Spear Phishing: Top-Bedrohungen und Trends

Ausgabe 6 Juli 2021

Einblicke in die sich entwickelnden Taktiken der Angreifer und deren Zielgruppen

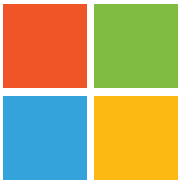
Ob es darum geht, den Hype um Kryptowährungen auszunutzen, Anmeldedaten zu stehlen, einen Ransomware-Angriff zu starten oder Angriffe auf weniger verdächtige Ziele in unauffälligen Rollen zuzuschneiden – Cyberkriminelle passen ihre Taktiken stetig an und gestalten ihre Angriffe immer raffinierter. Dieser fundierte Bericht behandelt die aktuellsten Trends in Sachen Spear Phishing sowie die neuen Tricks, mit denen Angreifer ihre Opfer hinters Licht führen.»

Barracuda
Your journey, secured.

Inhaltsverzeichnis

Zentrale Ergebnisse

1 von 10 Social-Engineering-Angriffen beruhen auf **Business E-Mail Compromise**



43 % der Phishing-Angriffe geben sich als **Microsoft** aus

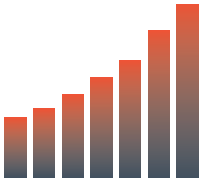
Ein durchschnittliches Unternehmen wird **in einem Jahr von über 700 Social-Engineering-Angriffen** heimgesucht

1 von 5 BEC-Angriffen (Business Email Compromise) zielt auf **Mitarbeiter in Vertriebsfunktionen** ab

77 % der BEC-Angriffe zielen auf **Mitarbeiter außerhalb der Finanz- und Führungsebene** ab

IT-Mitarbeiter verzeichnen **in einem Jahr durchschnittlich 40 gezielte Phishing-Angriffe**

Im Durchschnitt erhält ein **CEO 57 gezielte Phishing-Angriffe** in einem Jahr



Kryptowährungsbedingte Identitätsmissbrauchs-Angriffe **stiegen zwischen Oktober 2020 und April 2021 um 192 %**

Zunehmende Komplexität der E-Mail-Bedrohungen

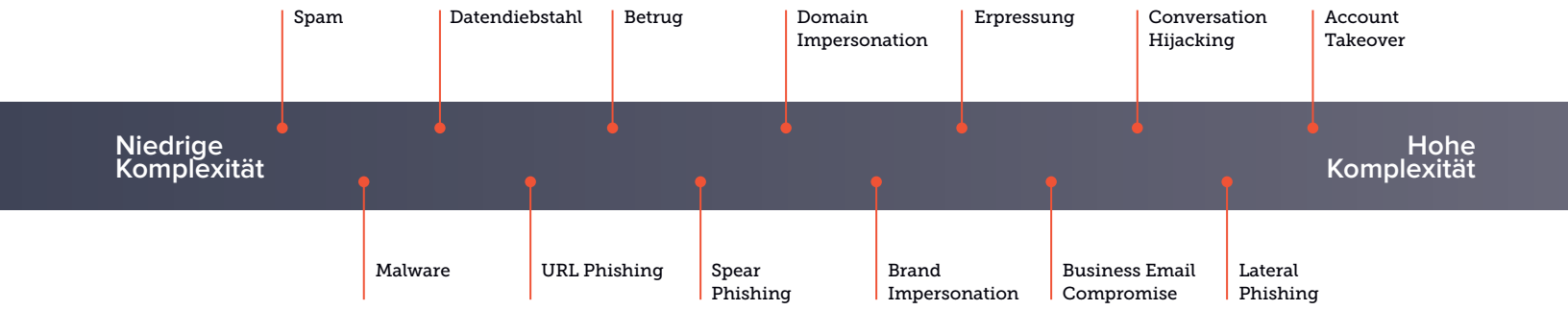
In den letzten Jahrzehnten haben Security-Anbieter in den Schutz vor E-Mail-Angriffen investiert, und der für ihre Kunden entwickelte Schutzumfang hat sich bei der Blockierung der meisten bösartigen oder unerwünschten E-Mail-Nachrichten als wirksam erwiesen.

Obwohl Unternehmen die Möglichkeit haben, Millionen von Angriffe zu stoppen, sind E-Mail-Bedrohungen immer noch erfolgreich und werden immer komplexer. Es ist ein echter Wandel von volumetrischen zu gezielten Angriffen im Gange, von Malware zu Social Engineering, von einzelnen Hackern zu organisierten kriminellen Unternehmen, die von Angriffen profitieren, die mit einer einzigen Phishing-E-Mail beginnen.

Alte Methoden des E-Mail-Schutzes, die sich auf Regeln, Richtlinien, Erlaubnis- oder Sperrlisten, Signaturen und andere Attribute der traditionellen E-Mail-Sicherheit stützen, sind gegen die wachsende Bedrohung durch Social-Engineering-Angriffe nicht mehr wirksam.

Die Forscher von Barracuda haben 13 unterschiedliche Arten der E-Mail-Bedrohung ermittelt, denen Unternehmen aktuell ausgesetzt sind. Das Spektrum reicht von breit gestreuten Angriffen wie Spam oder Malware bis hin zu zielgerichteten Bedrohungen mit Social-Engineering-Komponenten wie Business Email Compromise und Identitätsmissbrauch.

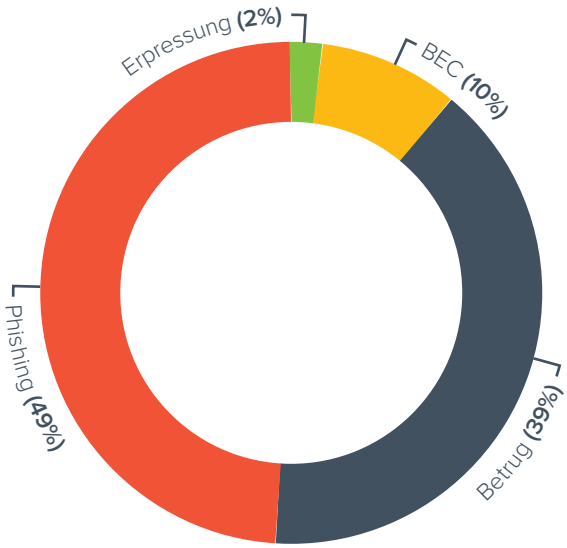
13 Arten von E-Mail-Bedrohungen



Hacker verwenden eine Kombination von Taktiken, um die Benutzer zu einer Aktion zu verleiten, z. B. die Preisgabe ihrer Anmeldedaten, damit die Angreifer Zugriff auf die Unternehmensumgebung erhalten oder einen Ransomware-Angriff starten können, die Weitergabe vertraulicher Informationen, die verkauft oder für weitere Angriffe verwendet werden könnten, oder einfach das Senden einer Zahlung, von Geschenkkarten oder Geldüberweisungen.

Zwischen Mai 2020 und Juni 2021 analysierten Barracuda-Forscher mehr als 12 Millionen E-Mail-Angriffe, die mehr als 3 Millionen Postfächer bei rund 17.000 Unternehmen betrafen. Bei dieser Analyse haben wir vier verschiedene Kategorien von Social-Engineering-Angriffen verfolgt:

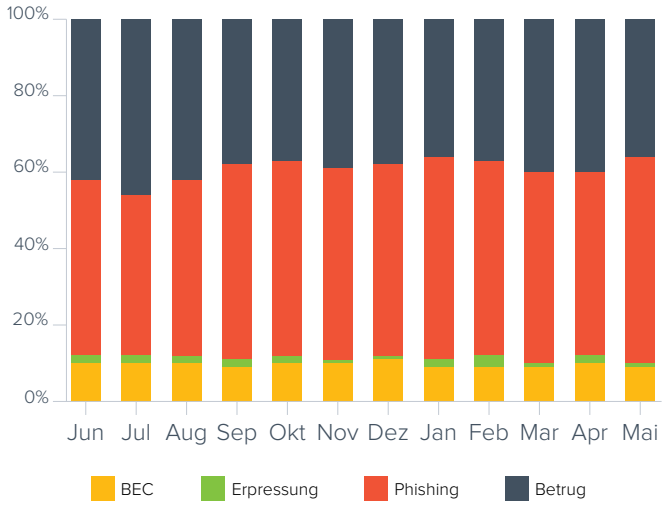
Social Engineering Angriffe (Juni 2020 - Mai 2021)



Business Email Compromise, abgekürzt BEC – Diese Angriffe beinhalten in der Regel den Identitätsmissbrauch einer Person entweder innerhalb oder außerhalb einer Organisation. Im vergangenen Jahr machten diese Angriffe 10 % aller Social-Engineering-Angriffe aus, die wir analysiert haben, mit steigender Tendenz. Das Bildungswesen, das Gesundheitswesen, der Handel, die Reisebranche – Unternehmen aus jeder Branche wurden Opfer eines dieser Angriffe und haben dabei oft Millionen von Dollar verloren. Bei einem typischen BEC-Angriff gibt sich ein Hacker als Mitarbeiter aus, in der Regel eine Führungskraft, und veranlasst Überweisungen, fordert Geschenkkarten oder die Überweisung von Geld an gefälschte Wohltätigkeitsorganisationen.

Phishing-Identitätsmissbrauch – Diese Angriffe geben sich in der Regel als E-Mails einer bekannten Marke oder eines Dienstes aus, um die Opfer dazu zu bringen, auf einen Phishing-Link zu klicken. Diese Angriffe machen 49 % aller Social-Engineering-Bedrohungen aus, die wir im letzten Jahr analysiert haben. Fast alle Angriffe in dieser Kategorie enthalten eine bösartige URL. Obwohl Phishing-E-Mails nichts Neues sind, haben Hacker inzwischen ausgeklügelte Methoden entwickelt, um nicht entdeckt zu werden und ihre bösartige Payload in die Posteingänge der Benutzer zu liefern. Sie verkürzen URLs, setzen zahlreiche Umleitungen ein und hosten bösartige Links auf Filesharing-Seiten, um E-Mail-Scan-Technologien zu umgehen. Auch bei Phishing-Identitätsmissbrauch ist ein Aufwärtstrend zu verzeichnen. Diese Angriffe machten im Juni 2020 46 % aller von uns erkannten Social-Engineering-Angriffe aus und stiegen bis Ende Mai 2021 auf 56 %.

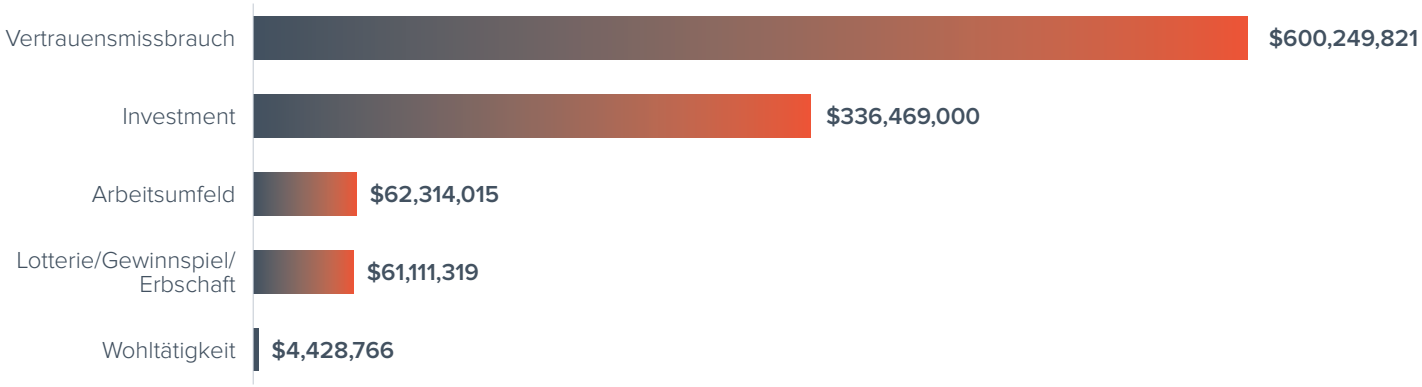
Social Engineering Angriffe im letzten Jahr



Erpressungsangriffe machen nur 2 % der Gesamtzahl der gezielten Phishing-Angriffe aus, die wir im vergangenen Jahr analysiert haben. Bei diesen Angriffen handelte es sich meist um E-Mail-Bedrohungen mit Erpressung, bei denen Hacker damit drohen, sensible oder peinliche Inhalte an die Kontakte ihres Opfers weiterzugeben, wenn kein Lösegeld gezahlt wird. Die Forderungen belaufen sich in der Regel auf ein paar Hundert oder ein paar Tausend Dollar und müssen in Bitcoin bezahlt werden, was potenziell schwer nachzuverfolgen ist. Da so viele Menschen im Homeoffice arbeiten, wurde Zoom im Zusammenhang mit diesen Angriffen mehrfach erwähnt, manchmal mit Verweis auf Jeffrey Toobins weithin bekannten Skandal. Die Anzahl der dem FBI gemeldeten Erpressungsangriffe im Jahr 2020 stieg im Vergleich zum Vorjahr um 78 %, und die geschätzten Verluste betrugen über 70 Millionen US-Dollar. Diese Betrügereien können auch sehr tragische Folgen haben, die über monetäre Verluste hinausgehen. Es kam unter Opfern dieser Betrügereien auch zu Selbstmord, weil sie die Veröffentlichung ihres Privatlebens befürchteten.

Betrügerische Angriffe können viele Formen annehmen und reichen von angeblichen Lotteriegewinnen und nicht beanspruchten Geldern oder Paketen bis hin zu gefälschten Geschäfts- und Stellenangeboten, Spenden und anderen Betrugsmaschen. Sie sind tendenziell etwas weniger zielgerichtet als die oben beschriebenen Angriffsarten, doch stellen betrügerische Angriffe 39 % aller Social-Engineering-Angriffe dar, die wir im vergangenen Jahr nachgewiesen haben, und sie sind nicht weniger erfolgreich. Da Hacker mit den verschiedenen von ihnen entwickelten Arten von Betrügereien ein weites Netz auswerfen, werden die Opfer um Hunderte Millionen von Dollar gebracht. Im vergangenen Jahr nutzten Hacker zum Beispiel COVID-19 in ihren investitionsbezogenen Betrügereien, um Investitionen in betrügerische Coronavirus-Behandlungen oder -Impfstoffe zu erhalten.

Kosten von Betrugs-Angriffen



Source: FBI Internet Crime Complaint Center Internet Crime Report 2020

...Betrugs-Angriffe entsprechen 39% aller Social Engineering Angriffe, die wir letztes Jahre entdeckt haben...»

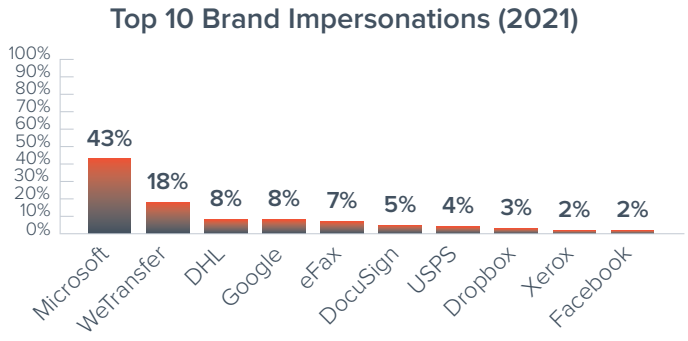
Phishing Identitätsmissbrauch von Top-Marken

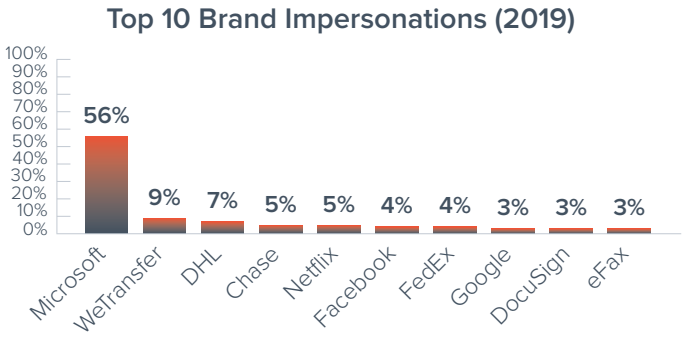
Die Identität einer bekannten und vertrauten Marke anzunehmen ist ein alter Trick vieler Hacker. Menschen neigen dazu, Mitteilungen von unseren Lieblingsmarken zu erwarten, und es ist umso wahrscheinlicher, dass sie diesen vertrauen. Seit 2019 sind die drei meistgenutzten Marken bei Phishing-Angriffen gleich geblieben – Microsoft, WeTransfer und DHL.

79 % der Unternehmen nutzen Office 365 und viele weitere planen eine Migration in naher Zukunft. Es ist daher nicht überraschend, dass Microsoft-Marken ein Top-Ziel für Cyberkriminelle bleiben.

Betrachtet man die Top 10 der imitierten Marken, so wurde Microsoft in den letzten 12 Monaten bei 43 % der Phishing-Angriffe verwendet. Hacker machen sich die zunehmende Beliebtheit von Microsofts Cloud-basierten Diensten und die Verlagerung zum externen Arbeiten im letzten Jahr zunutze. Cyberkriminelle senden gefälschte Security-Warnungen oder Informationen zur Kontoaktualisierung an ihre Opfer, um sie zum Anklicken eines Phishing-Links zu bringen. Das Ziel dieser Angriffe ist einfach: Stehlen von Anmeldedaten, um Zugang zu Unternehmensnetzwerken zu erhalten. Von dort aus können die Hacker andere Arten von Angriffen starten, einschließlich Ransomware.

Ein kompromittiertes Konto kann in Unternehmen echten Schaden anrichten. Anfang dieses Jahres wurde Colonial Oil Pipeline Opfer einer Ransomware-Attacke, die Berichten zufolge durch kompromittierte Passwörter ermöglicht wurde. Obwohl eine Lösegeldzahlung in Höhe von 4,5 Millionen US-Dollar geleistet wurde, um den Betrieb wiederherzustellen, sind die tatsächlichen Kosten des Schadens kaum zu beziffern.





Der Online-Dateiübertragungsdienst WeTransfer ermöglicht es Benutzern, große Dateien auszutauschen, die sie möglicherweise nicht direkt per E-Mail versenden können. Diese Marke spielte bei 18 % der Phishing-Angriffe eine Rolle. Hacker senden Phishing-E-Mails, in denen sie zum Anmelden und Bestätigen von Kontoinformationen, zum Herunterladen potenziell schädlicher Dateien oder zur Weitergabe von Zahlungsangaben auffordern oder technischen Support anbieten. WeTransfer wurde bei Phishing-Angriffen in den letzten Jahren immer häufiger imitiert – von 9 % im Jahr 2019 auf 18 % Mitte 2021. Dieser Anstieg kann auf die steigende Beliebtheit des Dienstes und zusätzliche Möglichkeiten zurückgeführt werden, wie Hacker Filesharing-Seiten in ihren Angriffen nutzen können.

Einige Angriffe nutzen WeTransfer bei einem Phishing-Angriff als Zwischenwebsite. Die ursprüngliche E-Mail enthält einen legitimen Link zu einer Datei auf WeTransfer und durchläuft daher E-Mail-Scans. Sobald sie jedoch geöffnet wird, enthält die Datei einen Link zu einer Phishing-Website, die oft genauso aussieht wie die Anmeldeseite von Office 365 und fragt nach Anmeldedaten, um auf die Datei zuzugreifen. Diese Art von Redirect-Angriffen unter Verwendung von Filesharing-Websites wird immer beliebter.

To:
From: Microsoft <cloud@boxshare.biz>
Reply to:
Date: Nov 30, 2020 6:28 AM

Subject: Introducing OneDrive

Introducing Microsoft OneDrive

SHARED DOCUMENTS RECEIVED

Please login to Your Organization Cloud Storage to View Documents

Go To OneDrive

Logistik- und Speditionsunternehmen sind auch regelmäßig unter den wichtigsten Marken mit Identitätsmissbrauch. Etwa 12 % der Angriffe verwendeten entweder das Branding von DHL oder USPS, um gefälschte Updates zu Sendungen und Zustellungen bereitzustellen. Hacker haben sich die Tatsache zunutze gemacht, dass im vergangenen Jahr so viele Menschen zu Hause festsaßen und immer mehr Sendungen erhielten.

Andere Marken, die es 2021 in die Top 10 geschafft haben, waren Google, DocuSign und Facebook. Wenn eines dieser Konten kompromittiert wird, erhalten Hacker eine Fülle von persönlichen Informationen, die sie für weitere Angriffe nutzen können.

To:
From: EXPRESSDHL <trackingdhl-2021-@skynet.be>
Reply to:
Date: Mar 03, 2021 4:02 PM

Subject: EXPRESS SHIPMENT TRACKING NUMBER ... 978526330211

Hello,

Your DHL Express shipment with waybill number 978526330211
is waiting for delivery. Please confirm the payment details in the following link below.

The current Status of the shipment is: On Hold.

to complete your delivery options **Here**

DELIVERY INFORMATION

Waybill No.	978526330211
Available for delivery	We will message you when ready
Opening hours	Monday - Sunday 00:00-23:59 Holiday 00:00-23:59
Delivery Time	By End of Day

Thank you for using On Demand Delivery.
DHL Express – Excellence. Simply delivered?

DHL Express | Contact DHL | Privacy Policy | Unsubscribe

Ziel-Identität

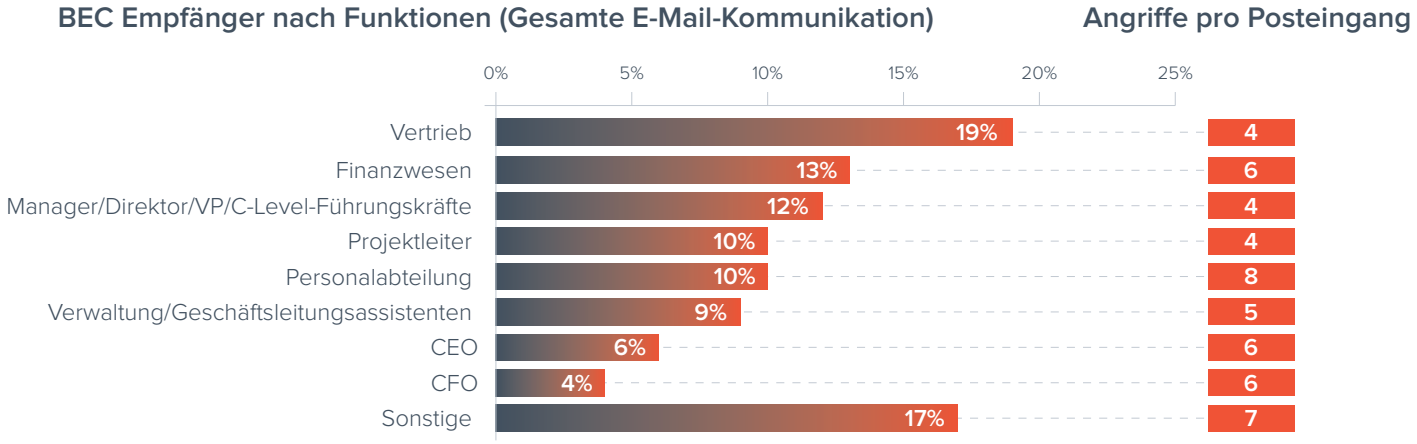
Spear-Phishing-Angriffe werden durch ihre gezielte Art definiert. Angreifer verbringen Zeit damit, ihre Opfer und deren Unternehmen zu recherchieren, indem sie Angriffe entwickeln, die bestimmte Personen mit einer individuellen Botschaft ansprechen. Es gibt viele öffentlich zugängliche Quellen und Social-Media-Websites, über die sich Angreifer ein relativ genaues Bild der Personen innerhalb eines Unternehmens und der Art ihrer Rollen verschaffen.

Basierend auf unserer Analyse wird ein durchschnittliches Unternehmen in einem Jahr von über 700 Social-Engineering-Angriffen heimgesucht. Unsere Forscher analysierten die 100 am häufigsten angegriffenen Geschäftstitel und die Art der Angriffe, die sie erhalten. Wir haben alle schon von CEO- und CFO-Betrug gehört, aber ist der CFO wirklich der am meisten gefährdete Mitarbeiter innerhalb des Unternehmens? Gibt es noch andere Ziele, auf die Hacker gerne ihre Bemühungen konzentrieren?

BEC-Angriffe

BEC-Angriffe zielen auf die unterschiedlichsten Rollen innerhalb des Unternehmens ab. Bei einem klassischen BEC-Angriff gibt sich jemand als Führungskraft aus und konzentriert sich auf Mitarbeiter in der Finanzabteilung, einschließlich des CFO oder anderer Personen mit Zugang zu Geldmitteln, um diese zu einer betrügerischen Zahlung zu verleiten. Interessanterweise waren im vergangenen Jahr bei etwa 4 % aller BEC-Angriffe CFOs betroffen, während 13 % dieser Angriffe auf andere Mitarbeiter in der Finanzabteilung abzielten. Dies lässt sich zum Teil durch die Größe der Finanzabteilung erklären, die in der Regel eine Reihe von Mitarbeitern hat, während CFO eine Einzelrolle ist. Mitglieder von Finanzabteilungen erhielten im Durchschnitt sechs gezielte BEC-Angriffe, genauso viele wie ein CFO.

Vertriebspositionen erhielten die meisten BEC-Angriffe, was jedoch hauptsächlich auf die Anzahl der Vertriebsmitarbeiter in den Unternehmen zurückzuführen ist. Die durchschnittliche Anzahl von Angriffen pro Postfach betrug vier, was unter dem Durchschnitt liegt. Aufgrund der Art ihrer Rolle sind Vertriebsmitarbeiter daran gewöhnt, externe Nachrichten von Absendern zu erhalten, mit denen sie vorher nicht kommuniziert



haben. Gleichzeitig sind sie alle mit der Buchhaltung und mit anderen Abteilungen verbunden, einschließlich der Finanzabteilung. Für Hacker stellen diese Personen einen perfekten Einstiegspunkt in ein Unternehmen dar, um andere Angriffe zu starten.

Auch Verwaltungsmitarbeiter und Geschäftsleitungsassistenten sind beliebte Ziele. Diese Personen haben in der Regel Zugang zu den Kalendern oder Konten der Führungskräfte. Sie werden oft hinsichtlich Geschenkgutscheinbetrug oder Diebstahl von Zugangsdaten anvisiert.

Viele Unternehmen konzentrieren ihre Schulungs- und Schutzmaßnahmen auf die Personen, die ihrer Meinung nach innerhalb des Unternehmens am stärksten betroffen sind: in der Regel Führungskräfte und Finanzabteilungen. Allerdings zielten 77 % der BEC-Angriffe auf Mitarbeiter in anderen Abteilungen ab. Angreifer suchen nach einem Einstiegspunkt und einem schwachen Glied in Ihrem Unternehmen und arbeiten sich dann an wertvollere Konten heran. Dies unterstreicht die Notwendigkeit, jeden Mitarbeiter auf dem gleichen Niveau zu schützen und zu schulen.

Phishing-Angriffe

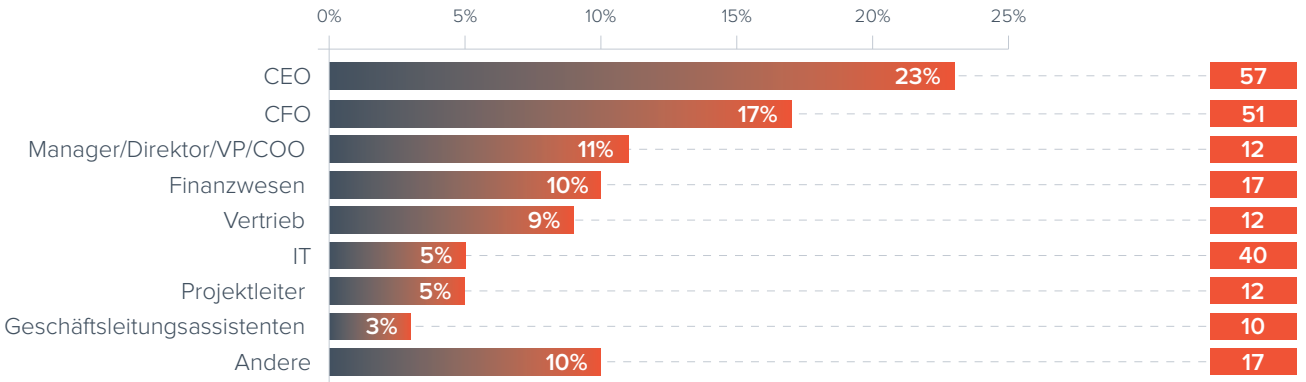
Phishing-Angriffe, die sich als ein Dienst oder eine Business-Anwendung ausgeben, beinhalten in der Regel eine Phishing-URL mit dem Ziel, Kontodaten oder andere wertvolle Informationen zu stehlen. Hacker zielen mit diesen Angriffen auf verschiedene Rollen ab.

Führungsteams und Personen auf Managementebene erhielten die meisten Phishing-Angriffe. Diese Konten sind für Hacker sehr wertvoll, da sie oft wichtige Korrespondenz enthalten, die für weitere Angriffe genutzt werden kann.

Wenn wir uns die Anzahl der auf IT-Teams ausgerichteten Phishing-E-Mails ansehen, obwohl diese nur 5 % der gesamten Angriffe ausmachen, waren auf jeden Mitarbeiter 40 E-Mail-Angriffe ausgerichtet, was weit über dem Durchschnitt liegt. IT-Mitarbeiter haben Zugriff auf geschäftskritische Anwendungen, sodass die Kompromittierung ihrer Konten für Hacker äußerst wertvoll sein kann, durch die sie Zugriff auf die Sicherheits- und IT-Infrastruktur von Unternehmen erhalten. Cyberkriminelle schneiden ihre Angriffe auf ihre Opfer zu, daher gab es kaum BEC-Angriffe auf IT-Teams, da diese in der Regel auf schnelle monetäre Gewinne aus sind. Bei Angriffen mit Phishing-URLs, die auf die Kompromittierung von Konten abzielen, war die IT jedoch eines der Top-Ziele.

Unternehmen müssen darauf achten, welche Mitarbeiter von welchen Arten von Bedrohungen betroffen sind. Diese Erkenntnisse können genutzt werden, um relevantere und effektivere Schulungen zur Stärkung des Risikobewusstseins zu konzipieren.

Phishing Empfänger nach Funktionen (Gesamte E-Mail-Kommunikation) **Angriffe pro Posteingang**



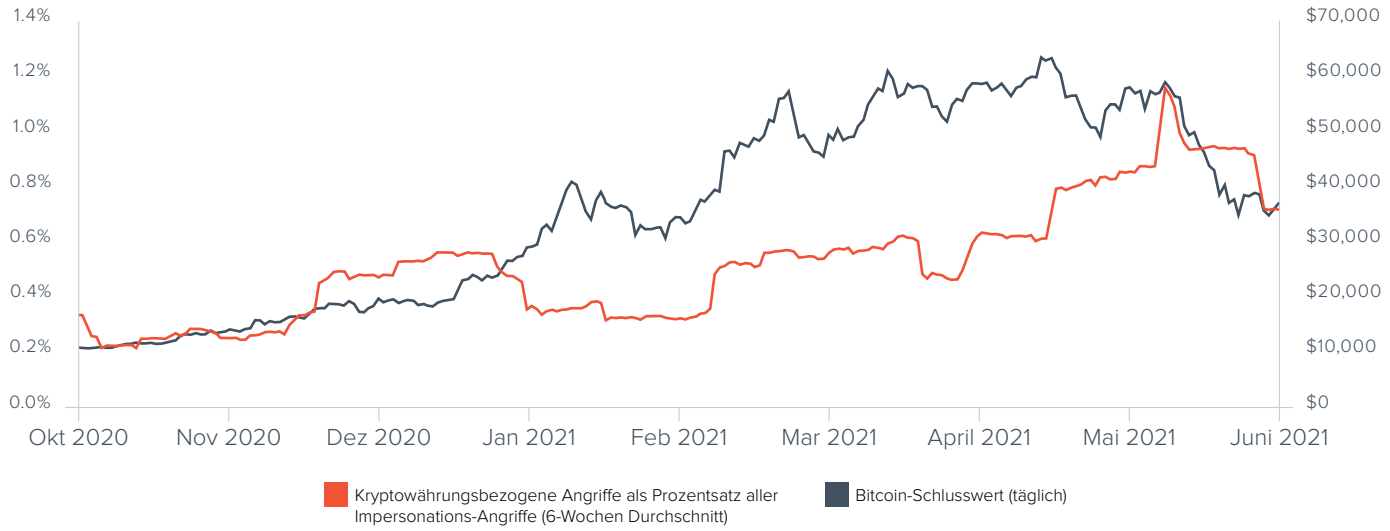
Kryptowährung und Spear Phishing

Kryptowährung ist eine Art von Währung, die nur in einem digitalen Format verfügbar ist. Ihre dezentrale Natur und mangelnde Regulierungen haben Kryptowährung zur bevorzugten Währung für Cyberkriminelle gemacht.

Üblicherweise wird sie bei Erpressungs- und Ransomware-Angriffen eingesetzt. Hacker haben nun aber begonnen, Kryptowährung auch bei Spear Phishing, Identitätsmissbrauch und Business Email Compromise-Angriffen zu nutzen.

Bis vor kurzem konnte Kryptowährung nicht in der realen Welt verwendet werden, um Waren des täglichen Lebens zu bezahlen. Als jedoch einige Unternehmen ankündigten, in Zukunft Zahlungen in Bitcoin zu akzeptieren, erhöhte dies das Interesse an Kryptowährungen und ihr Wert begann zu steigen. Angeheizt durch die Nachrichtenflut rund um Bitcoin stieg der Preis zwischen Oktober 2020 und April 2021 um fast 400 % an. Cyberangriffe folgten gleich darauf, und Angriffe mit Identitätsmissbrauch nahmen im gleichen Zeitraum um 192 % zu.

Wert der Kryptowährung und Volumen der damit verbundenen Impersonations-Angriffe



Hacker nutzen Bitcoin, um sich bei Erpressungs-Angriffen bezahlen zu lassen, wobei sie behaupten, über kompromittierende Videos oder Informationen zu verfügen, die veröffentlicht werden, wenn das Opfer nicht für deren Geheimhaltung bezahlt. Dieser Trick wird zwar schon seit einiger Zeit angewandt, mit dem Anstieg des Bitcoin-Preises haben Cyberkriminelle aber noch ausgeklügeltere Pläne entwickelt, um aus der Bitcoin-Mania Profit zu schlagen.

In den letzten Monaten konnten wir einige Phishing-Angriffe mit Identitätsmissbrauch und Business-Email-Compromise-Angriffe in Zusammenhang mit Kryptowährung beobachten, die direkt auf den Anstieg des Bitcoin-Preises folgten. Hacker gaben vor, Cyberwallets und andere Kryptowährungs-Apps zu sein, um mit gefälschten Sicherheitswarnungen Zugangsdaten zu stehlen. In der Vergangenheit gaben sich Angreifer als Finanzinstitut aus, um an Ihre Bankdaten zu gelangen. Heute nutzen sie dieselbe Taktik, um wertvolle Bitcoins zu stehlen.

To: [redacted]
From: Trezor <trezor-update-id25440580640197330@peugeot.com.br>
Reply to:
Date: Mar 11, 2021 7:28 PM

Subject: Your Trezor assets might be vulnerable

We regret to inform you that we have experience a security breach affecting approximately 94,000 of our customers, and that the wallet associated with your e-mail address is within those affected by the breach.

Namely, on Wednesday, March 10th, our forensics team have found a several of the admin servers to be infected with malware.

At this moment, it's technically impossible to conclusively assess the severity, and the scope of the data breach. Due to these circumstances, we must assume that your cryptocurrency assets are at the risk of being stolen.

If you're receiving this e-mail, it's because you've been affected by the breach. To protect your assets, please update your 12, 18 or 24-Word Phrase and follow the instructions to set up a new PIN for your wallet.

Sincerely, Support Team

Update

To: [redacted]
From: [redacted]
Reply to:
Date: May 29, 2021 12:50 PM

Subject: Subject: I invested 1 bitcoin and after 5 minutes I received 2 bitcoins from Elon Musk

Name: [redacted]
Phone: [redacted]
Email: [redacted]
Message: You have received 10 BTC, urgently pick it up today >>>>>>>>>>>>>>> http://www.tesla.com.donaldtrumpcoin.store/bitcoin?8743<<<<<<<<<<<<<<<

Cyberkriminelle verwenden Bitcoin auch als Teil ihrer Business-Email-Compromise-Angriffe, bei denen sie sich als Mitarbeiter eines Unternehmens ausgeben. Sie gehen mit diesen E-Mails gezielt vor und personalisieren sie, um ihre Opfer dazu zu bringen, Bitcoins zu kaufen, an vermeintliche Wohltätigkeitsorganisationen zu spenden oder sogar gefälschte Lieferantenrechnungen mit Kryptowährung zu bezahlen.

To: [redacted]
From: [redacted] <smsinfo@verizonsmswireles.com>
Reply to:
Date: Jan 15, 2021 1:40 PM

Subject: Gift Reward

Hi [redacted] a quick message before it skips my mind again. I have been updated and concluded that we can use bitcoin to pay compensation and bonuses as rewards for some staffs because the Pandemic has changed many things as I have switched to using bitcoin too.

I need you to help purchase some bitcoin to kickstart the process from any Bitcoin ATM which can be found nowadays in many stores.

Kindly try to locate any BTC ATM closest to you and let me know how soon you can get it done.

[redacted]
COO

Sent from my iPhone

To: [redacted]
From: [redacted] <xonlyfamily@gmail.com>
Reply to:
Date: April 07, 2021 9:00 AM

Subject: RESPONSE NEEDED

[EXTERNAL]

Hello [redacted]

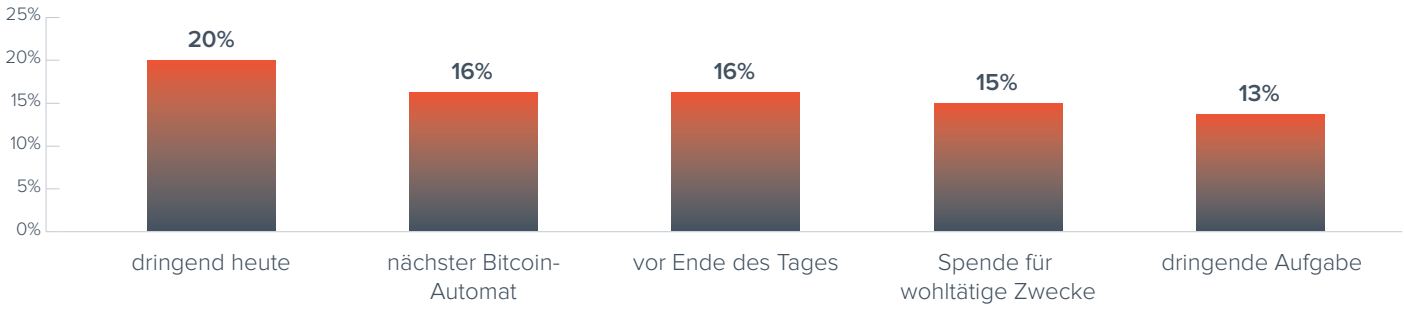
Are you available at the moment? If you are, I have a task for you to carry out urgently today, I need you to head to the nearest Bitcoin Machine to make a charity donation on my behalf before the day runs out.
Email me once you get this.

Regards,
[redacted]
Executive Vice President

Sent from my iPhone

Wir nutzten die KI-Funktionen zur natürlichen Sprachverarbeitung von Barracuda auch, um die Sprache zu analysieren, die in BEC-Angriffen im Zusammenhang mit Kryptowährungen verwendet wird, und die Schlüsselsätze und Handlungsaufforderungen zu untersuchen, mit denen die Hacker ihre Opfer ködern. Ähnlich wie bei typischen BEC-Angriffen erzeugen die Cyberkriminellen ein Gefühl der Dringlichkeit, indem sie Formulierungen wie „dringend heute“ oder „vor Ende des Tages“ verwenden. In der Regel rufen sie ihr Opfer dazu auf, zum „nächsten Bitcoin-Automaten“ zu gehen. Sie zielen auch auf die Gefühle ihrer Opfer ab, indem sie sie zu einer Zahlung als „Spende für wohltätige Zwecke“ auffordern und in dem Glauben lassen, etwas Gutes zu tun.

Schlüsselsätze und Handlungsaufforderungen bei BEC-Angriffen



Best Practices zum Schutz vor Spear-Phishing-Angriffen

Unternehmen sind heute zunehmend Bedrohungen durch gezielte Phishing-Angriffe ausgesetzt. Ein wirksamer Schutz Ihres Unternehmens und Ihrer Benutzer erfordert sowohl Investitionen in Technologie zur Verhinderung von Angriffen als auch in Mitarbeiterschulungen zum Aufbau einer starken Abwehrlinie.

Technology

- **Nutzen Sie die Vorteile künstlicher Intelligenz.** Betrüger passen ihre Taktiken laufend an, damit ihre E-Mails Gateways und Spam-Filter umgehen. Daher sollte unbedingt eine Lösung eingesetzt werden, die Spear-Phishing-Angriffe einschließlich Business Email Compromise, Identitätsmissbrauch und Erpressung zuverlässig erkennt und abwehrt. Insbesondere empfiehlt sich der Einsatz speziell entwickelter Technologien, die über die Suche nach schädlichen Links oder Anhängen hinausgehen. Mithilfe von maschinellem Lernen zur Analyse normaler Kommunikationsmuster innerhalb Ihres Unternehmens können Anomalien erkannt werden, die möglicherweise auf einen Angriff hindeuten.

- **Implementieren Sie effektive Maßnahmen zum Schutz vor Account Takeover.** Häufig gehen Spear-Phishing-Angriffe von kompromittierten Konten aus. Sie müssen also unbedingt verhindern, dass Betrüger Ihr Unternehmen als Ausgangsbasis für diese Angriffe missbrauchen. Abhilfe schafft hier eine Lösung, die künstliche Intelligenz zur Erkennung und Echtzeit-Behebung von Kontoübernahmen einsetzt, indem Benutzer gewarnt und schädliche E-Mails entfernt werden, die von kompromittierten Konten ausgehen.

- **Implementieren Sie DMARC-Authentifizierung und -Reporting.** Domain-Spoofing zählt zu den häufigsten Techniken, die für Angriffe mit Identitätsmissbrauch verwendet werden. Mithilfe von DMARC-Authentifizierungs- und -Durchsetzungsmaßnahmen lassen sich Domain-Spoofing und Brand-Hijacking verhindern. DMARC-Reporting und -Analyse unterstützen Unternehmen beim Einrichten entsprechender Richtlinien für die Durchsetzung.

Mitarbeiter

- **Schulen Sie Mitarbeiter im Erkennen und Melden von Angriffen.** Klären Sie die Benutzer im Rahmen von Schulungen zur Stärkung des Sicherheitsbewusstseins über Spear-Phishing-Angriffe auf. Auf diese Weise lässt sich gewährleisten, dass die Mitarbeiter diese Angriffe erkennen, ihren betrügerischen Charakter verstehen und wissen, wie sie die Angriffe melden können. Verwenden Sie Phishing-Simulationen für E-Mails, Voicemail-Nachrichten und SMS, um Benutzer darin zu schulen, Cyberangriffe zu erkennen, die Wirksamkeit Ihrer Schulungen zu testen und die Benutzer zu identifizieren, die am anfälligsten für Angriffe sind.

- **Überprüfen Sie interne Richtlinien.** Durch Richtlinien und Verfahren, die vorsehen, dass alle E-Mail-Anfragen in Zusammenhang mit Überweisungen, dem Kauf von Geschenkkarten usw. vorschriftsmäßig bestätigt werden, unterstützen Sie Ihre Mitarbeiter dabei, kostspielige Fehler zu vermeiden.

- **Optimieren Sie Ihren Schutz vor Datenverlusten.** Mit der richtigen Kombination aus Technologien und Unternehmensrichtlinien wird eine Blockierung ausgehender E-Mails gewährleistet, die vertrauliche, personenbezogene und andere sensible Daten enthalten.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Überzeugung, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen und anpassungsfähigen Lösungen, die mit den Unternehmen unserer Kunden wachsen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Somit können sie sich darauf konzentrieren, ihr Geschäft auf die nächste Stufe zu bringen.

Weitere Informationen finden Sie unter barracuda.com.

Barracuda
Your journey, secured.