proofpoint

BERICHT

EMAIL FRAUD THREAT REPORT

DAS JAHR IM RÜCKBLICK

E-MAIL-BETRUG-BEDROHUNGSBERICHT

proofpoint.com

E-Mail-Betrug, auch BEC (Business Email Compromise) genannt, ist heutzutage eine der häufigsten Cyberbedrohungen. Diese per Social Engineering ausgeführten Angriffe richten sich mehr auf Personen als auf Technologie. Es handelt sich um sehr zielgerichtete, in geringem Umfang gesendete E-Mails, in denen sich Betrüger als Authoritätspersonen ausgeben.

E-Mail-Betrug zielt auf die menschliche Natur ab – auf Ängste, den Wunsch, andere zufriedenzustellen und mehr – um Geld und wertvolle Informationen von Mitarbeitern, Kunden und Geschäftspartnern zu stehlen.

Proofpoint analysierte über 160 Milliarden E-Mails, die an mehr als 2.400 Unternehmen in 150 Ländern gesendet wurden.

Hier sehen Sie unsere Erkenntnisse für 2017.

E-MAIL-BETRUG
Bei E-Mail-Betrug wird vorgetäuscht, dass eine E-Mail, bzw. eine Reihe von E-Mails von einer Führungskraft oder einem Geschäftspartner stammen. Angeblich bittet der Ansprechpartner den Empfänger um die Überweisung eines Geldbetrags oder zur Herausgabe empfindlicher Informationen. Es werden keine schädlichen Anhänge oder URLs verwendet, daher lässt sich diese Methode schwer erkennen und stoppen.

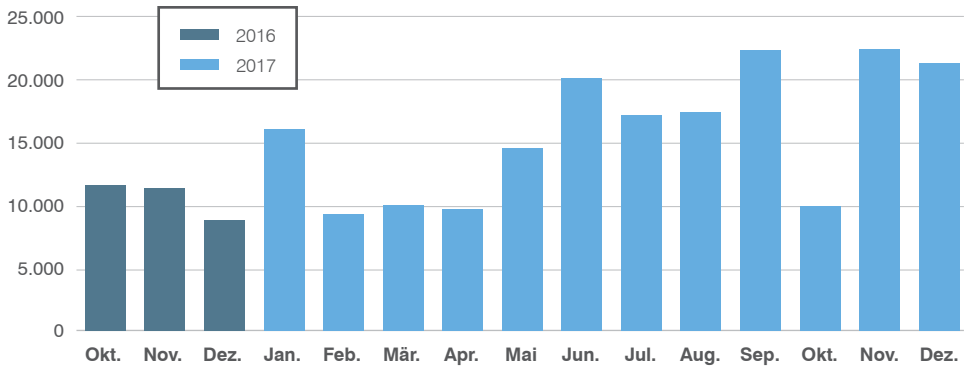
E-MAIL-BETRUG STEIGT WEITER

E-MAIL-BETRUG grassierte 2017. Während die Bedrohungen nach wie vor sehr gezielt ausgeführt werden, wurden die Angriffe im Vgl. zu 2016 häufiger und an mehr Unternehmen gesendet.

Der Prozentsatz an Unternehmen mit mindestens einem E-Mail-Betrugsangriff nahm stetig zu und erreichte im 4. Quartal ein neues Hoch von 88,8 %. Das sind 13,8 Prozentpunkte mehr als die 75 % an Unternehmen, die im selben Quartal des Vorjahres angegriffen wurden.

Im Durchschnitt wurden Unternehmen pro Quartal von 18,5 betrügerischen E-Mails attackiert, was 17 % mehr entspricht als im Jahr davor. Wenn man nur das reine Volumen berücksichtigt, endete das Jahr mit zwei der drei wichtigsten Quartale für E-Mail-Betrug, die wir je gesehen haben.

Proofpoint erkennt und blockiert BEC(Business Email Compromise)-Angriffe
Die Quartale 3 und 4 waren die umfangreichsten bzgl. des Volumens von E-Mail-Betrug, die wir je gesehen haben.



BETRÜGER REICHEN AUF DEM ORGANISATIONSPLAN IMMER WEITER NACH UNTEN

Kriminelle beschränken sich bei ihrem Angriff auf Organisationen nicht mehr auf CEO-an-CFO-Betrug.

Vortäuschen mehrerer Identitäten

Nachdem die ersten drei Quartale stabil verliefen, mehr als verdoppelte sich die durchschnittliche Anzahl an Personen, die pro Organisation betrügerisch nachgeahmt wurden, im vierten Quartal auf ca. 10.

Diese Verlagerung macht Sinn. Während die Sicherheitsteams alle Angestellten vor CEO-Betrug warnen, finden die „bösen Buben“ andere Authoritätsfiguren, die sie verkörpern können. Im vierten Quartal wurden in nahezu der Hälfte (47 %) aller Organisationen jeweils mehr als 5 Identitäten personifiziert – das sind fast doppelt so viele wie im vorherigen Quartal.

Mehr Rollen werden anvisiert

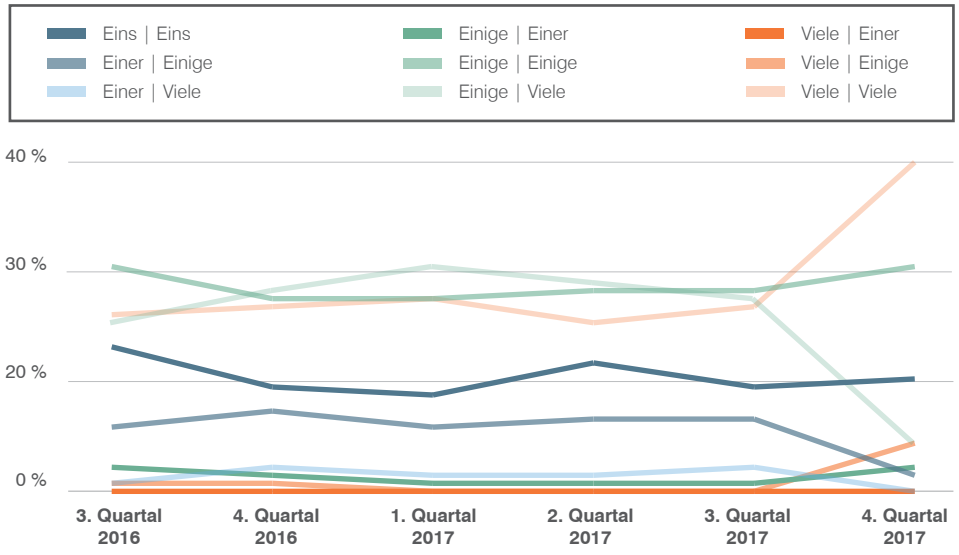
Die durchschnittliche Anzahl der Zielpersonen in einem Unternehmen stabilisierte sich im 4. Quartal bei etwa 13. Doch Kriminelle zielen auf Opfer ab, die einer größeren Anzahl an Geschäftsgruppen angehören bzw. auch tiefer auf dem Organigramm stehen, so beispielsweise HR und Lieferantenkonten. In vielen Fällen verfassen sie überzeugende E-Mails mithilfe von Social Engineering und anhand von Mitarbeiterinformationen, die im Web und auf sozialen Medien überall verfügbar sind.

Im 4. Quartal gruben die Angreifer noch tiefer im Organigramm und 41 % der angepeilten Unternehmen sahen sich Angriffen ausgesetzt, in denen mehr als 5 Identitäten nachgeahmt und über 5 Mitarbeiter angegriffen wurden.

„ONE-TO-ONE“-ANGRIFF
Beim „One-to-One“E-Mail-Angriff ahmt der Betrüger eine Identität nach (normalerweise die des CEO) und zielt auf einen Empfänger ab (üblicherweise den CFO).

„MANY-TO-MANY“-ANGRIFFE
Bei „Many-to-Many“-Angriffen verkörpern die Betrüger mehrere Führungskräfte und greifen mehrere Empfänger an. Beispiel: Ein Angreifer kann versuchen, mehrere Manager zu verkörpern und das gesamte Finanzteam des Unternehmens anzugreifen.

Erkannte Nachahmungen gegenüber gesendete E-Mails
Von der einfachen **One-to-One**-Attacke gehen Betrüger dazu über, sich als immer mehr Authoritätsfiguren auszugeben und damit mehr Personen im Unternehmen unter Beschuss zu nehmen. Wir nennen dies **Many-to-Many**-Angriffe.



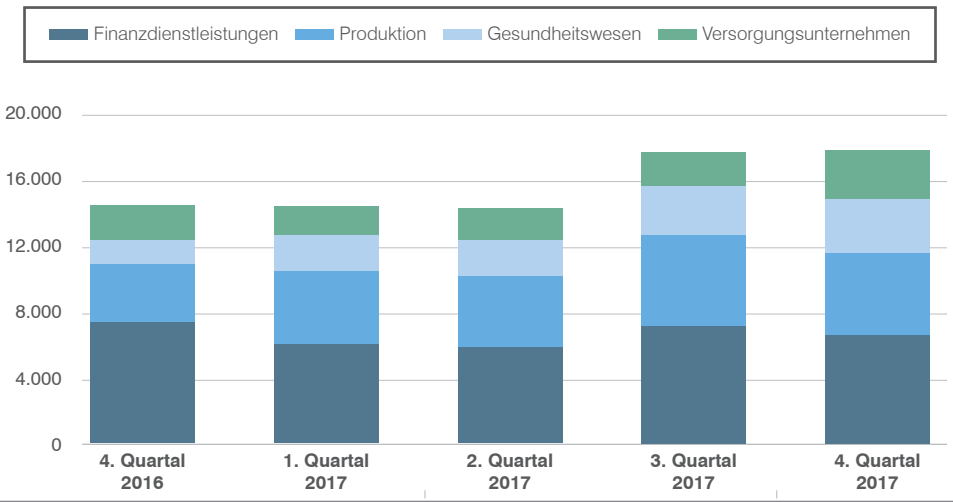
FÜR DIE BETRÜGER SPIELT DIE GRÖSSE KEINE ROLLE

Betrüger greifen Organisationen jeder Größe an. Außerdem sind sie opportunistisch und zielen auf Unternehmen in allen Branchen ab.

Unternehmen aller Größen unter Attacke

Wir konnten praktisch keine Verbindung zwischen der Unternehmensgröße und der Häufigkeit der Angriffe über E-Mail-Betrug feststellen, seit wir 2016 anfingen, diese Informationen zu sammeln. Nur ein Quartal (2. Quartal 2017) zeigte überhaupt irgendeine Korrelation – die Betrüger zeigten eine leichte Präferenz für größere Ziele.

Angreifer zielen auf viele Branchen ab
Die Branchen Finanzdienste und Herstellung befinden sich unter den häufigsten Zielen. Doch wir sahen breitgefächerte E-Mail-Betrugsangriffe über alle Branchen hinweg.



Das die Angreifer kleine und große Ziele gleichermaßen anpeilen, scheint zu überraschen. Doch vom Standpunkt des Angreifers aus macht dieses Muster Sinn. Größere Organisationen sind zwar lukrativer, aber kleinere Unternehmen sind oftmals anfälliger für diese fortschrittlicheren Bedrohungen.

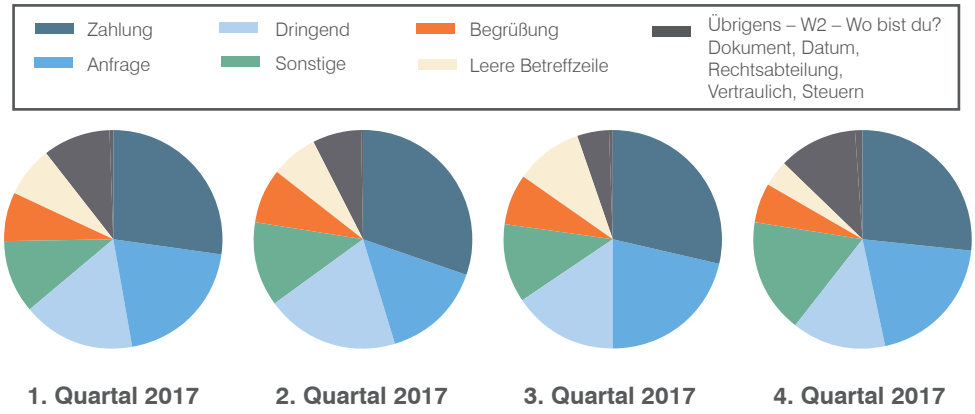
Kriminelle greifen viele Branchen an
In früheren Studien sahen wir meist eine gleichmäßige Verteilung von E-Mail-Betrugsversuchen über alle Branchen hinweg. (Obwohl die Sektoren Finanzdienste, Herstellung, Gesundheitswesen und Energie/Versorgung etwas mehr angezielt wurden.)

Im 4. Quartal hatten es die Betrüger auf neue Branchen abgesehen. Auf dem Gebiet der Immobilien fanden Kriminelle neue Wege, aus hochkarätigen Transaktionen Kapital zu schlagen. Im Ausbildungswesen stiegen die Angriffe gegenüber dem vorherigen Quartal sprunghaft um 77 % und gegenüber dem gleichen Zeitraum des Vorjahres um 120 % an.

VERLAGERUNG DER E-MAIL-BETRUGSTAKTIKEN

Um traditionelle Sicherheitstools zu umgehen und ihre Opfer zu erreichen, ändern die Betrüger ständig ihre Methoden.

Betreffzeilen bei E-Mail-Betrugsversuchen
„Zahlung", „Anfrage" und „Dringend" sind immer beliebte Betreffzeilen, doch wir sahen einen Anstieg an rechtsbezogenen Betreffzeilen im 4. Quartal



Überweisungsbetrug
ÜBERWEISUNGSBETRUG ist mit nahezu 27 % des E-Mail-Betrugsvolumens nach wie vor die häufigste Form des E-Mail-Betrugs. E-Mail-Betreffkategorien enthalten normalerweise eine Variante des Wortes „Zahlung".

Steuerbetrug
W2-STEUERDOKUMENTBETRUG stieg jeweils in den ersten Quartalen der vergangenen beiden Jahre an, wahrscheinlich wegen des näherrückenden U.S.- Abgabetermins. Beispiel: Im 1. Quartal sahen wir gegenüber dem vorangehenden Quartal eine Steigerung um 3,408 %. Im 2. Quartal, nach Ende des Abgabetermins, sank das Volumen dieser Angriffe auf ein stetiges Maß.

Neue Rollen und Betreffszeilen
Angreifer nehmen verschiedene Rollen an, um eine vertraute Authorität zu personifizieren. Im Verlauf von 2017 verlagerten sich E-Mail-Angriffe zwischen Betreffskategorien, die „Dringend" enthielten zu solchen mit dem Inhalt „Anfrage".

„Dringend" und „Anfrage"
Nachrichten, die unter die Betreffskategorie „Dringend" fallen, sind üblicherweise direkter und sehr prägnant. Nachrichten mit dem Wort „Anfrage" in der Betreffszeile lassen einen sanfteren Ansatz erkennen. Sie bauen eine längere Korrespondenz auf, bevor Sie sich nach den begehrten Informationen erkundigen.

„Rechtsabteilung"
Zwei weitere Betreffskategorien, die im 4. Quartal häufiger vorkamen: solche mit einem Datum und solche, die „Rechtsabteilung" enthielten.

Obwohl sich dies zahlenmäßig in Grenzen hielt, stiegen Angriffe mit einem Rechtsansatz um 1,850 % im Vergleich zum Vorjahr an. Den größten Anstieg verzeichneten Betrügereien, deren Betreff lautete: „Anruf vom Rechtsanwalt".

ÜBERWEISUNGSBETRUG
Beim Überweisungsbetrug sendet der Betrüger eine E-Mail, in der er sich als Führungskraft ausgibt. Die E-Mail soll den Empfänger dazu überlisten, Geld zu überweisen, indem der Transfer als normale Geschäftstransaktion oder wichtige Handlung ausgegeben wird, die unter Geheimhaltung durchgeführt werden muss.

W2-STEUERFORMULARBETRUG
Bei diesem Betrug ahmt jemand eine Führungskraft nach und bittet die Finanzabteilung, Mitarbeiterakten zu senden. Diese Akten werden dann für Identitätsdiebstahl oder andere Angriffe verwendet. Er wurde nach dem W2-Steuerformular der USA benannt, das Mitarbeiter zum Einreichen der Steuererklärung verwenden.

Bei diesen Angriffen versucht der Kriminelle in der Regel, die Interaktion von der E-Mail wegzulenken und die Überweisung telefonisch zu erwirken. Diese Angriffe funktionieren, da der Angreifer jemanden verkörpert, der zwar Autorität besitzt, mit dem Opfer jedoch normalerweise keinen Kontakt hat. Und da der Kontakt weitestgehend offline stattfindet, ist der Betrug für Sicherheitsteams schwerer zu erkennen und zu stoppen.

Fabrizierte E-Mail-Verläufe

Betrugsversuche, die einen gefälschten E-Mail-Verlauf umfassen, sind 2017 in jedem Quartal angestiegen.

Diese Methode verwendet „Re:“ (AW) oder „Fwd:“ (WE) im Betreff, einen gefälschten E-Mail-Verlauf oder beides. Die fabrizierte E-Mail-Kette enthält einen völlig realistischen E-Mail-Verlauf, der den Eindruck erweckt, dass die erforderlichen Stakeholder bereits ihr Einverständnis für die Anfrage gegeben haben.

Im 4. Quartal enthielten über 11 % aller BEC-Angriffe eine Version dieser Methode. Das ist ein Anstieg um 7,3 % seit demselben Quartal des Vorjahres.

HÄUFIGSTE ANGRIFFSMETHODEN MIT NACHAHMUNG VON DOMÄNEN- UND ANZEIGENAMEN

Im Verlauf 2017 schwankte die Mischung von betrügerischen E-Mail-Nachrichten zwischen Angriffen mit Domänennachahmung, Anzeigenamennachahmung und ähnlichen Domänen (oder verwandten Domänen).

DOMÄNENNACHAHMUNG
Beim Nachahmen (Spoofing) wird ein vertrauter Kollege oder Kontakt verkörpert, wobei die betrügerische E-Mail scheinbar von einer rechtmäßigen und erwarteten Adresse stammt.

ANZEIGENAMEN-NACHAHMUNG
Beim Domänennamen-Spoofing werden ein bekannter Name und eine vertraute E-Mail-Adresse ins Absenderfeld eingesetzt, das der Benutzer auf der eingehenden E-Mail sieht. Wenn der Empfänger antwortet, geht die Antwort tatsächlich an die in der Kopfzeile angegebene E-Mail-Adresse unter „Antworten an“.

DMARC
Bei DMARC (steht für „Domain-based Message Authentication, Reporting and Conformance“) handelt es sich um ein E-Mail-Authentifizierungsprotokoll, das viele E-Mail-Betrugsangriffe verhindern kann.

Domänennachahmung

ANGRIFFE MIT DOMÄNENNACHAHMUNG, in denen Kriminelle die vertraute Domäne eines Unternehmens übernehmen, stellen nach wie vor einen großen Teil des E-Mail-Betrugs dar. Im 4. Quartal sahen 69 % aller per E-Mail-Betrug angegriffenen Unternehmen mindestens einen Angriff durch Domänennachahmung. Und 2017 wurden insgesamt 93 % aller Organisationen von einem solchen Angriff attackiert.

Anzeigenamennachahmung

IM 4. QUARTAL TRUG DIE NACHAHMUNG VON ANZEIGENAMEN durch webbasierte E-Mail-Dienste zu ca. 40 % aller E-Mail-Betrugsangriffe bei. Aol.com und gmail.com waren bei diesen Bedrohungen die bevorzugten Absender-Domänen, obwohl die Angreifer auch viele andere Domänen verwendeten.

DMARC-Übernahme

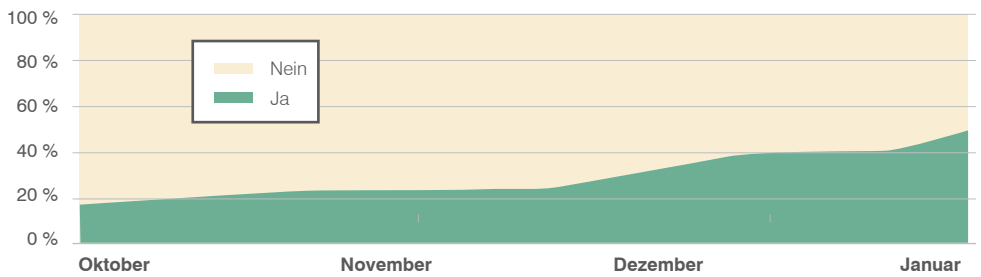
Angriffe durch Domänennachahmung können vermieden werden, indem eine **DMARC**-E-Mail-Authentifizierung eingesetzt wird. Es ist kein Wunder, dass erhebliche Initiativen ins Leben gerufen wurden, um die DMARC-Übernahme 2017 zu erhöhen.

Im Oktober brachte das US-Ministerium für innere Sicherheit (Homeland Security) die verbindliche Betriebsrichtlinie 18-01 heraus. Die Richtlinie zielt darauf ab, die Sicherheit von Personen zu erhöhen, die E-Mails von Bundesanstalten erhalten oder Bundeswebsites besuchen. Ein wichtiger Teil der Anweisung weist alle zivilrechtlichen Bundesagenturen an, DMARC so schnell wie möglich bereitzustellen.

Zum Zeitpunkt der Herausgabe der Anweisung war nahezu eine von acht E-Mails von einer .gov-E-Mail-Adresse betrügerischer Herkunft. Nur ca. 17 % der Agenturen setzten DMARC ein.

Ca. 90 Tage nach Beginn der Initiative hatte sich dieser Prozentsatz mehr als verdreifacht. Fast 52 % der Agenturen haben den ersten DMARC-Meilenstein erreicht.

Bundes-DMARC-Entwicklung unter zivilen Behörden
Immer mehr Agenturen bauen als Folge einer Bundesverordnung E-Mail-Authentifizierungen ein. Doch fast die Hälfte hat den ersten Meilenstein noch nicht erreicht.



Kurz nach Ankündigung der Richtlinie bat das NH-ISAC (National Health Information Sharing and Analysis Center) – eine Industriegruppe, die Gesundheitsdienstleistern hilft, Daten sicher weiterzugeben – sich zu verpflichten, DMARC 2018 einzusetzen.

EIN NÄHERER BLICK AUF ÄHNLICHE DOMÄNEN

ÄHNLICHE DOMÄNE
Beim Nachahmen von Domänen registrieren die Betrüger Domänennamen, die denen von vertrauten Marken zum Verwechseln ähnlich sehen.

DAS NACHAHMEN VON DOMÄNEN, bei denen der Angreifer eine Domäne registriert, die einer vertrauten Domäne zum Verwechseln ähnlich sieht, ist eine weitere wirksame Taktik. Angreifer überlisten Leute mit E-Mails, die von einer bekannten Quelle zu stammen scheinen, dazu, wertvolle Informationen preiszugeben.

Die Angreifer gestalten diese gefälschten Domänen, indem sie schwer erkennbare Änderungen an der Originaldomäne vornehmen. Sie vertauschen einzelne Zeichen, z. B. eine „0“ statt einem „O“. Oder sie schieben Zeichen ein, wie beispiesweise ein „S“ am Ende der Domäne.

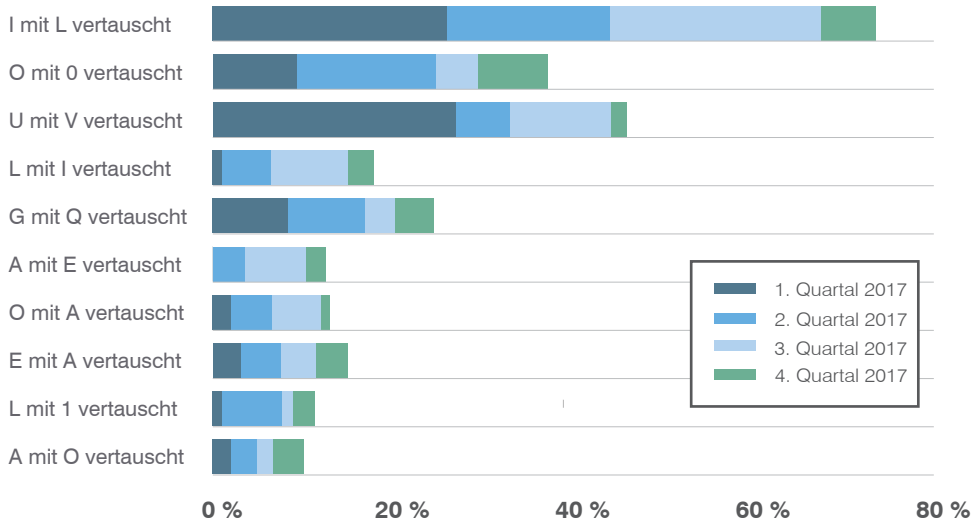
Die Menge der Angriffe mit ähnlichen Domänen ist nicht so groß wie die Nachahmung von Anzeigenamen oder die allgemeine Domänennachahmung. Das liegt wahrscheinlich daran, dass der Betrüger für diese Methode eine Domäne registrieren muss, was Geld kostet. Doch angesichts der Tatsache, dass eine einzelne vertraute Domäne zahllose ähnliche Varianten haben könnte, haben die Angreifer viele Gelegenheiten, solche Angriffe zu starten.

Zeichenaustausch

Wie bei anderen E-Mail-Betrugstaktiken ändern sich auch die Methoden der ähnlichen Domänen jedes Quartal. Doch im Verlauf 2017 war die beliebteste Methode mit nahezu 38 % das Austauschen von Zeichen. Am häufigsten wurden folgende Zeichen ausgetauscht:

- Ein L statt einem I (17,4 %)
- Eine 0 statt des Buchstaben O (8,7 %)
- V statt U (8 %)

Zeichenaustausch auf ähnlichen Domänen
Weil manche Zeichen anderen ähneln haben Betrüger viele Optionen zum Erstellen von Domänen, die so aussehen wie Ihre.



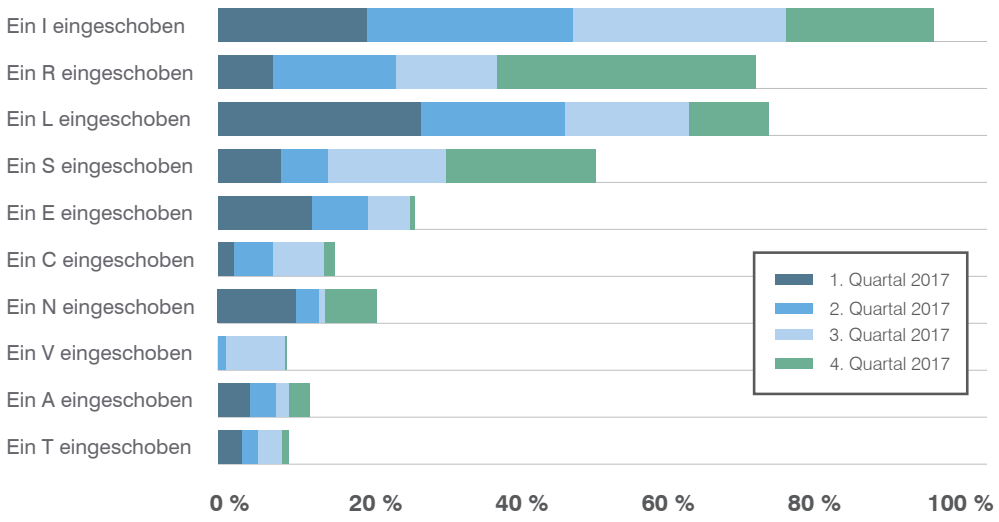
Einschub von Zeichen

Betrügerdomänen mit einem zusätzlichen Buchstaben traten im Verlauf des Jahres in ca. 34 % der Fälle auf. Die häufigsten Einschübe waren:

- Ein I (23,7 %)
- Ein R (19,3 %)
- Ein L (15,4 %)

Zeicheneinschub in ähnlichen Domänen

In E-Mail-Adressen sind zusätzliche Zeichen manchmal schwer zu erkennen, wodurch Betrüger neue Variationen vertrauter Domänen erstellen können.



Andere Methoden

Eine weitere beliebte Methode ist das Einfügen oder Entfernen eines führenden oder nachfolgenden Zeichens in der Domäne. Dieser Ansatz trug zu ca. 13 % der registrierten ähnlichen Domänen bei.

Zu weiteren Nachahmungstaktiken für ähnliche Domänen gehören:

- Hinzufügen eines Bindestrichs
- Entfernen von Zeichen
- Typografie und **HOMOGRAFIE**

HOMOGRAF-SPOOFING

Beim Homograf-Spoofing werden Zeichensätze von verschiedenen Sprachen vermischt, um ähnliche Domänen zu erstellen, die dem bloßen Auge identisch erscheinen, aber vom Computer unterschieden werden. Beispiel: Eine unsichere Domäne verwendet ein kyrillisches „A“, das zwar genauso aussieht wie das lateinische „A“, das in der vertrauten Domäne verwendet wird.

SCHLUSSFOLGERUNG UND EMPFEHLUNGEN

Trotz der umfangreichen Investitionen der Unternehmen in die Sicherheit, nimmt der E-Mail-Betrug zu. Cyberkriminelle werden immer besser. Sie umgehen traditionelle Sicherheitslösungen und hinterlassen Mitarbeiter als die letzte Verteidigungslinie.

Die Taktiken der E-Mail-Betrüger wandeln sich ständig. Darum brauchen Sie eine mehrschichtige Abwehr, die Folgendes umfasst:

1. **DMARC-E-Mail-Authentifizierung**. Blockierung aller Betrügerangriffe, die vertraute E-Mail-Domänen nachahmen.
2. **Dynamische Klassifizierung**. Analyse von Inhalt und Kontext der E-Mail, um Anzeigenamen-Spoofing und Doppelgänger-Spoofing bereits am E-Mail-Gateway zu stoppen.
3. **Erkennung ähnlicher Domänen.** Erkennen und Markieren potenziell gefährlicher Domänen, die von Fremdunternehmen registriert wurden.
4. **Data Loss Prevention.** Vermeiden, dass empfindliche Daten, z. B. W2-Steuerformulare, Ihre Umgebung verlassen.

SIND SIE AUSGERÜSTET, UM E-MAIL-BETRUG ZU STOPPEN?

Lassen Sie eine kostenlose DMARC-Bewertung ausführen, um schnell zu verstehen, welches potenzielle Risiko Sie tragen und wie die DMARC-Authentifizierung bei der Vorbeugung gegen E-Mail-Betrug helfen kann.

proofpoint.com/de/learn-more/dmarc-assessment

ÜBER PROOFPOINT

Proofpoint Inc. (NASDAQ: PFPT), ein Unternehmen für Internetsicherheitslösungen der nächsten Generation, ermöglicht Organisationen, das Arbeitsumfeld ihrer Mitarbeiter vor fortschrittlichen Bedrohungen und Compliance-Risiken zu schützen. Proofpoint hilft Internetsicherheitsexperten dabei, ihre Anwender vor den hochentwickelten Angriffen zu schützen, die in E-Mails, mobilen Apps und in den sozialen Netzwerken gegen sie gerichtet werden. Es schützt die wichtigen Daten, die Menschen erstellen, und stattet Teams mit den richtigen Informationstools aus, die ihnen bei Problemen eine schnelle Reaktion ermöglichen. Führende Unternehmen aller Größenordnungen, darunter mehr als 50 % der Fortune 100-Unternehmen, vertrauen auf Proofpoint-Lösungen, die für die mobilen und von den sozialen Netzen geprägten Umgebungen der heutigen Zeit konzipiert sind. Zur Bekämpfung der modernen Bedrohungen stützen sich die Lösungen sowohl auf die Macht der Cloud als auch auf eine große datengesteuerte Analyseplattform.

proofpoint. www.proofpoint.com