze 99 % aller E-Mail-basierten Angriffe mit Finanzbetrug setzten für die Installation der Malware auf Klicks durch den Empfänger statt auf automatisierte Exploits.

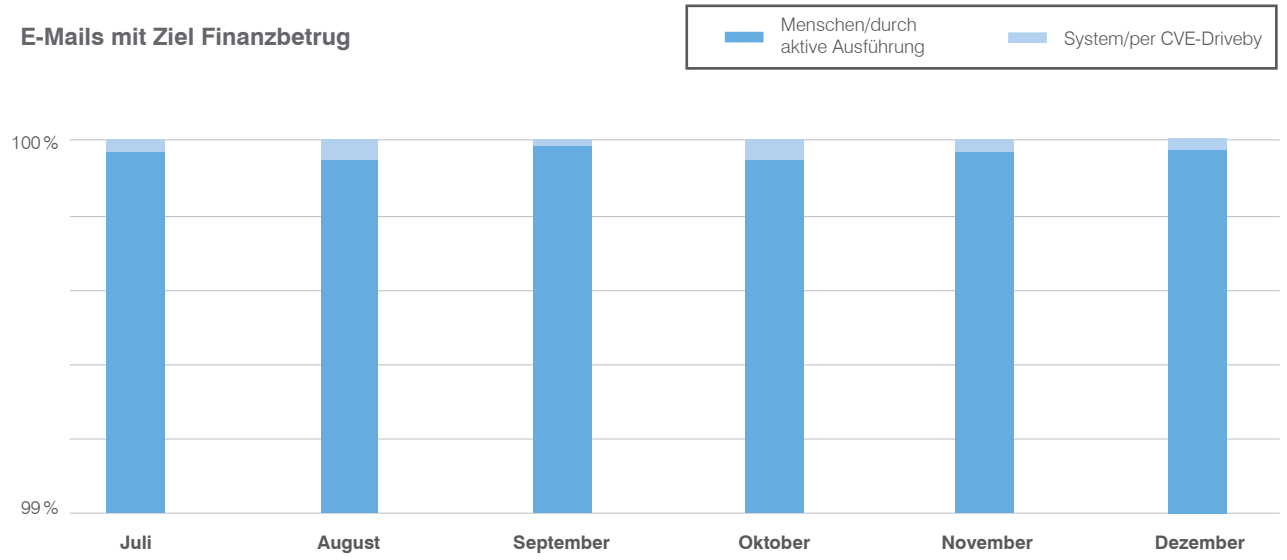


Abb. 1: Verhältnis von E-Mails mit Ziel Finanzbetrug, die auf Social Engineering setzen, zu automatisierten Exploits, Juli bis Dezember 2016

Dieser Trend gilt auch für URL-basierte böswillige Nachrichten. Im Monatsdurchschnitt führten 90 % der böswilligen Nachrichten mit URLs zu Anmeldedaten-Phishing (Doppelgängerseiten offizieller Anmeldeseiten, auf denen Benutzer zur Eingabe ihrer Kontoanmeldedaten aufgefordert werden) statt zu Exploit-Kits (Seiten, die Schwachstellen auf dem jeweiligen System suchen und ausnutzen).

EXPLOIT-KITS NUTZEN DEN FAKTOR MENSCH AUS

Nur wenige Angriffsvektoren sind scheinbar so sehr mit automatisierten Software-Exploits verbunden wie Exploit-Kits. Doch selbst hier ändern die Angreifer ihre Taktiken und setzen mittlerweile verstärkt auf die Ausnutzung des menschlichen Verhaltens.

Das seit mehreren Jahren etablierte Exploit-Kit Magnitude wird über Malvertising verbreitet (d. h. über Online-Werbung, die versteckten böswilligen Code enthält und Benutzer legitimer Webseiten überlistet). Magnitude filtert dabei den Datenverkehr und leitet ihn so weiter, dass nur bestimmte Benutzer betroffen sind. In letzter Zeit wurde dabei Cerber verbreitet – und zwar fast ausschließlich in Südkorea und Taiwan. Doch im ersten Quartal 2016 beobachteten wir in Magnitude eine neue Social-Engineering-Infektionskette, die auf Internet Explorer-Benutzer unter Windows 10 abzielt.

Bei diesem Angriff leitete Malvertising bestimmte Besucher einer legitimen Webseite auf eine Landing Page um, die Benutzer mithilfe von eingebettetem Code am Schließen oder Umgehen von Dialogfeldern hindert. Gleichzeitig werden mehrere Bildschirmabfragen angezeigt, die zu erwartende Windows-Dialogfelder nutzen und den Benutzer zum Herunterladen einer Verknüpfung auffordern, die Windows PowerShell-Befehle enthält. Mit diesem Befehl wird wiederum Cerber-Ransomware heruntergeladen und ausgeführt.

Dieser Social-Engineering-Taktik fehlt die Raffinesse, die wir bei anderen per E-Mail verteilten Varianten beobachtet haben. Sie bestätigt jedoch, dass die Angreifer immer mehr dazu übergehen, den „Faktor Mensch“ auszunutzen. Aufgrund der auf Social Engineering basierenden Ansätze sind Exploit-Kits nicht mehr zwingend auf automatisierte Software-Exploits beschränkt. Stattdessen verleiten diese Angriffe Benutzer dazu, auf Schaltflächen zu klicken, Sandboxen zu unterlaufen, PowerShell-Code auszuführen und weitere Aktionen durchzuführen, mit denen die eigenen Systeme infiziert werden.

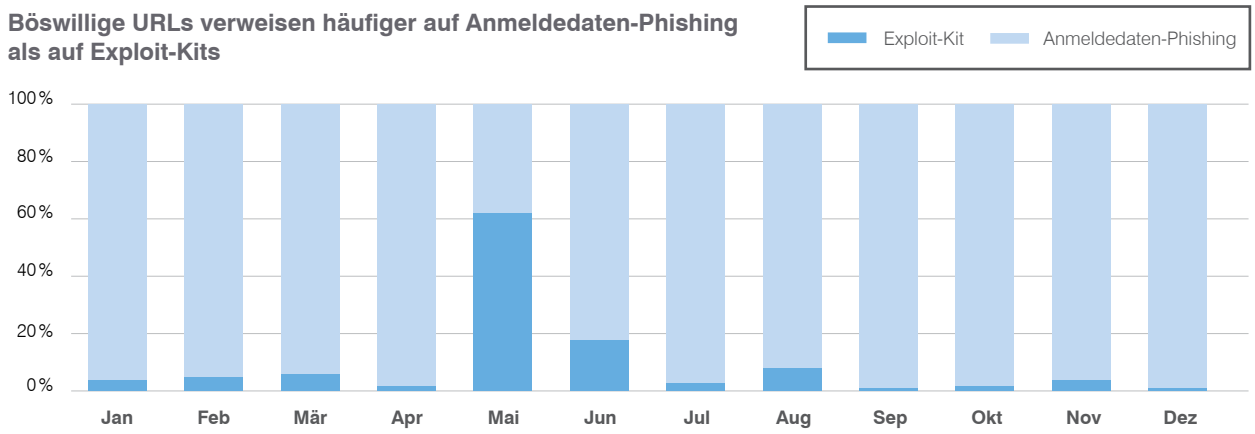


Abb. 2: URLs in böswilligen E-Mails, die auf Anmeldedaten-Phishing verweisen, im Vergleich zu Exploit-Kits

Diese beiden Veränderungen zeigen, dass die Cyberkriminellen zur Infizierung von Systemen, für den Diebstahl von Anmeldeinformationen und die Überweisung von Geldbeträgen nicht mehr auf automatisierte Exploits setzen, sondern sich auf Angriffstechniken konzentrieren, die menschliche Interaktionen ausnutzen.

TRENDS BEI GEZIELTER MALWARE-VERBREITUNG

Die Kriminellen nutzten Bank-Trojaner, um ihre Opfer in den jeweiligen Regionen gezielt anzugreifen. Auch dies spiegelt den Trend zur Ausnutzung menschlichen Verhaltens wieder. Bei diesen Angriffen kommen Köder und Anhänge in den jeweiligen Sprachen sowie regional angepasster Code zur Übertragung böswilliger Anweisungen (Web-Injektionen) zum Einsatz. Zudem waren die Kampagnen zeitlich so optimiert, das sie ideal an die Bürozeiten – und das Klickverhalten – der beabsichtigten Empfänger angepasst waren.

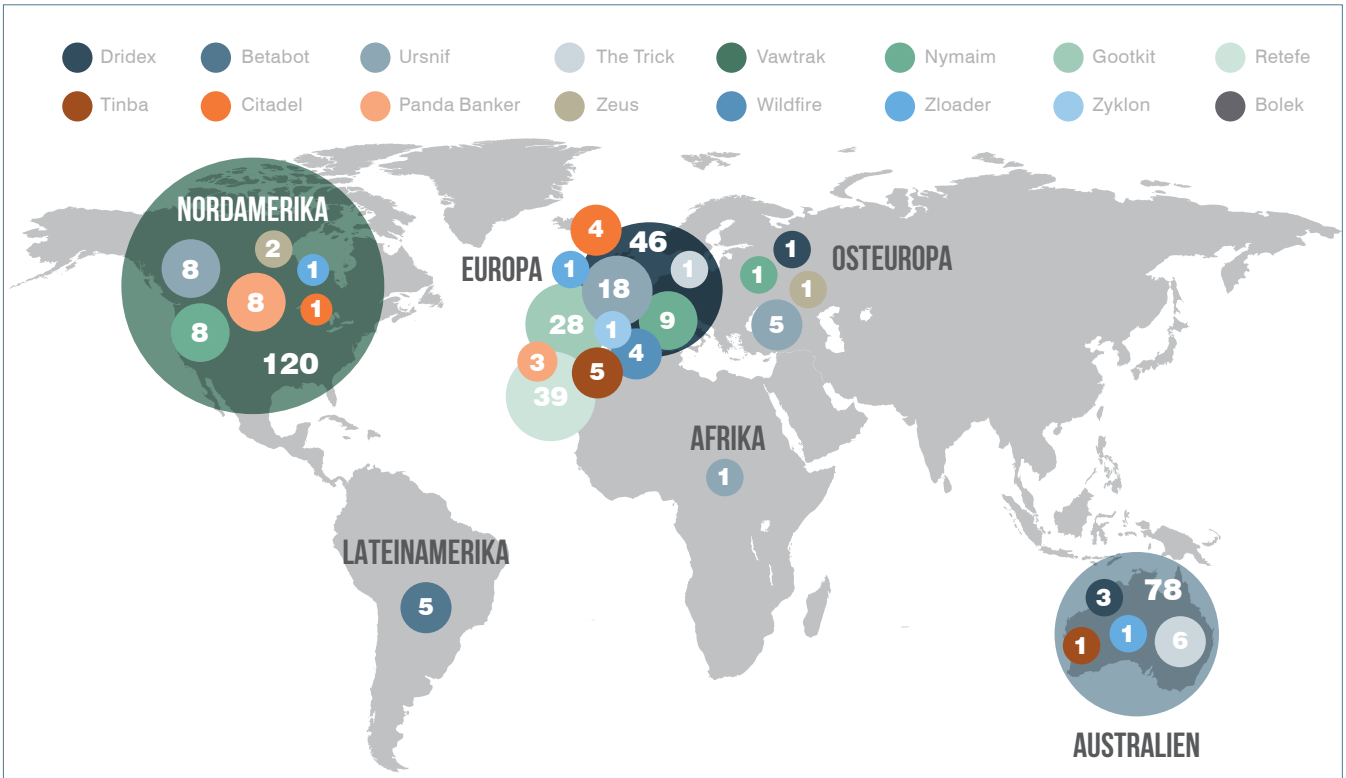


Abb. 3: Weltweite Bank-Trojaner-Aktivitäten nach Region und mit Anzahl der Kampagnen

Empfehlung: Setzen Sie erstklassige Schutzmaßnahmen ein, die für bestimmte Regionen optimierte Kampagnen erkennen und blockieren können. Nutzen Sie Bedrohungsdaten, die Ihr Team über neueste Trends bei Angreifern sowie darüber auf dem Laufenden halten, wie Schaddaten an ihre Opfer angepasst werden.

AUF DEN WOCHENTAG ABGESTIMMTE NACHRICHTEN MIT SCHÄDLICHEN ANHÄNGEN

E-Mail-basierte Bedrohungen können Benutzer an jedem Tag der Woche angreifen, und die Angreifer optimieren den Versandzeitpunkt (Wochentag und Uhrzeit) ihrer Kampagnen für maximalen Erfolg. Wenn böswillige Nachrichten zu Beginn des Bürotages zugestellt werden, ist die Wahrscheinlichkeit am größten, dass die Benutzer sie sehen und im Laufe des Tages darauf klicken.

E-Mail-basierte Bedrohungen werden an jedem Wochentag versendet, doch an einigen Tagen ist ihre Zahl höher als an anderen. In Abb. 4 sehen Sie das typische Wochenmuster:

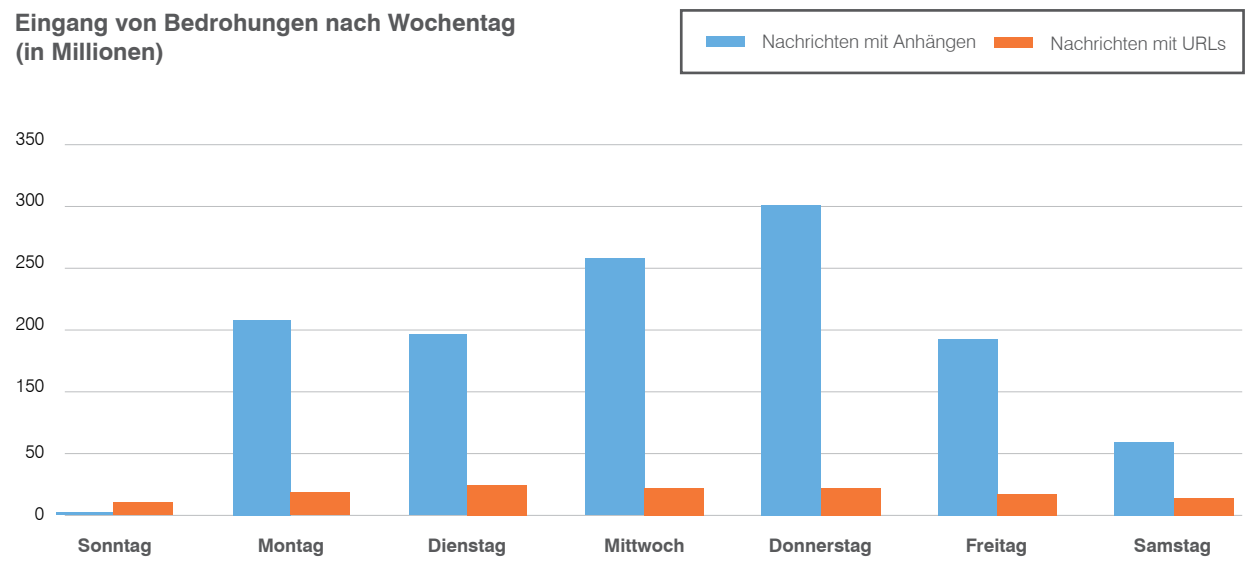


Abb. 4: Bedrohungsaufkommen nach Wochentag

Die Zahl böswilliger Anhänge ist mit 38 % des durchschnittlichen Wochenaufkommens an Donnerstagen am höchsten. Der Trend, Nachrichten gezielt an bestimmten Wochentagen zu senden, scheint weltweit verbreitet zu sein: In allen von uns untersuchten Ländern werden donnerstags die meisten Nachrichten mit Anhängen versandt.

Die Zahlen dahinter decken weitere wichtige Muster auf:

- Das Aufkommen von Nachrichten mit böswilligen URLs ist gleichmäßiger über die Wochentage verteilt. Die meisten Nachrichten mit böswilligen URLs – die Hauptmethode für Anmeldedaten-Phishing – werden weiterhin dienstags und donnerstags versendet. Die Varianz ist jedoch etwas geringer als in den vergangenen Jahren.
- An Wochenenden werden weiterhin nur wenige E-Mail-basierte Bedrohungen verbreitet. Gleichzeitig geht das Aufkommen von Nachrichten mit URLs nicht so stark zurück wie bei Nachrichten mit Anhängen. Dies gilt vor allem im Vergleich zu den Vorjahren, als das Nachrichtenaufkommen am Wochenende vernachlässigbar gering war.

Die vom jeweiligen Wochentag abhängigen Schwankungen bei URL-Kampagnen sind auch regional größer. In den von uns untersuchten Regionen wichen die Versandtage in Europa am stärksten von den USA und Kanada ab. An Donnerstagen werden mit 20,2 % des Wochenaufkommens eindeutig die meisten Nachrichten verbreitet. Während dienstags immerhin 17,6 % verzeichnet werden, sind es montags, mittwochs und freitags jeweils etwa 15 %.

Empfehlung: Implementieren Sie Schutzlösungen, mit denen Sie Ihre Benutzer an jedem Wochentag vor allen E-Mail-basierten Angriffen schützen können. Diese Lösungen sollten in der Lage sein, große Nachrichtenvolumen zu verarbeiten, ohne dabei die Leistung oder die Effektivität zu beeinträchtigen.

DER DONNERSTAG BRINGT NICHT NUR NEUE RABATTAKTIONEN: TRENDS BEIM MALWARE-VERSAND NACH KATEGORIE

Malware-Kampagnen werden nicht über die gesamte Woche hinweg gleichmäßig verteilt. Stattdessen gibt es deutlich sichtbare Muster, da einige Malware-Kategorien bevorzugt an bestimmten Wochentagen verbreitet werden.

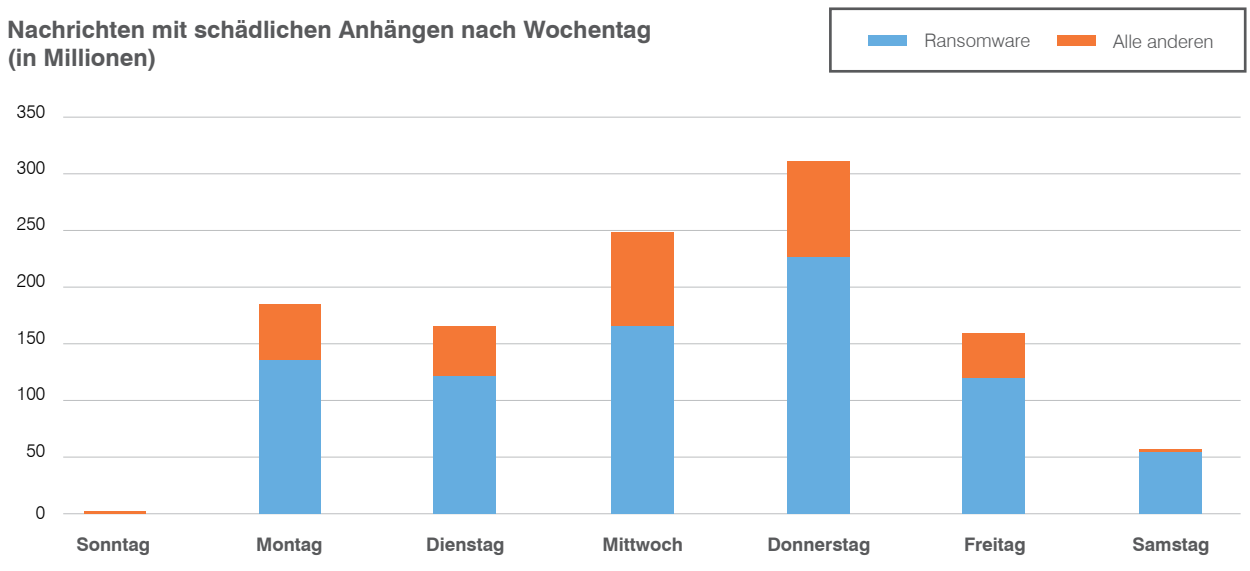


Abb. 5: Erfasstes Gesamtaufkommen der Malware-Kategorien pro Tag

Ein Beispiel dafür ist Ransomware, die die Daten ihrer Opfer bis zur Zahlung eines Lösegeldes blockiert. Die Zahl der Ransomware-Nachrichten ist donnerstags erheblich höher als an anderen Wochentagen. Sie werden dabei vor allem von hochvolumigen Locky-Kampagnen verbreitet. Mit wenigen Ausnahmen war Ransomware die einzige Malware-Form, die an Wochenenden verteilt wird.

Durch die Größe der Ransomware-Kampagnen des Jahres 2016 waren die Trends bei anderen Malware-Kategorien nicht direkt sichtbar. In Abb. 6 wird das Nachrichtenaufkommen ohne Ransomware dargestellt.

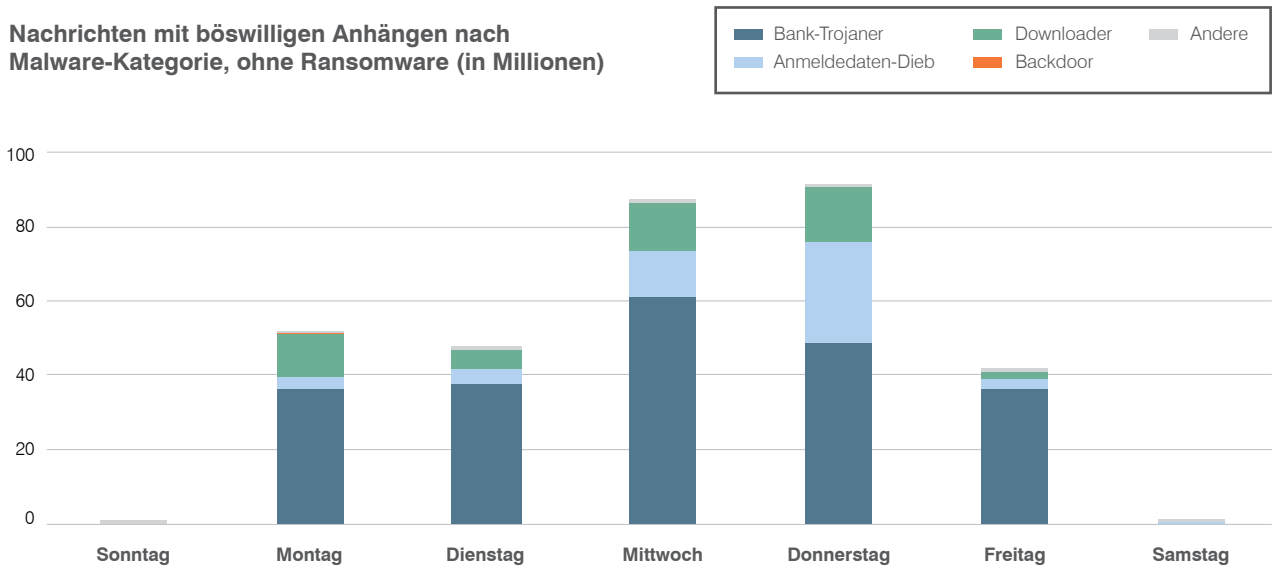


Abb. 6: Erfasste böswillige Nachrichten nach Malware-Kategorie, ohne Ransomware

Während mittwochs die meisten Bank-Trojaner verteilt werden, bevorzugen Anmeldedatendiebe den Donnerstag, während sich Downloader von Montag bis Donnerstag relativ gleichmäßig verteilen.

Die Zahlen der seltener versandten Malware-Formen zeigen eine noch deutlichere Präferenz für Wochentage:

- Keylogger und Backdoor-Trojaner bevorzugen den Montag. Die Zahl der montags versendeten Backdoor-Kampagnen lag um 68 % über dem Durchschnitt für die Zeit von Dienstag bis Donnerstag. Noch deutlicher ist die Vorliebe für den Montag bei Keyloggern: An diesem Tag wurden doppelt so viele Kampagnen gestartet wie durchschnittlich von Dienstag bis Donnerstag.
- POS-Kampagnen (Point of Sale, Kassensysteme) wurden fast ausschließlich donnerstags oder freitags gesendet: 80 % dieser Kampagnen wurden im Jahr 2016 an einem der beiden Tage gestartet.

UNWIDERSTEHLICHE KÖDER

Verbreitung und Effektivität von Phishing

Die beliebtesten Köder für Anmeldedaten-Phishing sind seit 2015 fast unverändert. Genauer gesagt: Die fünf am häufigsten verwendeten Köder sind praktisch gleich geblieben.

Die zehn häufigsten Köder für Phishing von Anmeldedaten

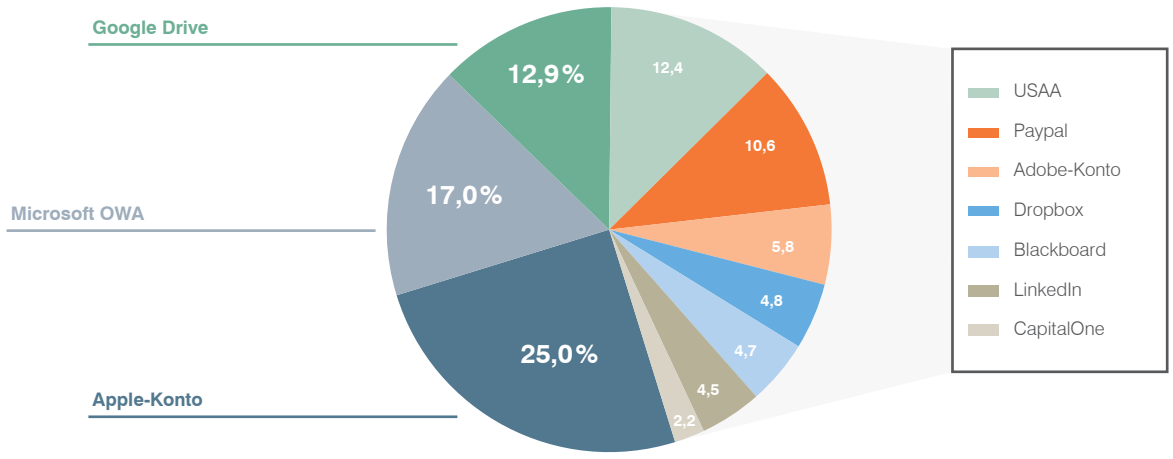


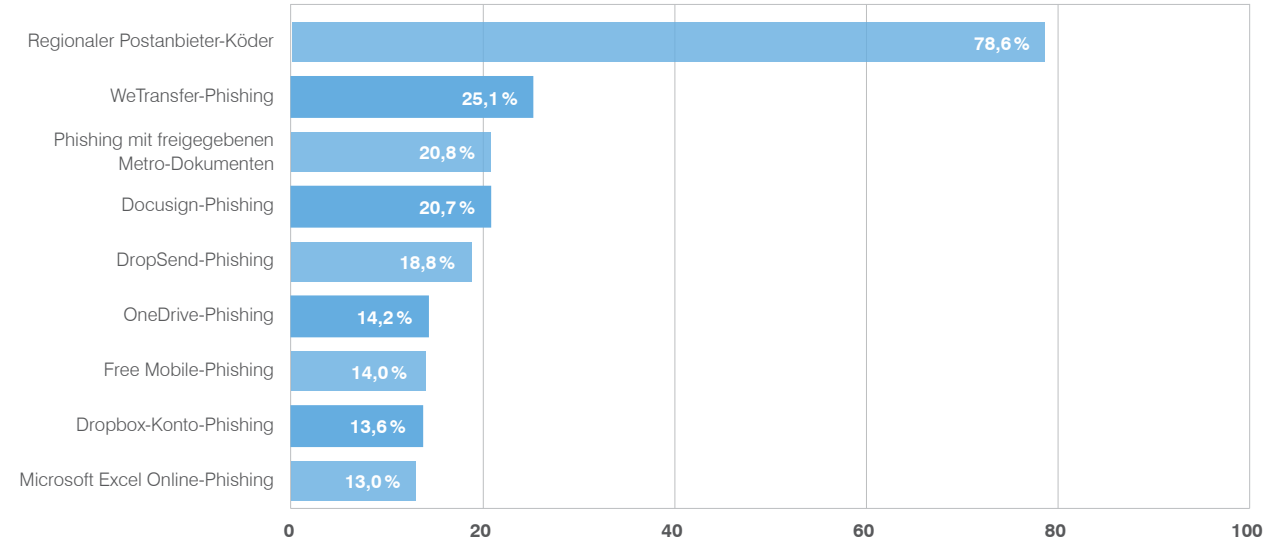
Abb. 7: Die zehn häufigsten Köder für Phishing von Anmeldedaten (Anteil in Prozent)

Ebenso wie im Vorjahr korrelierte das Verteilungsvolumen von 2015 nicht mit den Klickraten. Am häufigsten wurden zum Beispiel Phishing-Nachrichten zum Diebstahl von Apple IDs versendet, die höchste Klickrate erzielten jedoch Phishing-Links zu Google Drive.

Als effektivste Köder erwiesen sich Konten, über die Dateien und Bilder geteilt werden (z. B. Google Drive, Adobe Creative Cloud und Dropbox). Diese Nachrichten machten unter den häufigsten Ködern weniger als 24 % des Nachrichtenaufkommens aus, erzielten jedoch die höchsten Klickraten. Wir stellten in Bezug auf Köder und Effektivität zudem einen deutlichen Unterschied zwischen großen und kleinen Anmeldedaten-Phishing-Kampagnen fest (siehe Abb. 8).

Vergleich der Effektivität von Ködern nach Kampagnengröße

Klickrate bei kleinen Kampagnen (mehr als 100 E-Mails)



Klickrate bei großen Kampagnen (mehr als 20.000 E-Mails)

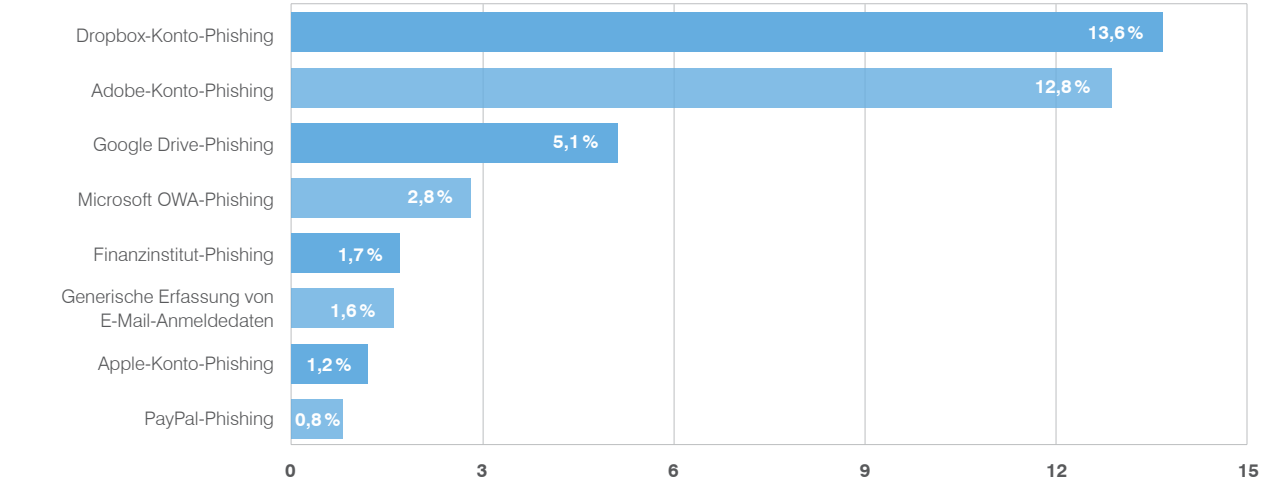


Abb. 8: Häufigste Köder und ihre Klickraten, große und kleine E-Mail-Kampagnen im Vergleich

Während Social-Media-Köder unsere Bedrohungsdaten statistisch gesehen wenig beeinflussen, können sie für kleinere, gezieltere Kampagnen durchaus effektiv sein. Köder mit Dokumentenweitergabe sind jedoch bei kleinen und großen Kampagnen gleichermaßen effektiv (und daher bei Angreifern beliebt). Gleichzeitig ist zu beachten, dass kleinere Kampagnen eine höhere Klickrate erzielen als große Kampagnen, weshalb ihre Erkennung und Blockierung besonders wichtig ist.

Empfehlung: Es ist wichtig, die Mitarbeiter zu schulen, damit sie auch die neuesten und effektivsten Phishing-Köder erkennen. Da die Angreifer jedoch ihre Köder, Schaddaten oder andere Aspekte ihrer Kampagnen über Nacht ändern können, benötigen Sie Lösungen, mit denen Sie dank einer Kombination aus proaktiver und Echtzeit-Sandbox-Analyse von E-Mail-URLs verschiedenste Anmeldedaten-Phishing-Angriffe erkennen können.

KLICKVERHALTEN: KLICKS VOM BÜRO-PC – 2014 LÄSST GRÜSSEN

Im Jahr 2014 erfolgten 91 % der Benutzerklicks von einem Microsoft Windows-PC. In den vergangenen zwei Jahren ist dieser Anteil um die Hälfte gesunken. Im gleichen Zeitraum hat sich der Anteil der Klicks von Mobilgeräten mehr als verdoppelt – auf 42 % der insgesamt erfassten Klicks auf böswillige URLs.

Fünf häufigste Betriebssysteme, in denen Benutzer 2016 klickten

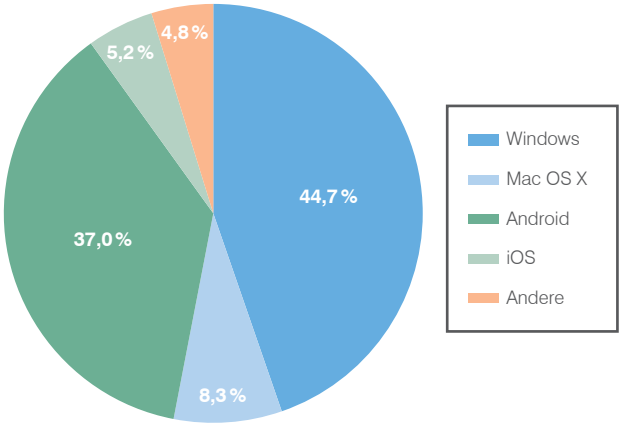


Abb. 9: Betriebssysteme, in denen Benutzer am häufigsten klicken (Anteil in Prozent)

Benutzer verlagern ihre Arbeit – und ihre Klicks – auf Mobilgeräte. Kriminelle nutzen diesen Wechsel aus, um ihre Opfer gezielt mit Social-Media-, Banking- und anderen Mobilgeräte-Apps anzugreifen und so zur Preisgabe vertraulicher Informationen zu verleiten. Dazu ist kein automatisiertes Software-Exploit erforderlich.

Klicks von Windows-PCs bereiten Sicherheitsverantwortlichen weiterhin Probleme:

- 66 % aller Windows-PC-Klicks (29 % der gesamten Klicks) erfolgen in einer Windows-Version, für die kein Mainstream-Support mehr angeboten wird (Windows 7).
- 19 % aller Windows-PC-Klicks (8,5 % der gesamten Klicks) erfolgen in Versionen, für die keinerlei Sicherheitspatches mehr veröffentlicht werden (Windows XP, Windows Vista, Windows 2000). Ihr Anteil hat sich im Vergleich zu 2014 fast verdoppelt.

Während sich die Angreifer immer weniger auf automatisierte Exploits verlassen, nutzen die am häufigsten für E-Mail-Anhänge verwendeten Exploits eine vier Jahre alte Schwachstelle in Microsoft Office aus (CVE-2012-0158). Deshalb ist es weiterhin wichtig, Betriebssystem- und Anwendungspatches so schnell wie möglich zu installieren.

KLICKTRENDS NACH BRANCHE

Die Zahlen von 2016 zeigen erneut, dass bei Klicks keine Unterschiede bestehen: In Unternehmen aller Branchen werden durchschnittlich 4,6 % aller böswilligen URLs angeklickt. Genau wie in den letzten Jahren ist die Klickrate in einigen Branchen höher als in anderen. Eher auf physische Tätigkeiten ausgerichtete Unternehmen (z. B. Bauindustrie und Bergbau) klicken häufiger auf böswillige URLs als Vertreter des digitalen Zeitalters.

4,6 % Branchenübergreifende durchschnittliche Klickrate für böswillige URLs

Durchschnittliche Klickrate nach Branche, 2016

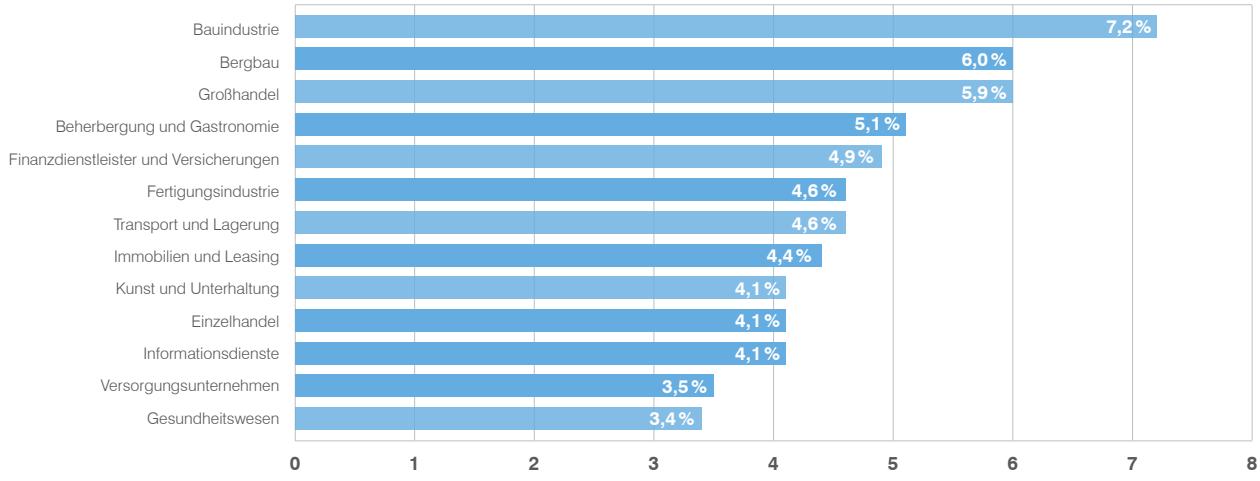


Abb. 10: Klickraten nach Branche

MITTAGSZEIT FÜR DIE BENUTZER – EIN FESTMAHL FÜR KRIMINELLE!

Benutzer in allen Regionen klicken zu den gleichen Tageszeiten auf böswillige URLs: Die Aktivitäten steigern sich schnell zu Beginn der Bürozeiten und erreichen etwa vier bis fünf Stunden später ihren Höhepunkt – genau zur Mittagszeit.

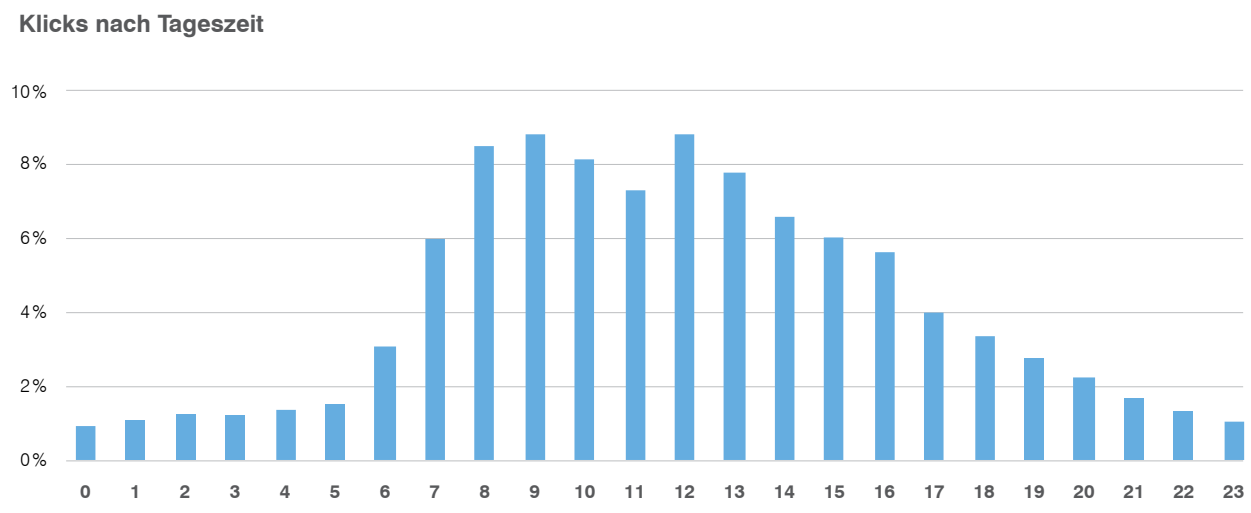


Abb. 11: Klicks nach Tageszeit für alle Regionen, als Anteil an der Gesamtzahl der Klicks pro Tag

Die wichtigste Erkenntnis aus den Daten in Abb. 11: Benutzer klicken über den ganzen Tag verteilt auf böswillige URLs. Ob am Arbeitsplatz oder zu Hause, tags oder nachts – Benutzer klicken zu allen Zeiten auf URLs, die sie auf Phishing-Seiten oder zu Malware-Downloads führen.

Im Verlauf des Tages konnten wir einige regionale Abweichungen bei den Zeiten beobachten, in denen Benutzer mit der größten Wahrscheinlichkeit auf böswillige URLs klicken (siehe Abb. 12).

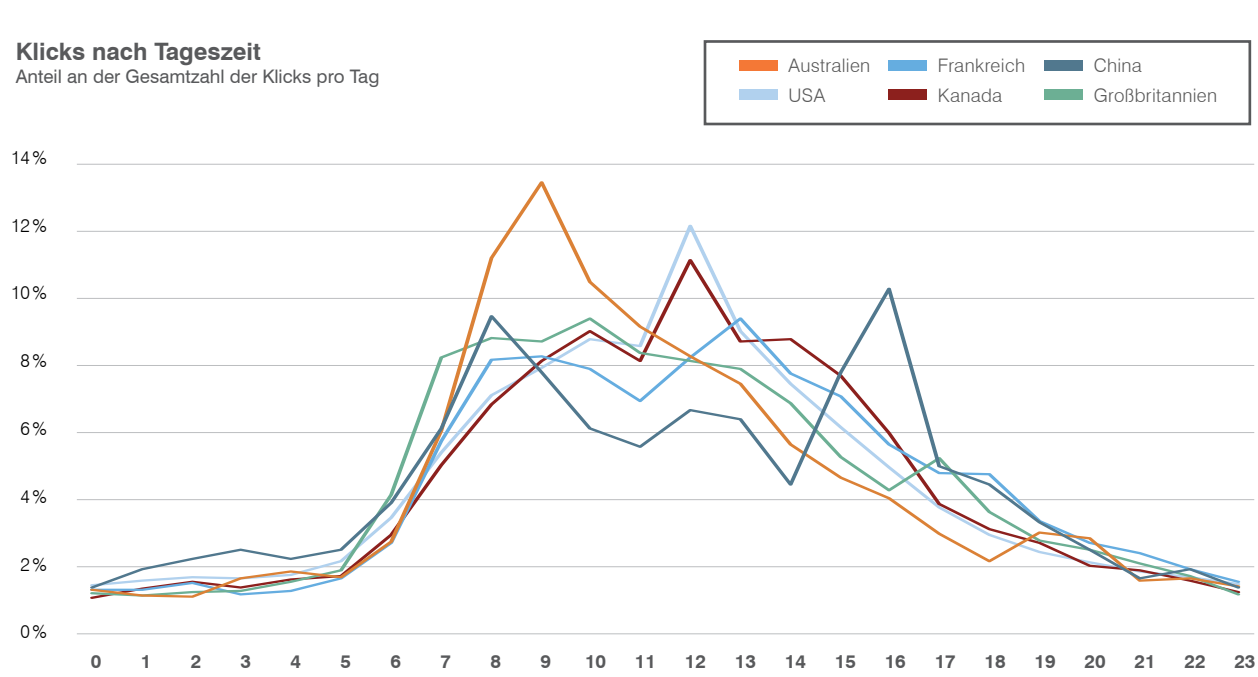


Abb. 12: Klicks auf böswillige URLs, nach Tageszeit und Land

Die Klickaktivitäten variieren je nach Land:

- Benutzer in den USA, Kanada und Australien klicken auf häufigsten um die Mittagszeit, Benutzer in Frankreich vor allem gegen 13 Uhr.
- Benutzer in der Schweiz und in Deutschland klicken hingegen deutlich früher – hier wird der Höhepunkt in den ersten Stunden des Bürotages erreicht.
- Angestellte in Großbritannien verteilen die Klicks gleichmäßig über den gesamten Tag, mit einem deutlichen Rückgang nach 14 Uhr.

ZEITRAUM BIS ZUM KLICKEN

Die Zeiten mit den meisten Klicks stimmen mit den Bürozeiten überein, d. h. hier vergeht am wenigsten Zeit, bis auf neu eingegangene böswillige URLs geklickt wird. Im Mittel beträgt der Zeitraum bis zum Klicken auf böswillige URLs während der Bürozeiten weniger als eine Stunde.

Die meisten Klicks erfolgen innerhalb von einem Tag, nachdem böswillige URLs in den Posteingang des Benutzers gelangten. Unten sehen Sie Details dazu, wie schnell auf URLs geklickt wird:

25,5% aller Klicks erfolgen innerhalb von zehn Minuten

48,6% aller Klicks erfolgen innerhalb von einer Stunde

87,1% aller Klicks erfolgen innerhalb eines Tages

98,3% aller Klicks erfolgen innerhalb einer Woche

Mittlere Zeit bis zum Klick während der Bürozeiten

< 1 STUNDE

AUTOMATISIERTE AUSNUTZUNG DES FAKTORS MENSCH

BEC (BUSINESS EMAIL COMPROMISE): AUSNUTZUNG DES FAKTORS MENSCH

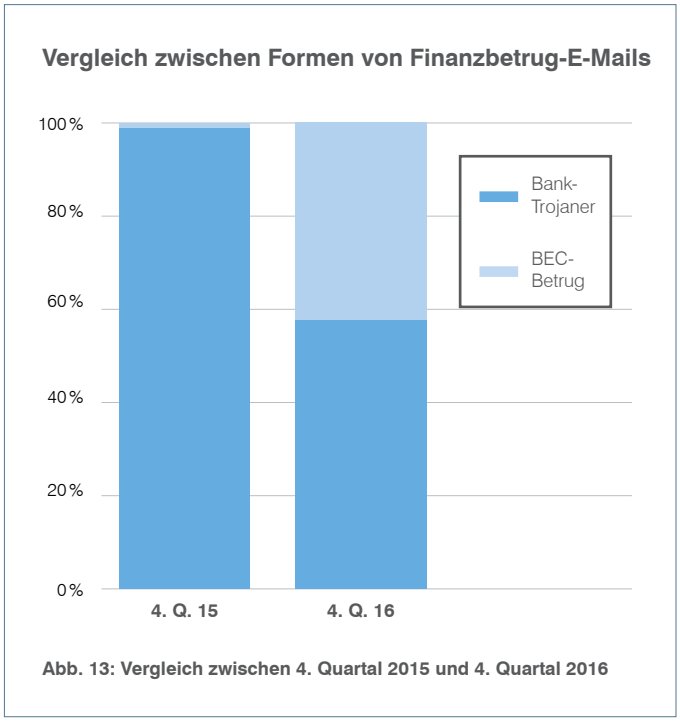


Abb. 13: Vergleich zwischen 4. Quartal 2015 und 4. Quartal 2016

Die Zunahme von BEC-Angriffen (Business Email Compromise) verdeutlicht das Wachstum der Angriffstechniken, die für den Wechsel von automatisierten Exploits oder Tools zur Ausnutzung menschlichen Verhaltens verantwortlich sind. Drei Viertel unseres weltweiten Kundenstamms waren in den letzten drei Monaten des Jahres 2016 von mindestens einem BEC-Angriffsversuch betroffen. Dieses Wachstum spiegelt sich in der Zunahme von BEC-Angriffen im Vergleich zu Bank-Trojanern bei Finanzbetrugsversuchen in der Zeit zwischen 2015 und 2016 wieder.

BEC ist eine neue Bedrohungsart, doch angesichts größerer Aufmerksamkeit bei den Benutzern und automatisierten Schutzmaßnahmen entwickeln die Angreifer ihre Techniken bereits weiter. BEC-Angreifer versendeten bislang häufig gefälschte, angeblich vom Geschäftsführer (CEO) stammende Nachrichten an den Finanzvorstand (CFO) eines attackierten Unternehmens. Wie Abb. 14 zu sehen, begann sich das gegen Ende 2016 zu ändern.

45 % Zunahme der BEC-Angriffe im 4. Quartal gegenüber dem vorherigen Quartal

Anteil der BEC-E-Mails, die sich als „CEO an den CFO“ ausgeben
Juli bis Dezember 2016

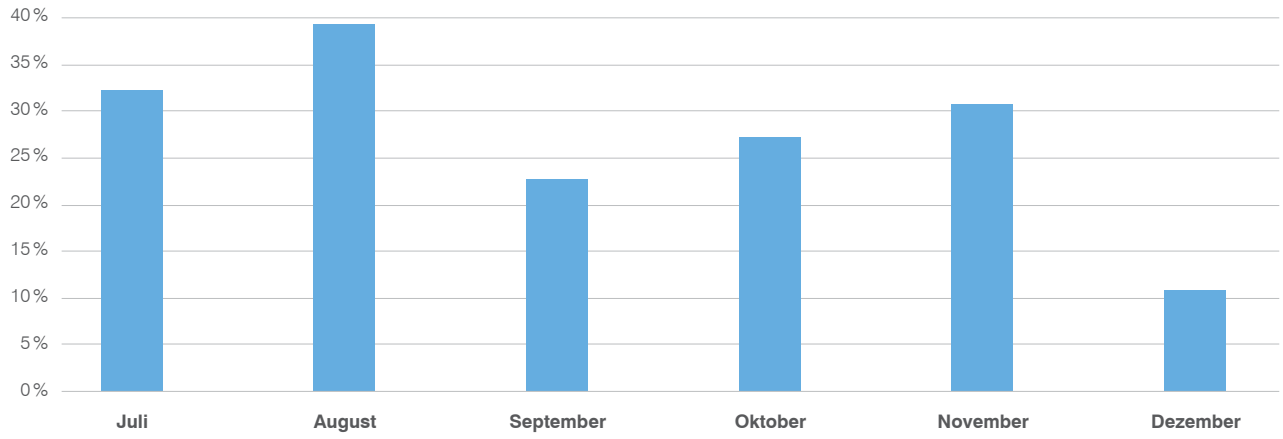


Abb. 14: Anteil aller BEC-E-Mails, die angeblich von der Geschäftsführung (CEO) an den Finanzvorstand (CFO) gingen, Juli bis Dezember 2016

Auch wenn es weiterhin zum Repertoire von BEC-Angriffen gehört, sich als CEO auszugeben (Spoofing), richten sich Cyberkriminelle immer häufiger an Opfer in den hinteren Reihen von Unternehmen, d. h. die Attacken beschränken sich nicht mehr auf die Verbindung zwischen CEO und CFO, sondern nutzen die Verbindung des CEOs mit anderen Mitarbeitergruppen aus. So können sie die Buchhaltung für Überweisungsbetrug missbrauchen, mithilfe der Entwicklungsabteilung geistiges Eigentum stehlen oder der Personalabteilung vertrauliche Steuer- und Identitätsinformationen entlocken.

SPEARPHISHING IN GROSSEM MASSSTAB: SOCIAL ENGINEERING DURCH AUTOMATISIERTE MASSENHAFTE PERSONALISIERUNG

Vor 2016 mussten E-Mail-Bedrohungsakteure meist zwischen zwei Ansätzen wählen:

- Hochvolumige „Spray-and-Pray“-Kampagnen, bei denen hunderttausende oder Millionen böswillige E-Mails an ungefilterte Empfänger gesendet werden
- Kleine, äußerst gezielte Kampagnen mit sorgfältig vorbereiteten Ködern

Im Jahr 2016 begann jedoch ein raffinierter Akteur, den wir als TA530 kennen, mit der Verbreitung personalisierter E-Mails in hochvolumigen Kampagnen, bei denen hochentwickelte Social-Engineering-Techniken zum Einsatz kamen. Diese Kampagnen umfassten tausende oder zehntausende E-Mails, die an verschiedene Branchen gerichtet waren und jeweils darauf zugeschnittenen Angriffscode nutzten. Beispielsweise kann POS-Malware in gegen den Einzelhandel gerichteten Kampagnen verwendet werden, während Bank-Trojaner und Informationsdiebe gegen Fertigungsunternehmen oder Technologiefirmen zum Einsatz kommen.

TA530 nutzte Informationen aus öffentlichen Quellen wie LinkedIn sowie Daten aus kompromittierten Online-CRM-Systemen (Customer Relationship Management), um höchst personalisierte E-Mail-Köder und -Anhänge zu entwickeln, die Namen, Positionen, Adressen, Unternehmensnamen und sowie weitere Angaben zu den Empfängern enthielten. Diese Elemente gaben den E-Mails den Anschein des Legitimen, während das Social Engineering für das notwendige Dringlichkeitsgefühl sorgte.

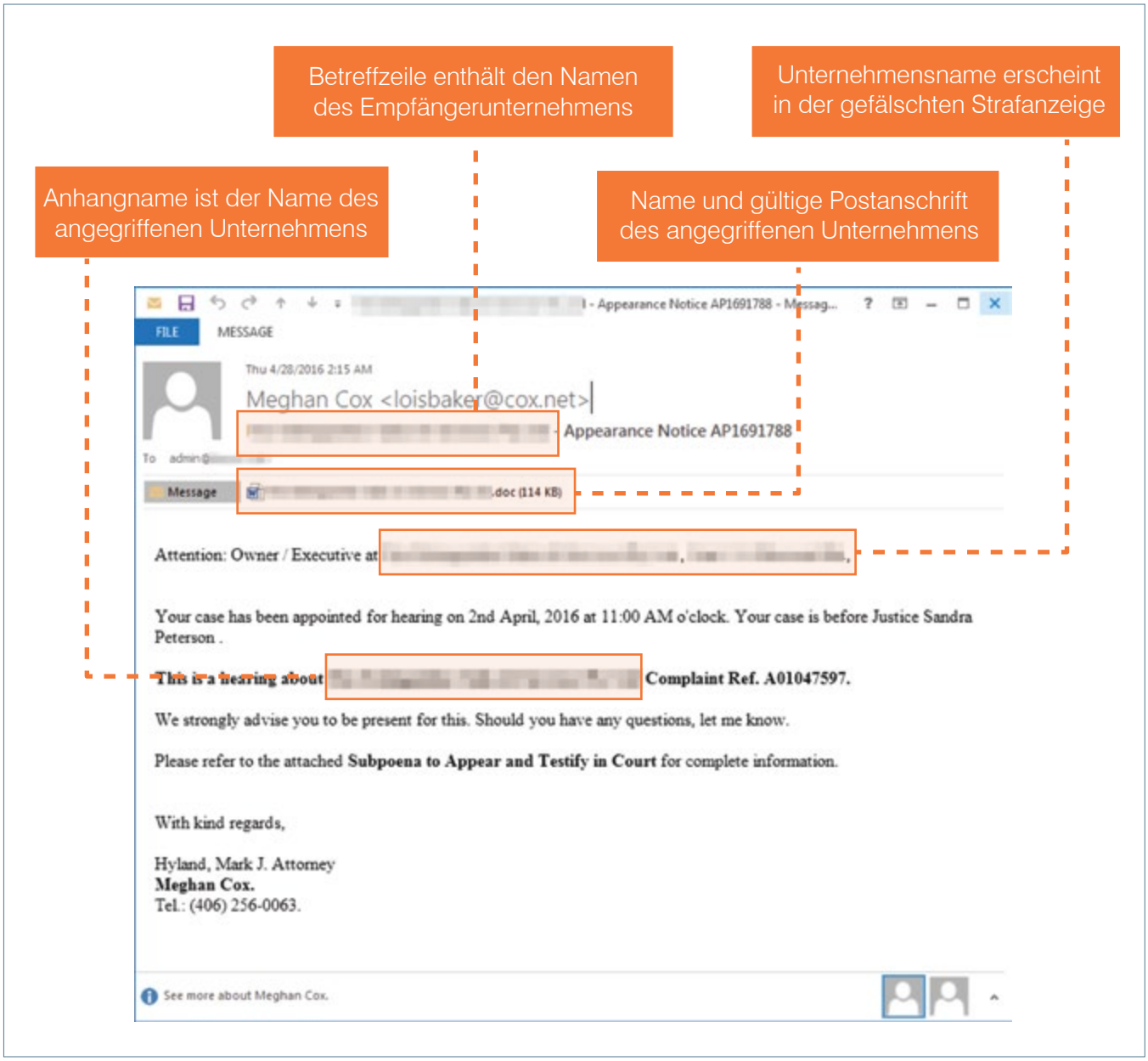
In einer gegen den Einzelhandel gerichteten Kampagne wurden in einer gefälschten Kundenbeschwerde die Adressen realer Ladengeschäfte genannt. Die E-Mail umfasste Dokumentanhänge, die vorgeblich weitere Details enthielten. Die Nachricht schloss mit der Warnung, dass der „Kunde“ die Beschwerde eskalieren würde, wenn sie nicht unverzüglich bearbeitet wird. Die angehängten Dokumente enthielten böswillige Makros – ein Klick auf die Schaltfläche „Inhalt aktivieren“ installierte die POS-Malware AbaddonPOS.

In einer weiteren Kampagne wurde behauptet, dass es sich bei den angehängten Dokumenten um Vorladungen für ein Gerichtsverfahren handeln würde. Auch hier sollten Social Engineering und persönliche Details in der E-Mail die Benutzer zum Öffnen des Anhangs verleiten. Das geöffnete Dokument ähnelte einer Vorladung, nutzte aber auch Social-Engineering-Methoden – ein übergeblendetes Bild mit einer Erklärung dazu, warum die Benutzer zum Lesen des Dokuments Makros aktivieren müssen. Durch das Aktivieren des Makros wurde der Bank-Trojaner Ursnif auf den PC des Opfers heruntergeladen.

TA530 stellte Cyberkriminellen ein breites Spektrum an Malware zur Verfügung. Das hohe Maß an Personalisierung sowie das für diese Kampagnen typische raffinierte Social Engineering ermöglichten die Ausnutzung des Faktors Mensch in großem Maße. Dadurch konnten zahlreiche und selbst erfahrene Benutzer zum Öffnen von Anhängen sowie Ausführen eines schädlichen Codes verleitet werden, was Bank-Trojanern, Informationsdieben und anderer Malware Tür und Tor öffnete.

ES WIRD PERSÖNLICH – ANALYSE EINES PERSONALISIERTEN ANGRIFFS

Zusätzlich zu den üblichen Tricks, mit denen Angreifer die Aufmerksamkeit eines potenziellen Opfers wecken und ein Gefühl der Dringlichkeit erzeugen, nutzen die personalisierten E-Mails, mit denen TA530 Malware verbreitete, auf das Unternehmen des Empfängers zugeschnittene Details. Techniken, die bisher bei kleinen und von Hand ausgearbeiteten Spearphishing-Kampagnen zum Einsatz kamen, wurden in den TA530-Kampagnen automatisiert, um hochvolumige Social-Engineering-E-Mail-Angriffe durchführen zu können.



SOCIAL ENGINEERING WIRD MOBIL

Obwohl diese Angriffsform nicht neu ist, nehmen SMS-Phishing-Attacken auf Verbraucher sowie Unternehmen zu, und die Akteure setzen immer neue Techniken zur Steigerung der Effektivität ein. Da für eingehende SMS-Nachrichten – im Gegensatz zu E-Mails – keine kommerziellen Filterprodukte angeboten werden, ist der Versand von SMS-Nachrichten aus Sicht der Angreifer eine sehr effektive Methode, um Benutzer zur Herausgabe ihrer Bankzugangsdaten zu verleiten.

42 % Zunahme der Benutzerklicks von Mobilgeräten auf böswillige URLs

Diese Schutzlücke wird dadurch verschärft, dass es auf den kleinen Bildschirmen von Mobilgeräten schwierig ist, die Echtheit von Webseiten zu erkennen. In der Vergangenheit umfasste SMS-Phishing meist eine Textnachricht mit einem einzigen Link, der auf eine gefälschte Kontoanmeldeseite führte, meist zu einem Telekommunikationsanbieter oder anderen Konten. Ende des Jahres 2016 stellten wir fest, dass die Angreifer neue Techniken und Methoden einsetzen, um das Potenzial der SMS-Phishing-Nachrichten noch besser ausnutzen zu können.

Unten sehen Sie ein Beispiel für eine Reihe von Phishing-Nachrichten, die Ende 2016 versendet wurden und vorgeblich von einer großen US-amerikanischen Bank stammen. Die Nachrichten wurden von E-Mail-Adressen sowie einer Telefonnummer gesendet und enthielten legitim erscheinende Links.

Statt die Benutzer direkt auf ein Phishing-Formular oder eine Webseite weiterzuleiten, führen die Links in Abb. 15 und 16 zuerst zu einem Bild (Abb. 17). Diese Technik überwindet viele Phishing-Filter, da der Link auf ein Bild verweist und daher nicht von automatisierten Tools analysiert werden kann. Nach sechs Sekunden werden die Opfer automatisch zur tatsächlichen Phishing-Webseite weitergeleitet.

Abb. 15: Phishing-SMS von einer Telefonnummer

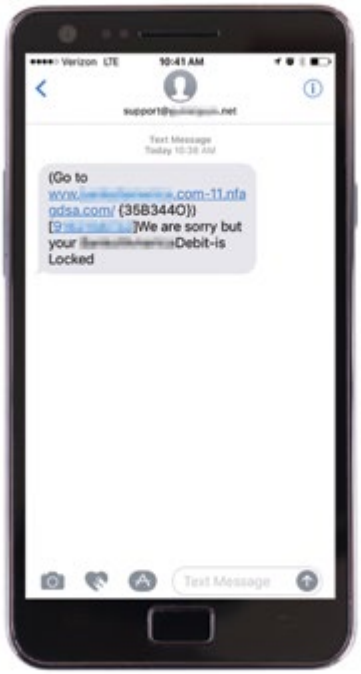


Abb. 16: Phishing-SMS von einer E-Mail-Adresse

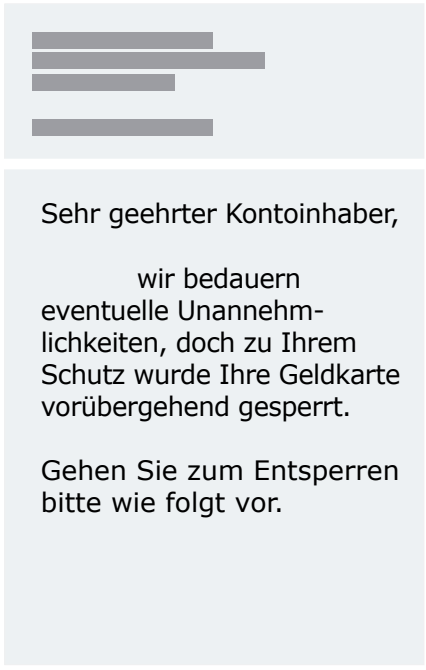


Abb. 17: Abbildung einer Phishing-Nachricht mit unkenntlich gemachten gefälschtem Unternehmensnamen

Die Phisher führen die Opfer anschließend durch einen raffinierten dreistufigen Prozess, der – im Gegensatz zu „herkömmlichen" Phishing-Webseiten, die gleich Kennwörter und Benutzernamen verlangen – zuerst die Telefonnummer und Postleitzahl des Opfers abfragt.

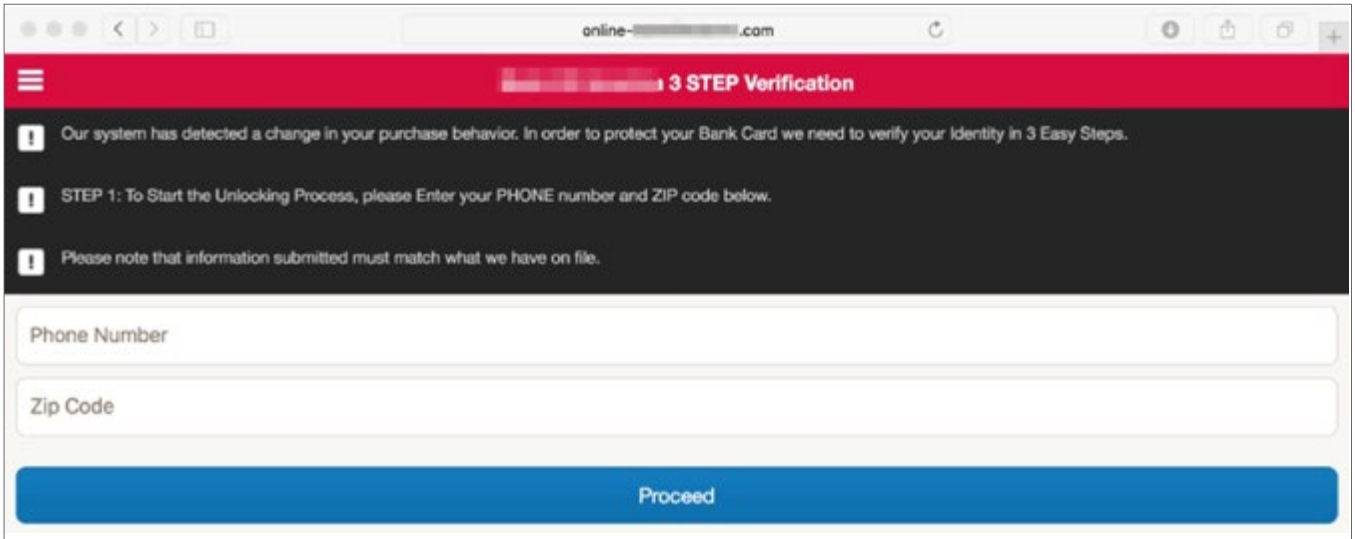


Abb. 18: Schritt 1 des gefälschten Verifizierungsprozesses, der mit der Abfrage von Telefonnummer und Postleitzahl beginnt; der unkenntlich gemachte Link nutzt eine Typosquatting-Domäne der Bank

Im nächsten Schritt des falschen Verifizierungsprozesses werden die Opfer zur Eingabe ihrer E-Mail-Adresse aufgefordert. Wenn die Empfänger eine Gmail- oder Yahoo!-Adresse eingeben, wird ihnen eine täuschend echte, aber gefälschte Anmeldeseite für diese Dienste angezeigt. Wenn die Opfer ihre Kennwörter eingeben, können die Angreifer die Kontrolle über das jeweilige Gmail- oder Yahoo!-Konto übernehmen und die Kennwörter aller weiteren Dienste zurücksetzen, die mit dieser E-Mail-Adresse verknüpft sind.

Zu diesem Zeitpunkt haben die Angreifer bereits die Telefonnummer, Postleitzahl, E-Mail-Adresse und das E-Mail-Kennwort ihrer Opfer erfasst. Der letzte Schritt des Angriffs leitet die Opfer zur Bankdaten-Phishing-Webseite zurück, wo sie zur Eingabe ihrer Kreditkartendaten und Identifikationsnummer aufgefordert werden. Selbst wenn die Empfänger nun misstrauisch werden, verfügen die Angreifer bereits über deren Telefonnummer und Zugang zum damit verbundenen E-Mail-Konto. Bei vielen Anbietern genügt das, um die Telefonnummer zu einem anderen Anbieter zu portieren und die Online-Identität des Opfers zu übernehmen. Da die Empfänger von Phishing-Nachrichten in vielen Fällen tatsächlich ihre Kreditkartendaten und Identifikationsnummer eingeben, können die Angreifer die Kreditkarte belasten und die Identitäten der Opfer stehlen.

SOCIAL-MEDIA-PHISHING: DIE KILLER-APP

Nach ihrem Auftauchen Ende 2015 haben betrügerische Kundendienstkonten in sozialen Netzwerken einen festen Platz in der Bedrohungslandschaft des Jahres 2016 erobert. Diese betrügerischen Konten, die bekannte Marken imitieren und Kundenanfragen beantworten, können täuschend echt wirken. Diese so genannten „Angler-Phishing"-Angriffe nahmen 2016 um 150 % zu, und im Laufe des Jahres wurden immer mehr Marken und Branchen attackiert.

Betrachten wir das Beispiel des Twitter-Benutzers „John Smith", der eine Frage an seine Bank tweetet, die hier als „Major Bank" (große Bank) mit dem Twitter-Namen „@majorbank" bezeichnet wird:

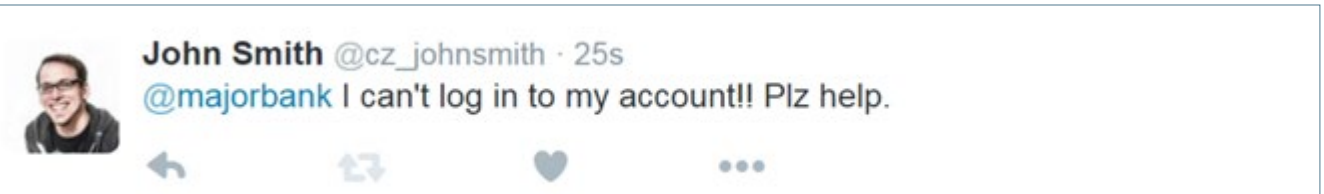


Abb. 19: Beispiel-Benutzerbeitrag

Da die Erwähnung von „@majorbank“ eine öffentliche Aktion auf Twitter ist, werden Angler-Phisher sofort darüber benachrichtigt, dass John Smith ein Kunde von Major Bank ist und Hilfe für sein Konto benötigt. Mithilfe dieser Information können sich die Angreifer in das Gespräch einklinken und John Smith antworten. Hier ein Beispiel für eine typische Antwort:

Abb. 20: Beispielantwort des Angler-Phishing-Angreifers, der den ursprünglichen Verfasser an die Phishing-Landing Page verweist

Das gefälschte Konto nutzt das Logo von „Major Bank“ und ein unverdächtiges Handle („@askmajorbank“). Legitime Support-Konten nutzen häufig andere Handles als das eigentliche Twitter-Konto der Marke, und viele Marken nutzen mehrere Konten für unterschiedliche Regionen, Produktfamilien usw. Selbst wenn John Smith also feststellt, dass sich das antwortende Handle von dem unterscheidet, das er angesprochen hat, weckt das nicht unbedingt Misstrauen. Social-Media-Bedrohungen treten weniger häufig auf als E-Mail-Phishing, sodass sich die meisten Benutzer wahrscheinlich gar nicht bewusst sind, dass sie angegriffen werden. Für den Fall, dass John Smith zum Anzeigen des Kontoprofils auf das Handle „@askmajorbank“ klickt, nutzen die meisten Angler-Phishing-Konten gestohlene Markeninhalte, um das legitime Profil der Marke nachzuahmen.

John Smith, der sich über die schnelle Antwort freut und keinen Zweifel an der Authentizität des Gesprächspartners hat, klickt auf den angebotenen Link zu „majorbankCA.com“. Diese Seite ahmt die reguläre Online-Banking-Anmeldeseite von Major Bank täuschend echt nach. John Smith gibt seine persönlichen Daten, darunter seine Bankkontonummer und die Anmeldedaten, ein und wird damit zu einem Phishing-Opfer. Leider sind sich weder John Smith noch Major Bank bewusst, dass das Konto jetzt kompromittiert ist.

Als unsere Forscher Ende 2015 zum ersten Mal auf diese Phishing-Form stießen, richteten sich die Angriffe vornehmlich gegen Kunden großer Banken. Sie fanden zwei bis drei Mal im Monat statt und griffen eine Handvoll Konten an. Bis Ende 2016 stieg die Häufigkeit bei einigen großen Banken auf zwei bis drei Versuche am Tag. Zudem richten sich die Angriffe auf Kunden anderer Branchen, darunter Online-Banken, Medienunternehmen sowie Firmen aus dem Unterhaltungssektor. Bei vielen dieser Angriffe kommen Komponenten zum Phishing von E-Mail-Adressen und Kennwörtern, Links zu Malware sowie weitere kriminelle Aktivitäten zum Einsatz.

ANGRIFFSZIEL: SPIELER

Ebenso wie viele andere gezielte Betrugsformen in sozialen Netzwerken treten Angler-Phishing-Angriffe zu besonderen angekündigten Ereignissen häufiger auf. So entdeckten wir zum Beispiel Angler-Phishing-Konten, die Benutzer mit dem „Gewinn“ von spielinternen Preisen lockten. Dazu sollten die Benutzer auf Phishing-Links klicken, die scheinbar auf einen großen Spielehersteller verwiesen. Diese Konten imitierten legitime Konten zum Spiel oder des Spieleherstellers und waren besonders in der Launch-Phase neuer Produkte aktiv.

GEFÄLSCHTE MOBILGERÄTE-APPS: AUSNUTZUNG DES FAKTORS MENSCH NUN AUCH UNTERWEGS

Im Jahr 2015 sowie Anfang 2016 erstellten Cyberkriminelle häufig Kopien beliebter Mobilgerätespiele, die für die Benutzer unsichtbaren böswilligen Code enthielten. Ende 2016 richteten sich die Mobilgeräte-Angriffe gegen Kunden bestimmter Banken, Mitarbeiter bestimmter Branchen, Veranstaltungsteilnehmer und andere. Angreifer nutzen gefälschte Marken, irreführende App-Namen sowie andere Täuschungsmethoden, um Benutzer zum Herunterladen versteckter Malware auf ihre Mobilgeräte zu verleiten.

Beispielsweise analysierten wir vor Kurzem eine Android-Beispiel-App, die in China im Umlauf war und als POS-Kontroll-App für einen großen POS-Systemhersteller auftrat. Das unten gezeigte in Chinesisch geschriebene Symbol verweist auf den Hersteller und zeigt eines seiner tatsächlichen POS-Systeme.

Während der Installation fordert die App umfangreiche Berechtigungen an, die sie für ihre eigentliche Aufgabe nicht benötigt. Die angeforderten Berechtigungen weisen darauf hin, dass es sich bei der App in Wirklichkeit um einen raffinierten Informationsdieb handelt, der dauerhaft im Hintergrund ausgeführt wird.

Ein weiteres Beispiel für eine getarnte App tauchte Ende 2016 im iOS-App-Store auf. Sie gab sich als Online-Banking-Anleitung aus und bot zahlreiche Tipps und Tricks für die offizielle App einer großen US-amerikanischen Bank. Weiter unten sehen Sie die Listung der App im iOS-App-Store.

Nach ihrer Installation bietet die App einen Nachrichten-Feed sowie einen Link zu weiteren Apps an (siehe Abb. 24). Bei der Anleitung selbst handelt es sich zwar nicht um Malware, doch die Artikel führen häufig auf Phishing-Webseiten und die verlinkten Apps enthalten Sideloading-Adware.

Dies ist kein Einzelfall. Mehr als 1 % aller weltweiten App-Entwickler – also mehr als 16.000 – verteilen böswillige Apps über die großen App-Stores sowie Drittanbieter-App-Stores. Die meisten geben sich als legitime Apps aus, sind jedoch alles andere als harmlos.

Abb. 21: Symbol einer gefälschten POS-App

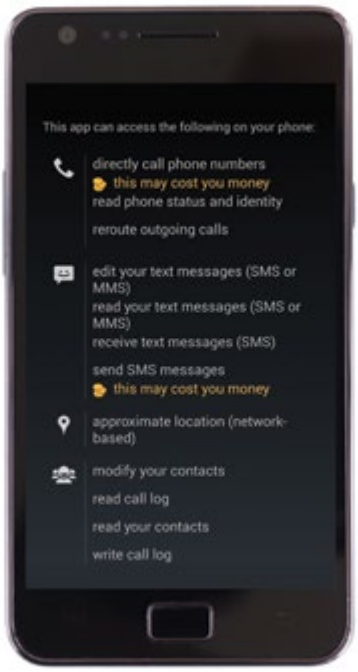


Abb. 22: Ausschnitt der Berechtigungen, die von der gefälschten POS-App angefordert werden

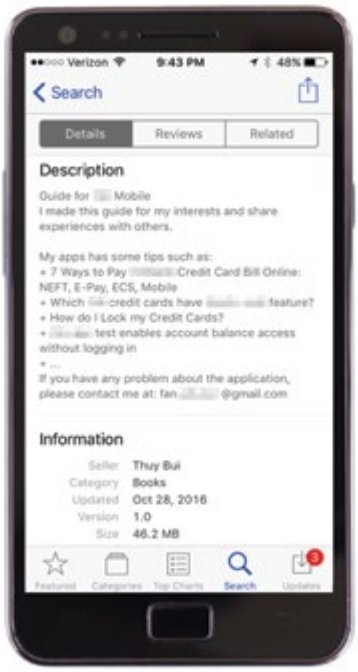


Abb. 23: Beschreibung einer Mobile Banking-Anleitung unter iOS

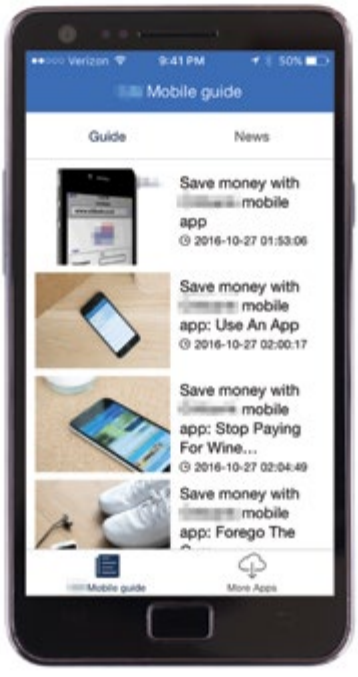


Abb. 24: Die Anleitungs-App agiert als Vermittler für Sideloading-Adware und verweist auf verschiedenste Phishing-Webseiten, die teilweise in anderen Ransomware-Kampagnen zum Einsatz kamen

ZUSAMMENFASSUNG

Die starken Veränderungen in der Bedrohungslandschaft, die bereits im Jahr 2015 begannen, setzen sich im gesamten Jahr 2016 sowie im laufenden Jahr 2017 fort. Während Exploit-Kits einen immer geringeren Anteil von Nachrichten mit böswilligen URLs ausmachen, führen mehr als 90% dieser Links inzwischen zu anderen Seiten, zum Beispiel zu Anmeldedaten-Phishing. Gleichzeitig nahm Ransomware explosionsartig zu, und bei gezielten Angriffen wurden neue Vektoren mit E-Mails kombiniert. Soziale Netzwerke gehören jetzt fest in das Arsenal der Angreifer: Angler-Phishing-Angriffe, die immer mehr Marken und Branchen ins Visier nehmen, nahmen um 150% zu.

Phishing-Kampagnen wechselten im Jahr 2016 zu neuen Kanälen wie zum Beispiel Mobilgeräten. Die Opfer dieser Angriffe erhalten häufig SMS-Nachrichten und E-Mails, die zur Eingabe von Anmeldeinformationen auffordern. Die Rate, mit der Mitarbeiter auf SMS-Nachrichten mit böswilligen Links klicken, lag im Jahr 2016 bei 42%, während die langfristige Rate bei lediglich 20% lag.

Angriffe, die auf menschliches Verhalten abzielen, spielten 2016 eine zentrale Rolle. Die Angreifer nutzen Automatisierung und Personalisierung, um das Volumen und die Klickraten ihrer Kampagnen zu erhöhen. Cyberkriminelle orientieren sich an Playbooks für E-Marketer im B2B-Bereich und nutzen die dort empfohlenen Vorgehensweisen, indem sie ihre Kampagnen an Dienstagen und Donnerstagen senden, wenn die Klickraten höher liegen. Gleichzeitig zielen BEC- und Anmeldedaten-Phishing-Angriffe direkt auf den Faktor Mensch ab, sodass sie ohne technische Exploits auskommen. Stattdessen verleiten sie ihre Opfer mit Social-Engineering-Taktiken dazu, Geld zu überweisen oder vertrauliche Informationen sowie Kontoanmeldedaten weiterzugeben.

Das Timing ist entscheidend: Die Angreifer wissen, dass eine optimal gestaltete und zum richtigen Zeitpunkt an Ihre Mitarbeiter gesendete E-Mail die besten Ergebnisse erzielt. Die Details variieren natürlich je nach Region. Wenn Sie also für die weltweiten Sicherheitsabläufe verantwortlich sind, müssen Sie nicht nur die typischen Angriffsmuster kennen, sondern auch wissen, welche Mitarbeiter zu welchem Zeitpunkt besonders häufig klicken.

EMPFEHLUNGEN

Konzentrieren Sie Ihre Sicherheitsmaßnahmen auf den wichtigsten Vektor für eingehende Bedrohungen: E-Mails. Setzen Sie Schutzlösungen ein, die den E-Mail-Fluss überwachen und Angriffe stoppen, bevor sie Ihre Mitarbeiter erreichen können.

Verwenden Sie Bedrohungsanalysedienste, die zur Untersuchung von Verhaltensweisen, Code und Protokollen mehrere Ansätze nutzen und dadurch Bedrohungen in Anhängen und URLs erkennen können. Je früher böswillige Inhalte innerhalb der Angriffskette identifiziert werden, desto schneller lassen sie sich blockieren, eindämmen und beseitigen.

Implementieren Sie cloudbasierte Sandbox-Analysedienste, die für den Schutz aller Mitarbeiter in Ihrem Unternehmen skaliert werden können. Der Dienst sollte in der Lage sein, Angriffskampagnen zu identifizieren und neue Angriffsmethoden, Taktiken und Ziele zu erkennen, sodass der nächste Angriff einfacher aufgedeckt werden kann.

Schützen Sie Ihre Außendienstmitarbeiter, indem Sie für deren Mobilgeräte die gleichen Sicherheitskontrollen bereitstellen wie für die unternehmenseigenen PCs im Büro. Außendienstmitarbeiter sind immer häufiger die Quelle für Klicks auf böswillige Links. Eine weiterer neuer Angriffsvektor sind SMS-Nachrichten. Ihre Lösung sollte Klicks auf böswillige URLs von Smartphones und Tablets erkennen und blockieren – inner- und außerhalb des Netzwerks sowie unabhängig vom Standort.

Wehren Sie Betrugsversuche mit Angler-Phishing-Konten oder böswilligen Apps ab, die mit Ihrer Marke Geld verdienen wollen. Verwenden Sie eine Lösung, die nach betrügerischen Konten und Anwendungen sucht, die App-Stores sowie Ihre Auftritte in sozialen Netzwerken missbrauchen.

Zu guter Letzt: Beschleunigen Sie Ihre Reaktion auf Zwischenfälle. Suchen Sie nach einer Lösung, mit der Sie bereits in den Postfächern Ihrer Benutzer eingegangene böswillige E-Mails entfernen können. Diese Lösung sollte dafür sorgen, dass Ihre Benutzer keinen Zugriff mehr auf böswillige E-Mails haben. Zudem sollte sie über eine Geschäftslogik verfügen, mit der bereits weitergeleitete Kopien dieser Nachrichten gefunden und entfernt werden können.

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