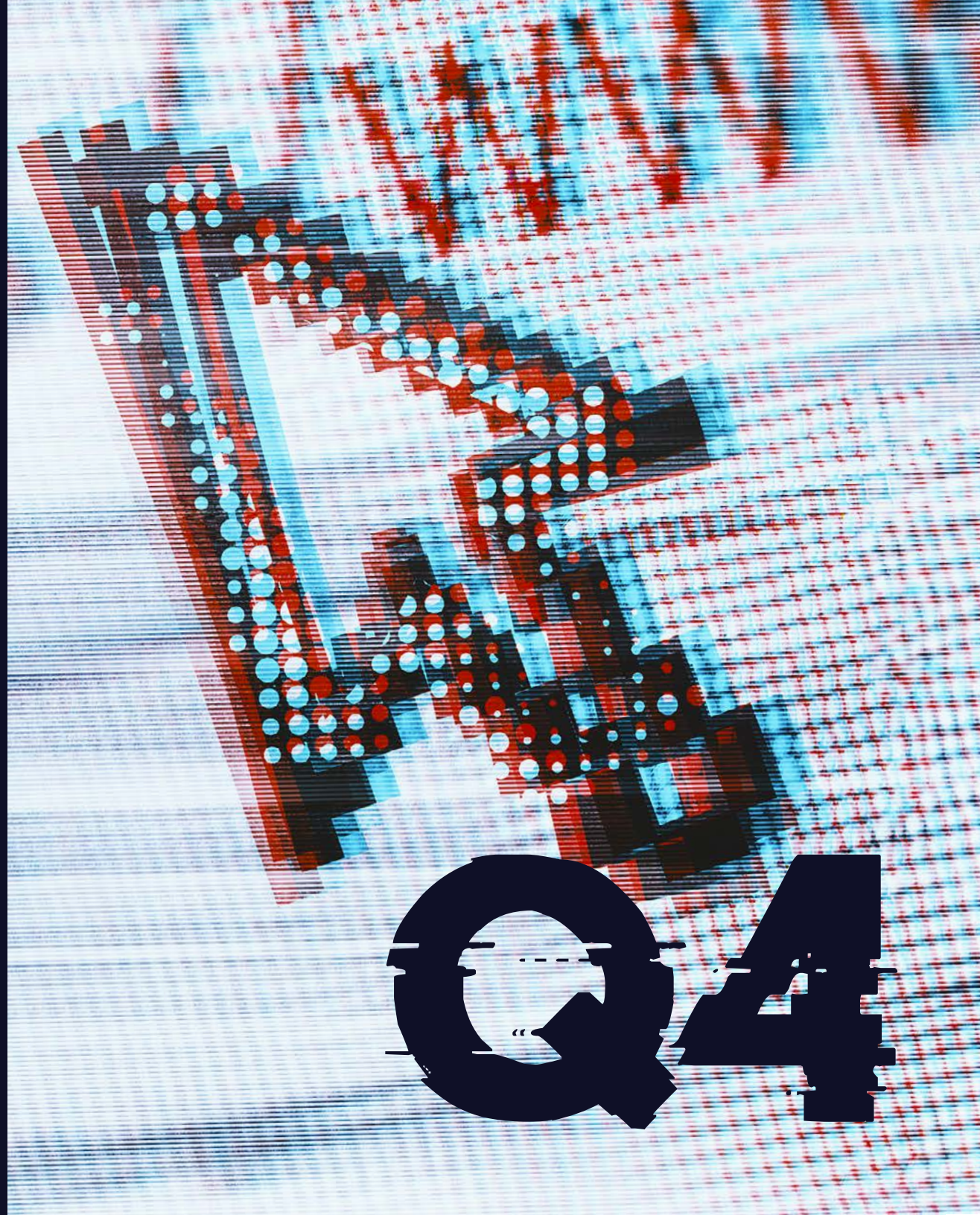
mimecast

Global Threat Intelligence Report

Oktober-Dezember 2023



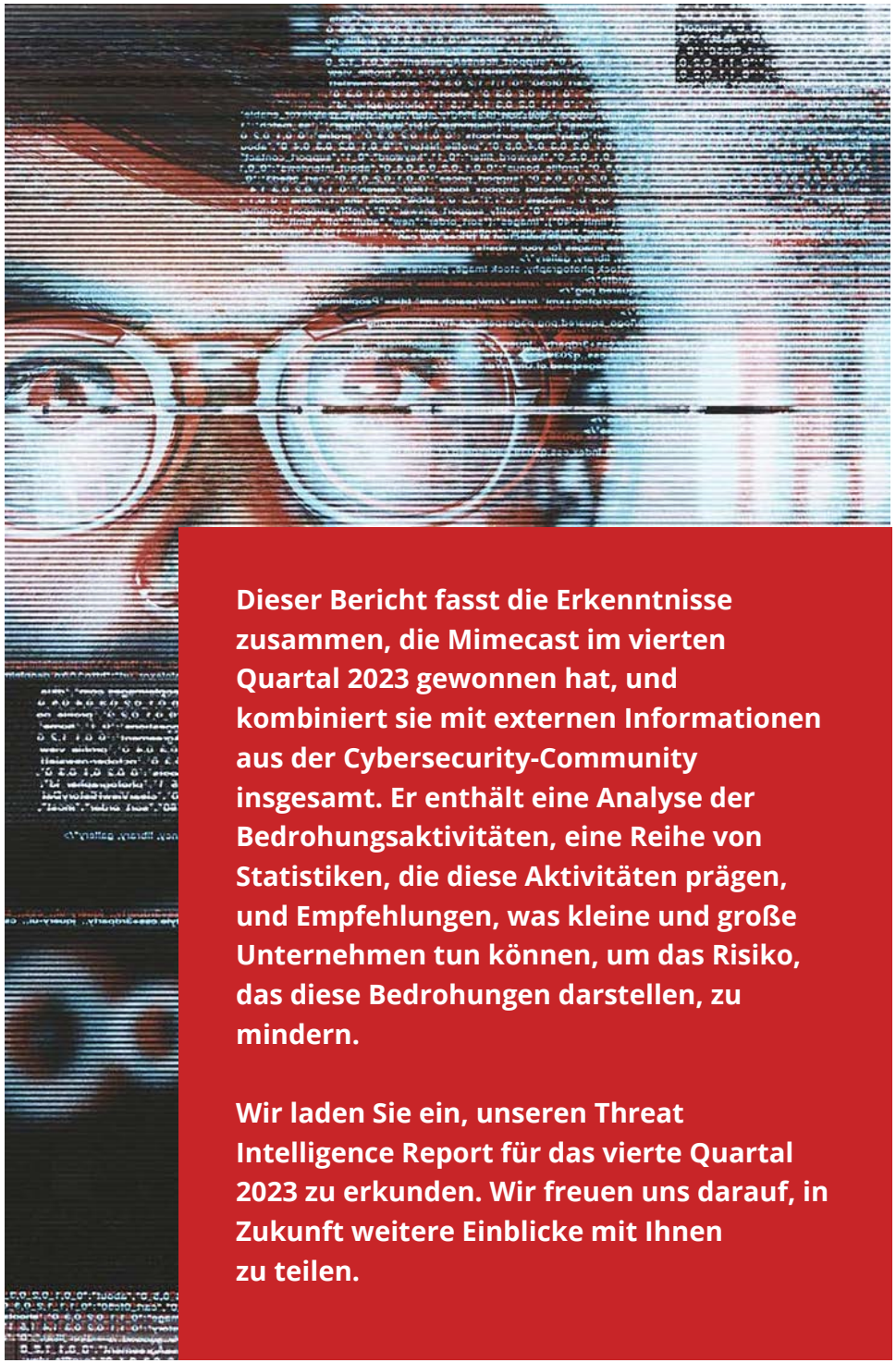
EINLEITUNG

Allzu oft erhalten Unternehmen Informationen über Bedrohungen in Form von Einzelanalysen bestimmterVorfälle, was den Sicherheitsteams einen eingeschränkten Blick auf die Bedrohungslandschaft verschafft. Mit diesem Global Threat Intelligence Report möchte Mimecast die Vorfälle der letzten drei Monate in einen Kontext stellen und Unternehmen die Werkzeuge an die Hand geben, die sie benötigen, um zu verstehen, wohin Angreifer steuern und wo die Verteidigung verbessert werden kann.

Mimecast generiert Bedrohungsdaten durch die Analyse von 1,7 Milliarden E-Mails pro Tag im Auftrag von mehr als 42.000 Kunden. Da E-Mail der Hauptangriffsvektor für Cyber-Bedrohungen ist, erkennt Mimecast viele neue Bedrohungen, bevor sie allgemein bekannt werden.

+ 1.7 Milliarden E-Mails pro Tag

42 000 Kunden



Dieser Bericht fasst die Erkenntnisse zusammen, die Mimecast im vierten Quartal 2023 gewonnen hat, und kombiniert sie mit externen Informationen aus der Cybersecurity-Community insgesamt. Er enthält eine Analyse der Bedrohungsaktivitäten, eine Reihe von Statistiken, die diese Aktivitäten prägen, und Empfehlungen, was kleine und große Unternehmen tun können, um das Risiko, das diese Bedrohungen darstellen, zu mindern.

Wir laden Sie ein, unseren Threat Intelligence Report für das vierte Quartal 2023 zu erkunden. Wir freuen uns darauf, in Zukunft weitere Einblicke mit Ihnen zu teilen.

KURZFASSUNG

Im vierten Quartal 2023 änderten die Angreifer ihre Methoden und setzten verstärkt auf Links für die erste Nutzlast, anstatt Malware als E-Mail-Anhang zu versenden. Darüber hinaus verwenden Bedrohungsakteure zunehmend QR-Codes, um Abwehrmaßnahmen zu umgehen, die bösartige Links blockieren und ihre Angriffe verschleiern sollen.

Nach den Angriffen auf große Kasinos zu Beginn des Jahres konzentrierten sich die Angreifer auch im vierten Quartal 2023 auf Unternehmen aus der Reise-, Hotel- und Gaststättenbranche. Dadurch wurde dieser Sektor in diesem Quartal zur am zweithäufigsten angegriffenen Branche, nur übertroffen von den Angriffen auf den Bankensektor. Während die Angriffe auf Personal- und Rekrutierungsdienste etwas nachgelassen haben, bleibt dieser Sektor weiterhin die am dritthäufigsten angegriffene Branche.

Mimecast Threat Intelligence Team

Das Threat Intelligence Team von Mimecast besteht aus einer weltweit verteilten Gruppe von Ingenieuren, Wissenschaftlern, Analysten und Bedrohungsforschern, die das Mimecast Security Operations Center (MSOC) unterstützen. Bedrohungen werden kontinuierlich überwacht über mehr als 1,7 Milliarden E-Mails pro Tag. Die Cybersicherheitsexperten von Mimecast rekonstruieren Angriffswerkzeuge, untersuchen Angriffe und testen die Effektivität von Kompromissindikatoren, um schnell Bedrohungsinformationen zu entwickeln und Schutzmaßnahmen über ihre Lösungen hinweg zu implementieren.

WICHTIGSTE ERKENNTNISSE

Sektoren

Im vierten Quartal 2023 waren die am stärksten von Angriffen betroffenen Sektoren Finanzinstitute, Reisen, Gastgewerbe und Catering sowie Personal- und Rekrutierungsdienste. Diese Angriffe wurden durch Ransomware, Datendiebstahl und die Kompromittierung geschäftlicher E-Mails (BEC) angetrieben. Darüber hinaus waren durchschnittlich kleine und mittlere Unternehmen über alle Branchen hinweg mit mehr als doppelt so vielen Bedrohungen konfrontiert wie große Unternehmen.

Links vs. Anhänge

Erstmals im vierten Quartal 2023 war es wahrscheinlicher, dass ein durchschnittlicher Benutzer auf einen bösartigen Link stieß als auf einen bösartigen Anhang. In der Vergangenheit nutzten Angreifer häufiger bösartige Anhänge, um schädliche Daten zu verbreiten.

Geopolitik

Die geopolitischen Spannungen haben zugenommen, was zu einer Zunahme von Cyberangriffen geführt hat. Über 100 Hackergruppen behaupten, allein am Konflikt zwischen Israel und Gaza beteiligt gewesen zu sein. Nationen nutzen Cyberoperationen, um Informationen über rivalisierende Regierungen zu sammeln sowie kritische Infrastrukturen und Informationssysteme anzugreifen.

Generative KI

Angreifer setzen generative KI und Machine-Learning-Modelle ein, um noch überzeugendere Phishing-Köder zu erstellen und Angriffe in verschiedene Sprachen zu übersetzen. Technische Bedrohungsindikatoren wie Domain-Reputation, Browser-Isolation und Malware-Analyse werden zunehmend erforderlich sein, um Angriffe abzuwehren.

QR-Codes

Die Verwendung von QR-Codes zur Verschleierung von Links hat weiter zugenommen. Sie erfüllen denselben Zweck wie URL-Verkürzungen, bieten aber einen zusätzlichen Vorteil für Angreifer, da Opfer sich bereits daran gewöhnt haben, QR-Codes einfach zu scannen, ohne deren Inhalte zu überprüfen.

ERPRESSUNGSKAMPAGNEN NEHMEN ZU, CYBERATTACKEN FOLGEN DER GEOPOLITIK

Ransomware und “Breach-for-Ransom”-Kampagnen nahmen im vierten Quartal 2023 weiter zu. Eine der größeren Gruppen, ALPHV Blackcat, kompromittierte mehr als 1.000 Opfer mit Ransomware und Datenerpressung und erzielte bis zum Ende des Quartals über 300 Millionen Dollar an Lösegeldzahlungen.

Die Angriffsstrategien haben sich von Krypto-Ransomware (bei der die Angreifer Daten verschlüsseln und den Entschlüsselungsschlüssel besitzen) über “Breach-for-Ransom”-Kampagnen (bei denen die Angreifer sensible Daten stehlen und mit der Veröffentlichung drohen, wenn kein Lösegeld gezahlt wird) bis hin zu Doppel- und Dreifach-Erpressungsstrategien entwickelt. Dabei kombinieren die Angreifer ihre Taktiken, um direktere Konsequenzen zu erzielen.

Ransomware und Gruppen, die Informationen stehlen, haben begonnen, raffiniertere Techniken anzuwenden, wie z. B. den Diebstahl von Token und Kontokennungen aus Google Chrome. Diese erfolgreichen Taktiken haben zu einer Konsolidierung der Anzahl der Ransomware-Tools geführt - mit 43 Malware-Familien, die im Jahr 2023 für Erpressungen verwendet wurden, im Vergleich zu 95 im Jahr 2022. Dies deutet darauf hin, dass Cyberkriminelle und ihre Partner sich auf eine bekannte Reihe beliebter Plattformen konzentrieren. Vier Gruppen - LockBit, Cl0p, ALPHV/ BlackCat und Play - dominierten die Ransomware-Landschaft in diesem Quartal und waren für 88 % aller Ransomware-Aktivitäten verantwortlich.

Während Ransomware und Datenschutzverletzungen im Jahr 2023 zunahmen, wehren sich die Unternehmen gegen Erpressungsangriffe. Die Rate der Lösegeldzahlungen ist stark gesunken und erreichte im 2. Quartal 2023 einen Tiefstand von 34 %, gegenüber 85 % auf Anfang von 2019. (Die Rate der Unternehmen, die Lösegeldforderungen zugestimmt haben, ist im 3. Quartal 2023 leicht gestiegen). Drei Veränderungen in den Sicherheitsprozessen der Unternehmen und die wirtschaftlichen Auswirkungen von Ransomware könnten diesen Wandel verursacht haben: Unternehmen haben weniger Vertrauen in die Fähigkeit der Cyberkriminellen, Daten wiederherzustellen; Unternehmen hatten Zeit, ihre Sicherheitsvorkehrungen langsam zu verbessern; und die Zahlung von Lösegeld an Bedrohungsakteure aus bestimmten Nationalstaaten verstößt nun gegen Bundesgesetze.

Ransomware Gruppen versuchen, diesen Trend umzukehren. Seit dem 1. Oktober hat die LockBit-Ransomware-Gruppe neue Regeln für Verhandlungen mit ihren Opfern eingeführt und ihre “Partner” gewarnt, dass großzügige Rabatte bei Lösegeldzahlungen nicht mehr akzeptabel sind.

Die geopolitische Lage hat sich seit dem Terroranschlag der militanten Gruppe Hamas auf Israel am 7. Oktober verschlechtert. Ähnlich wie bei anderen globalen Konflikten, wie dem Einmarsch Russlands in die Ukraine, haben auch die Cyberangriffe erheblich zugenommen. Nationale Cyberoperationen, Gruppen, die mit beiden Seiten verbunden sind, und Hacktivisten verstärken ihre Angriffe auf Websites, kritische Infrastrukturen und Computersysteme. Im vierten Quartal 2023 führten mindestens 90 pro-palästinensische Bedrohungsakteure und 23 pro-israelische Bedrohungsakteure Angriffe durch.

Es gibt bereits einige Anzeichen dafür, dass Machine-Learning-Modelle und generative KI auch die Bedrohungslandschaft verändern. Laut dem Threat Intelligence Team von Mimecast werden Täuschungsversuche immer überzeugender und lassen sich leichter auf bestimmte Regionen zuschneiden, da die Bedrohungsakteure generative KI einsetzen. Darüber hinaus haben Forscher bösartigen Code auf GitHub hochgeladen, der mit Komponenten für maschinelles Lernen wie PyTorch verknüpft war, ähnlich wie Angriffe auf andere Open-Source-Komponenten in der Lieferkette.

Q4 2023 IN GRAFIKEN

Die Sektoren, die im vierten Quartal 2023 die meisten Angriffe erlebten ,waren Finanzinstitute, Reise-, Gastgewerbe- und Catering-Unternehmen sowie Personalabteilungen. Diese Angriffe wurden durch Ransomware, Datendiebstahl und BEC verursacht.

Darüber hinaus waren die durchschnittlichen Benutzer in kleinen und mittleren Unternehmen über alle Branchen hinweg mit mehr Bedrohungen konfrontiert - im Durchschnitt etwa doppelt so viele wie Benutzer in großen Unternehmen.

01. KMUs sind doppelt so vielen Bedrohungen ausgesetzt wie Großunternehmen

02. Die Anzahl bösartiger Links nimmt zu

03. Phishing dominiert als der häufigste Angriffsvektor

04. Anstieg der Angriffe in allen Bereichen, Angriffe auf das Personalwesen

05. Haupt-Sicherheitslücken im Laufe der Zeit

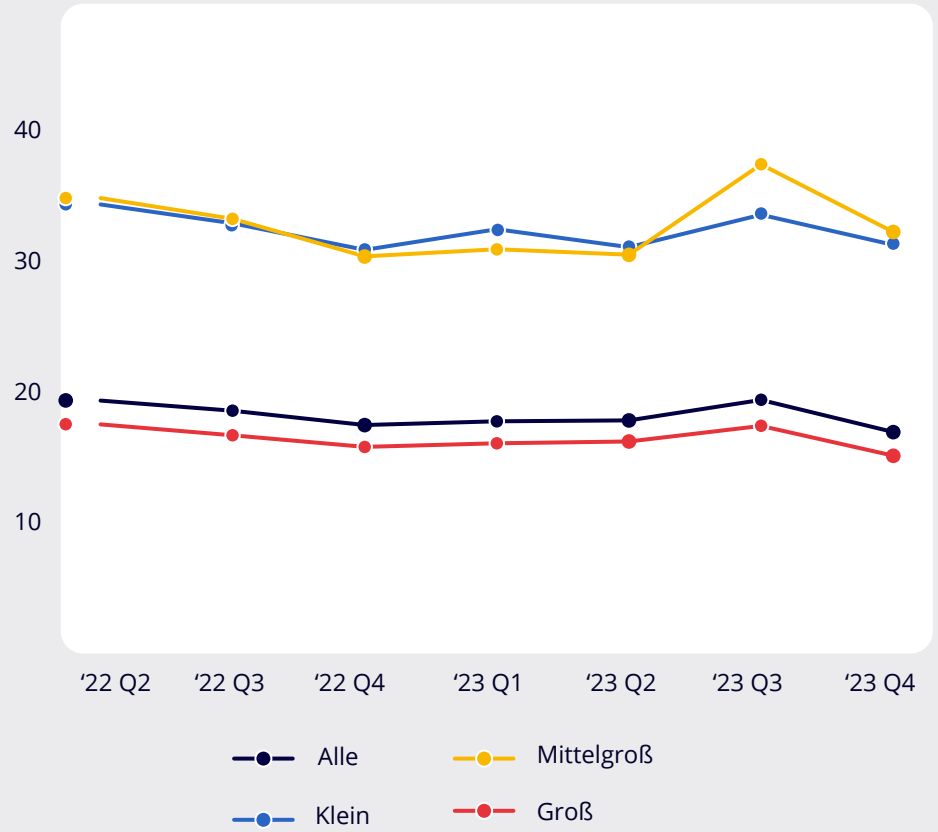
Begegnungsraten: Kleine und mittlere Unternehmen sind doppelt so oft bedroht

Der deutliche Anstieg an Bedrohungen, der im dritten Quartal zu beobachten war, scheint nachgelassen zu haben, aber mittelgroße Unternehmen haben immer noch etwas mehr Bedrohungen pro Benutzer (TPU) gesehen als kleinere Firmen im vierten Quartal. Durchschnittliche Benutzer in kleinen und mittelständischen Unternehmen (KMU) waren jeweils mehr als doppelt so vielen Bedrohungen ausgesetzt – 31 und 32 TPU – im Vergleich zu Benutzern in großen Unternehmen, die etwa 15 TPU im vierten Quartal erlebten.

Das größere Risiko für kleine und mittlere Unternehmen (KMUs) ist auf den höheren Anteil von Mitarbeitern in kritischen Positionen zurückzuführen; diese Benutzer ins Visier zu nehmen, führt zu einer erhöhten Bedrohung pro Benutzer. Da KMUs für viele ihrer Aktivitäten auf Cloud-Dienste angewiesen sind, die Zugangsdaten erfordern, konzentrieren sich Angreifer verstärkt auf den Diebstahl von Zugangsdaten, was ein häufiges Ziel von Phishing-Angriffen ist.

Im vierten Quartal eines jeden Jahres ist die Anzahl der Bedrohungen in der Regel geringer als im vorangegangenen Quartal, was zu einem gleichmäßigen Rückgang der Bedrohungen pro Benutzer (TPU) bei allen Unternehmen führt.

Abbildung 1. Bedrohungen pro Benutzer nach Unternehmensgröße



2. Begegnungsraten: Bösartige Links nehmen zu

Spam und Impersonation gingen im vierten Quartal 2023 beide zurück, dominierten jedoch weiterhin die bösartigen Aktivitäten, die auf die E-Mail-Postfächer der Benutzer abzielten. Die Mimecast-Abwehr blockierte durchschnittlich 9,5 bzw. 6,3 E-Mails pro Benutzer, die entweder als Spam oder Impersonation eingestuft wurden. Die Kategorie “unbekannte Malware”, die Mimecast aufgrund der Erkennung von Exploit-Code in Anhängen blockiert, ist zu klein, um in der ersten Grafik sichtbar zu sein.

Wenn man die beiden größten Bedrohungskategorien - Spam und Impersonation - außer Acht lässt, wird ein weiterer Trend deutlich. Im vierten Quartal war es zum ersten Mal wahrscheinlicher, dass der durchschnittliche Nutzer auf einen bösartigen Link stieß als auf einen bösartigen Anhang. Da Benutzer die überwältigende Menge an E-Mail-Nachrichten ignorieren, die entweder als Spam oder Impersonation (Phishing) blockiert werden, gehen Angreifer vermehrt dazu über, keine schädlichen Dateianhänge mehr zu versenden, sondern Links zu bösartigen Websites zu schicken, die dann die Nutzlast enthalten.

Abbildung 2a. Bedrohungen pro Benutzer nach Art der Bedrohung

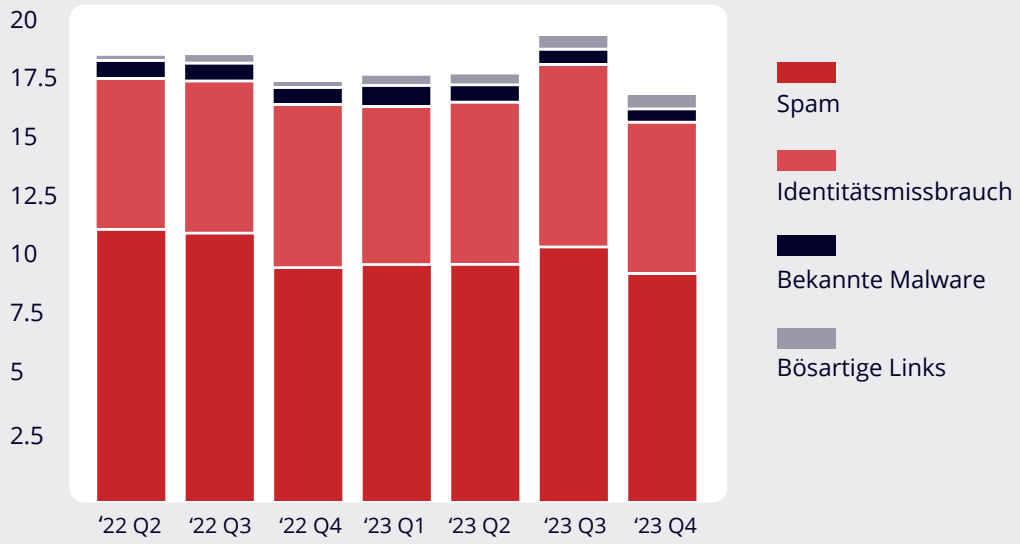
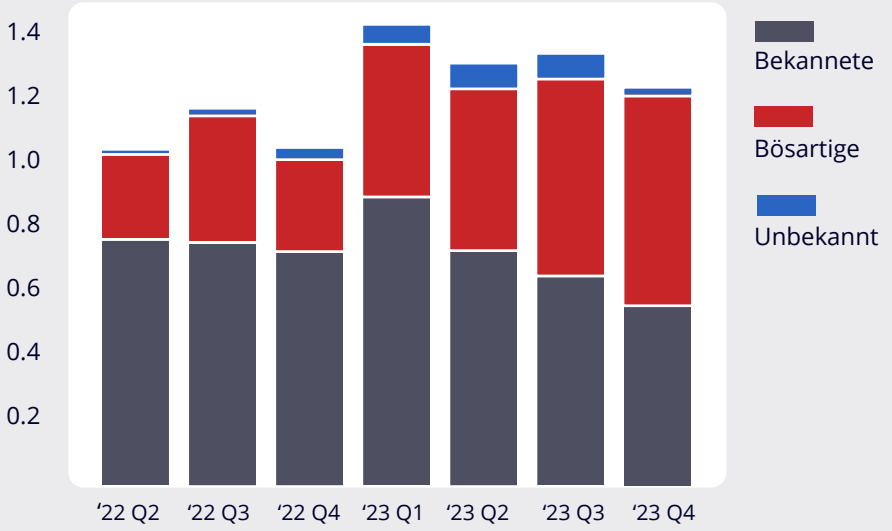


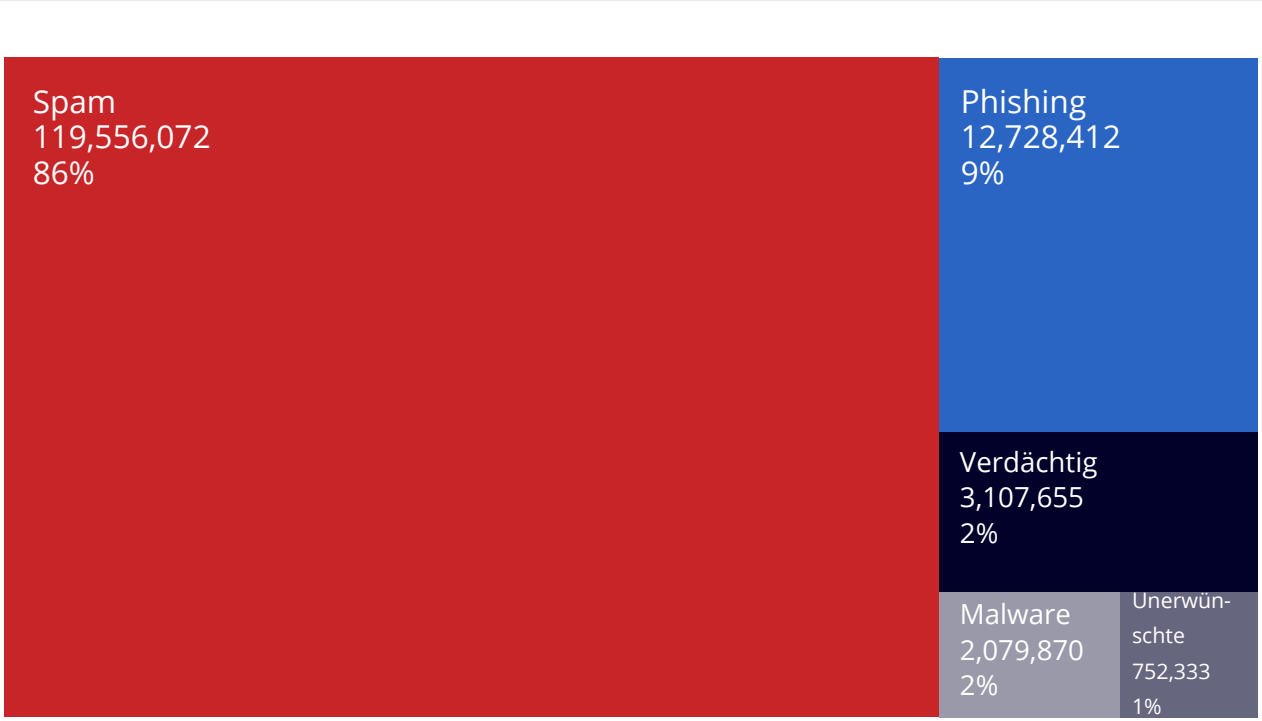
Abbildung 2b. Bedrohungen pro Benutzer für Malware & bösartige Links



Bedrohungsarten: Phishing dominiert aktive Bedrohungen, wobei Links der häufigste Vektor sind

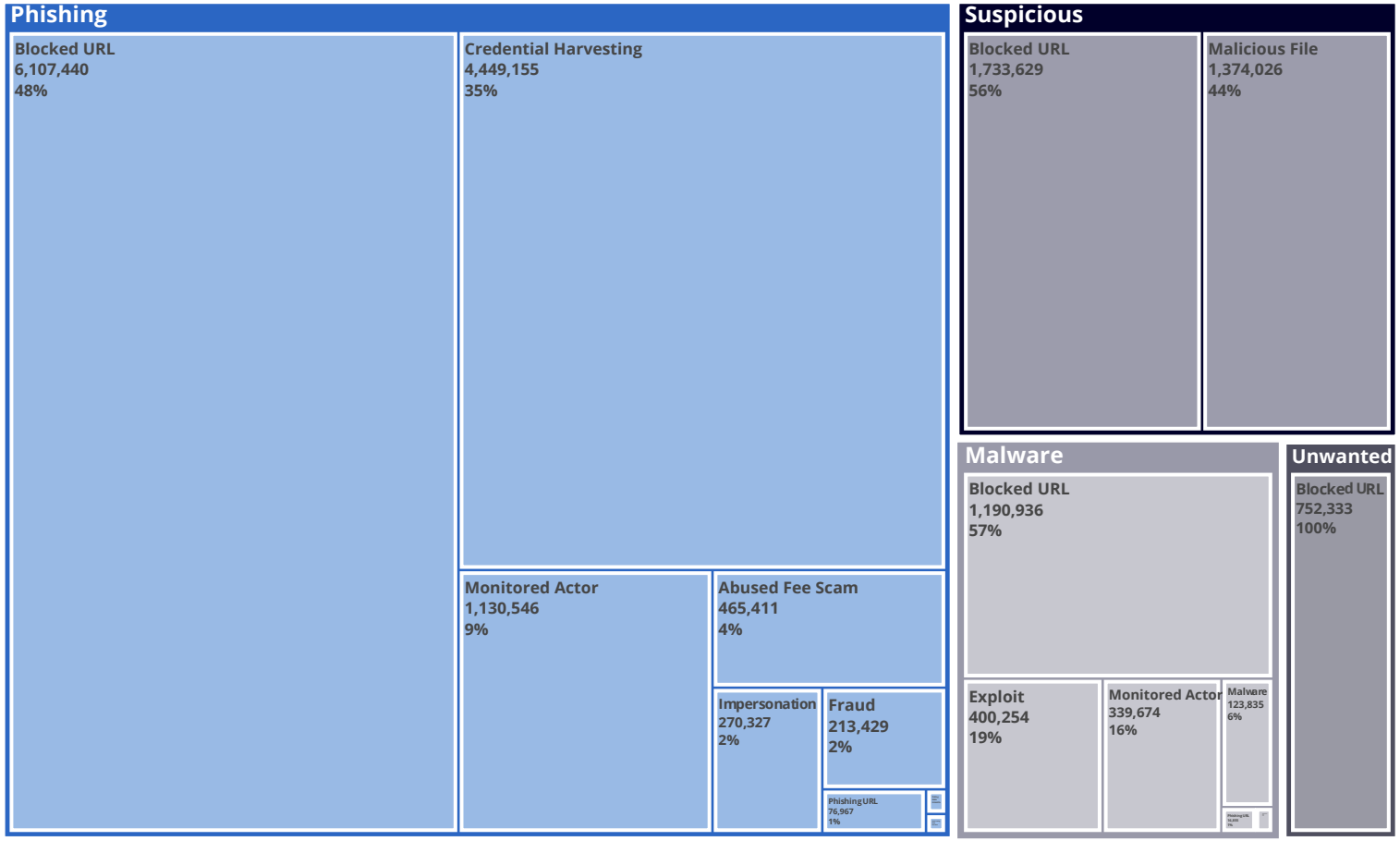
Während Spam weiterhin 86% aller blockierten Nachrichten ausmacht und damit den größten Anteil an abgelehnten bösartigen und verdächtigen E-Mails darstellt (siehe Abbildung 3(a)), zeigen die wichtigsten Bedrohungen neben Spam interessante Trends (siehe Abbildung 3(b)).

Abbildung 3a. Relatives Volumen aller Bedrohungen



Bösartige URLs machen weiterhin den größten Anteil aller wichtigen Erkennungstypen aus, darunter Phishing, Malware sowie verdächtige und unerwünschte E-Mails. Das Abgreifen von Anmeldedaten ist das zweithäufigste Merkmal von Phishing-Angriffen. Dies unterstreicht die Bedeutung von starken Anmeldedaten und deren Absicherung durch mehrstufige Authentifizierung für den Schutz von Unternehmen, die zunehmend Cloud-Dienste und -Infrastrukturen nutzen.

Abbildung 3b.Malware und bösartige Links

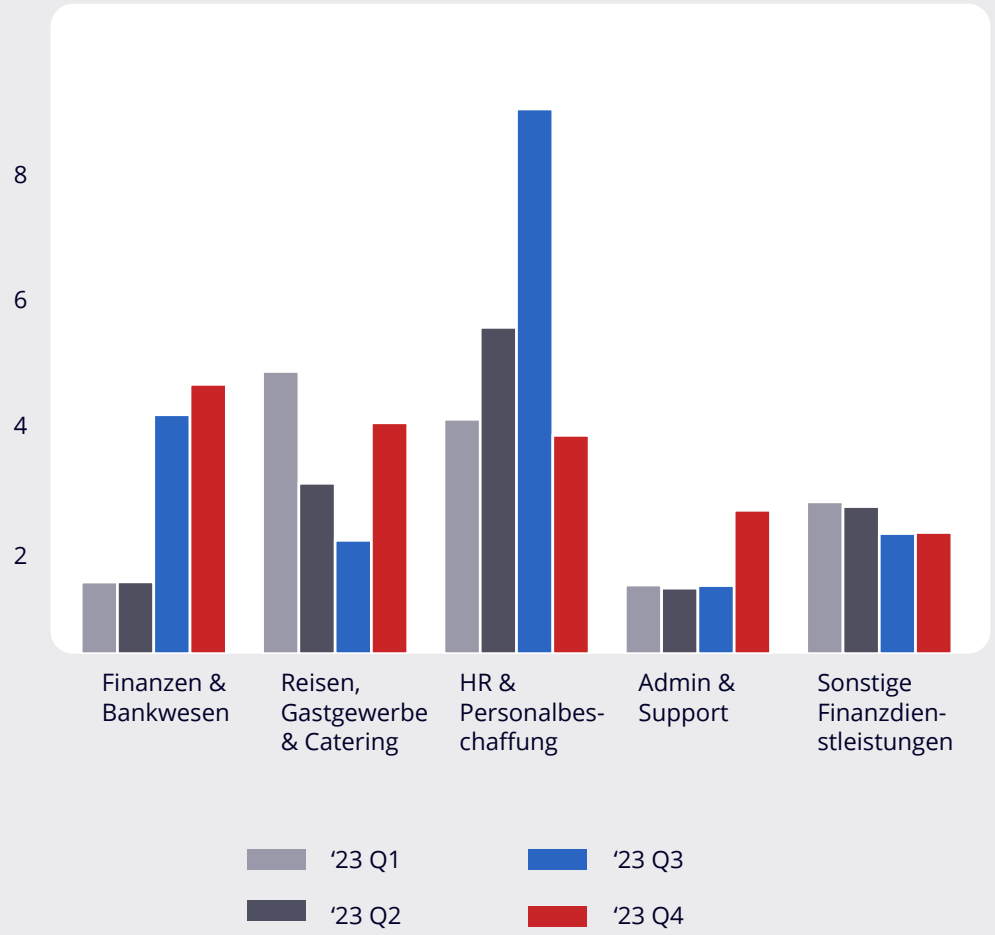


Überblick über die Branche: Angriffe nehmen branchenübergreifend zu, während Angriffe auf das Personalwesen nachlassen

Die durchschnittliche Anzahl der Angriffe (ohne Spam und Impersonation) ist im vierten Quartal 2023 gesunken. Benutzer im ehemals am stärksten angegriffenen Sektor, Personal- und Rekrutierungsdienstleistungen, waren um 60 % weniger Bedrohungen ausgesetzt als im vorherigen Quartal, wodurch dieser Sektor im vierten Quartal 2023 auf den dritten Platz zurückfiel. Gleichzeitig ist der Sektor IT-Software und Software-as-a-Service aus den fünf am meisten angegriffenen Sektoren herausgefallen und auf den letzten Platz, Nummer 20 in Q4 2023, zurückgegangen.

Alle anderen Sektoren verzeichneten jedoch einen Anstieg der wichtigsten Bedrohungen wie bekannte Malware, bösartige Links und unbekannte Malware im Vergleich zum Vorquartal. Nutzer im Bankensektor waren weiterhin mit einer hohen Anzahl von Angriffen konfrontiert, ebenso wie Nutzer im Reise-, Hotel- und Gaststättengewerbe, einschließlich Kasinos. Über alle Branchen hinweg war der durchschnittliche Nutzer im Quartal mit 1,2 Bedrohungen konfrontiert, was etwas weniger ist als der Durchschnitt von 1,3 Bedrohungen pro Nutzer im Q3 2023.

Abbildung 4. Top 5 Bedrohungen pro Benutzer nach Branche für Malware & bösartige Links



Statusbericht der Schwachstellen: Die wichtigsten Schwachstellen im Zeitverlauf

Die Gesamtzahl der Sicherheitslücken ist im Laufe des Quartals zurückgegangen. Dies ist ein typisches Muster für das vierte Quartal, da die Unternehmen schließen und sowohl Angreifer als auch Opfer zum Jahresende eine Pause einlegen.

Die Top-5-Sicherheitslücken zeigten unterschiedliche Nutzungsprofile. Die am häufigsten ausgenutzte Sicherheitslücke für Malware - ein Fehler bei der Remotecodeausführung im Gleichungseditor von Microsoft Office 2007 bis 2016 (CVE-2018-0802) - war das bevorzugte Werkzeug der Angreifer im vierten Quartal 2023. Eine weitere Schwachstelle im Speicher von Microsoft Office (CVE-2017-11882), die minimal genutzt wurde, erreichte ihren Höhepunkt erst in der dritten Novemberwoche, während der beliebtesten Einkaufstage des Jahres.

Nur eine Sicherheitslücke in der Top-5-Liste - und nur zwei in der Top-10-Liste - stammt aus dem Jahr 2023. Dies zeigt, dass Angreifer bevorzugen, Softwarelücken auszunutzen, die sie als am anfälligsten einschätzen, auch wenn die ausgenutzte Schwachstelle älter ist.

Abbildung 5a. Gesamtzahl der blockierten Sicherheitslücken im vierten Quartal 2023

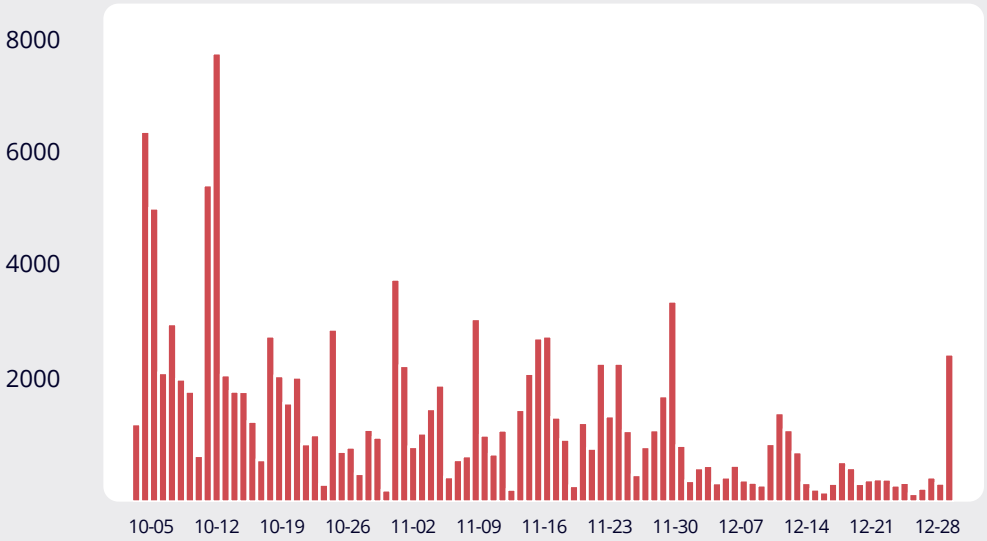
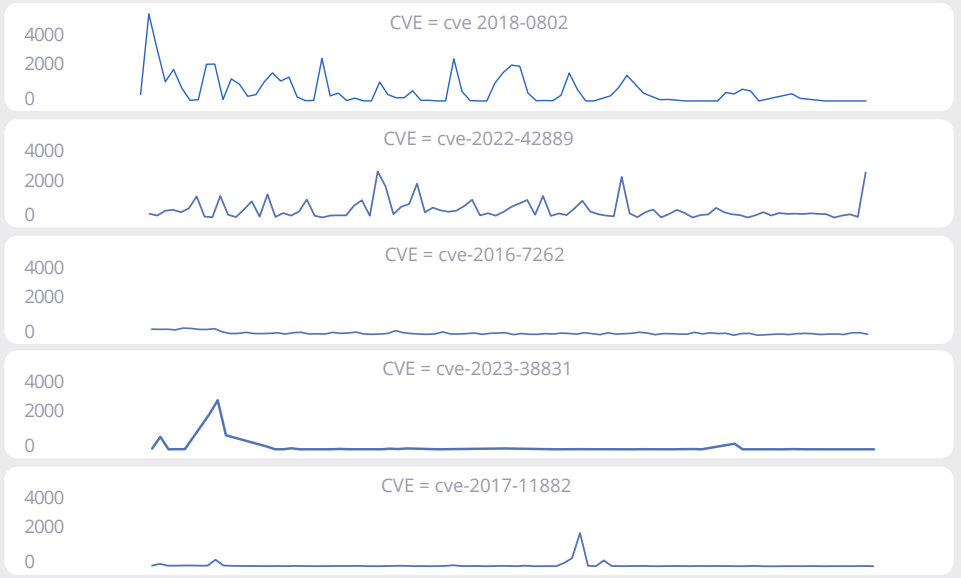


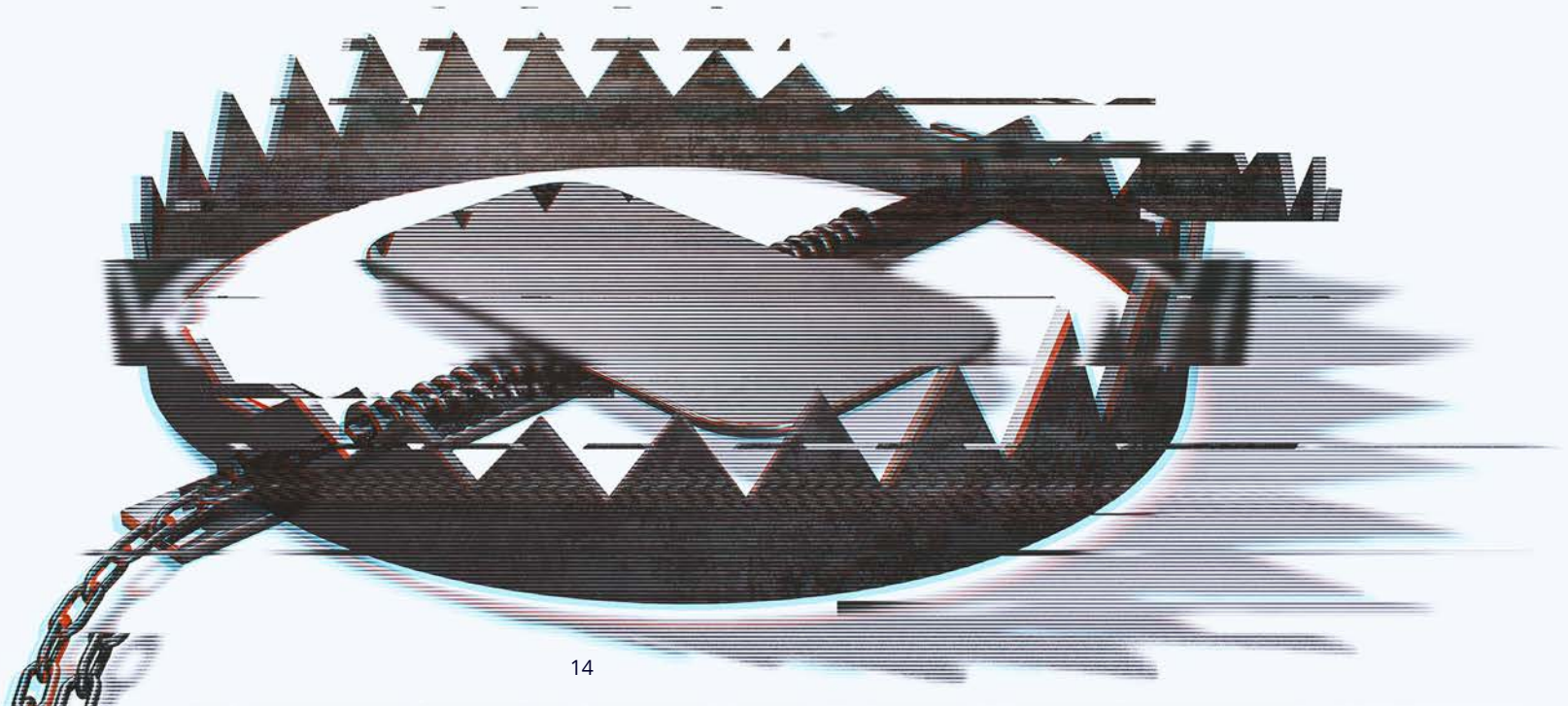
Abbildung 5b. Top 5 Schwachstellenentdeckungen für Q4 2023



MARKENMISSBRAUCH WIRD IMMER ÜBERZEUGENDER

Praktisch jede Art von E-Mail-Angriff nutzt legitime Marken, um das Vertrauen der Benutzer zu gewinnen und sie dazu zu verleiten, Handlungen auszuführen, die ihre Sicherheit gefährden, wie die Preisgabe vertraulicher Daten oder das Anklicken von Links. Im vierten Quartal 2023 nutzte ein Bedrohungsakteur beispielsweise den E-Mail-Marketingdienst von SendGrid, um E-Mail-Kampagnen zu versenden, die vorgaben, von Personalabteilungen zu stammen. Die Empfänger wurden aufgefordert, auf einen Link zu klicken, der angeblich von einem Microsoft SharePoint Online-Server stammte.

Angreifer setzen zunehmend generative KI ein, um täuschend echt wirkende Benachrichtigungen zu erstellen und missbrauchen dabei legitime Dienste, um Abwehrmaßnahmen zu umgehen, die auf Reputation basieren. Dies verschärft das Problem des Markenmissbrauchs erheblich.

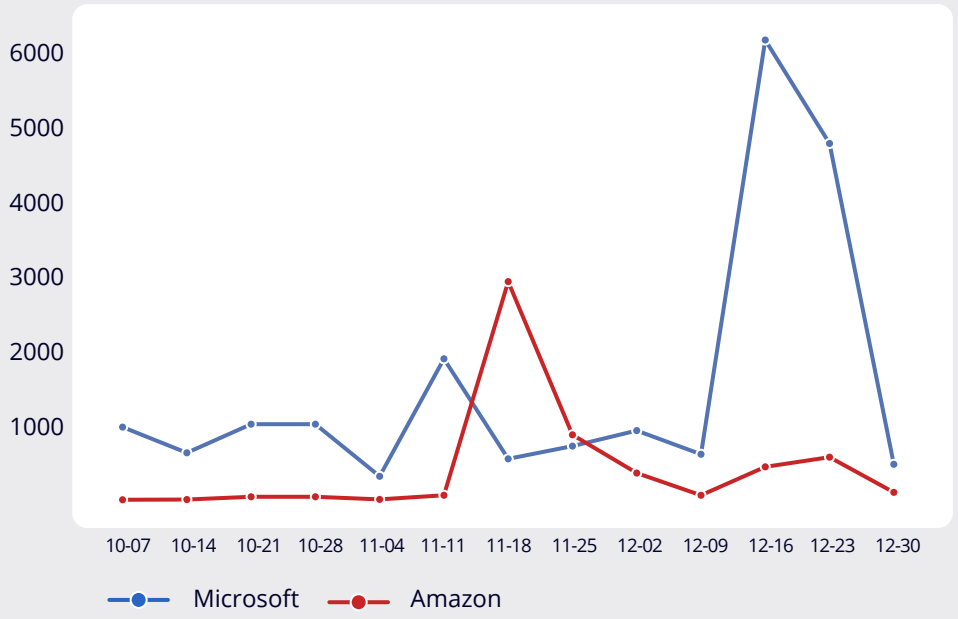


Angreifer verwenden je nach Kontext unterschiedliche Marken

Wie die Daten aus unserem Bericht für Q3 2023 zeigen, ist Microsoft die am häufigsten missbrauchte Marke. Bestimmte Ereignisse können jedoch dazu führen, dass Angreifer andere Marken verwenden, um das Vertrauen der Nutzer zu gewinnen. Zum Beispiel waren während der Coronavirus-Pandemie im Jahr 2020 Amazon, Apple und die Sozialversicherungsverwaltung die drei am häufigsten imitierten Marken.

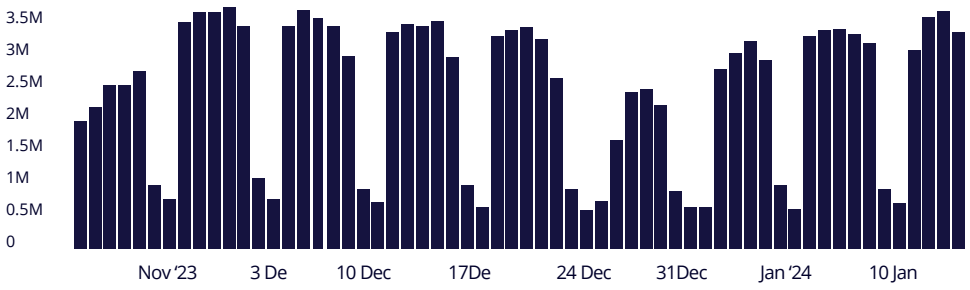
Im vierten Quartal änderten die Angreifer erneut ihre Taktik bezüglich der Markenidentität. Um das Weihnachtsgeschäft auszunutzen, gaben sich die Betrüger verstärkt als Amazon aus, was zu einem Anstieg von Spam- und Phishing-Angriffen unter dieser Marke führte. In den zwei Wochen vor dem Black Friday, der in den Vereinigten Staaten den Beginn der Weihnachtseinkaufssaison markiert, hat Mimecast mehr Bedrohungen unter der Marke Amazon entdeckt als unter der Marke Microsoft.

Abbildung 6. Angreifer konzentrieren sich vor dem Weihnachtsgeschäft auf Amazon



Inzwischen nutzen Angreifer QR-Codes, um die Ziele von Links zu verschleiern, und setzen dabei auf Branding, um Benutzer davon zu überzeugen, dass die QR-Codes von offiziellen Quellen stammen. Diese Methode hat sich von einer Nischenanwendung zum Mainstream entwickelt, wie man an der regelmäßigen Verwendung von mehr als 3,5 Millionen E-Mails pro Tag mit QR-Codes sieht (siehe Abbildung 7). Mimecast hat zwei größere Kampagnen dokumentiert, bei denen QR-Codes verwendet wurden - eine getarnt als Microsoft-Passwortrücksetzung und eine andere als DocuSign.

Abbildung 7. QR-Code-Erkennung über 60 Tage

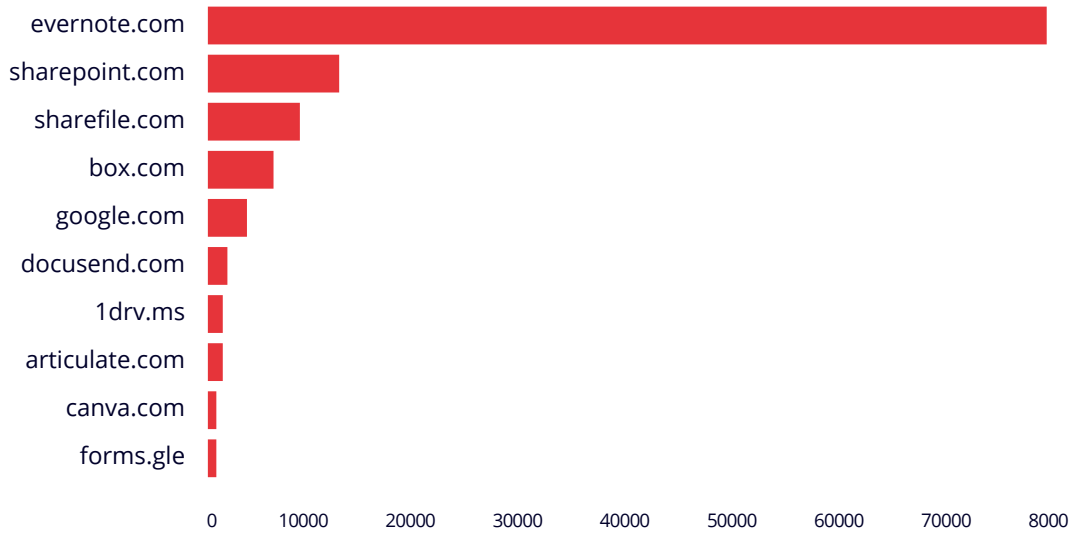


Bei Filesharing-Missbrauch geht es um Marken

Angreifer setzen zunehmend auf Links anstelle von Anhängen für ihre Payloads – sei es für Phishing-Websites zur Diebstahl von Anmeldeinformationen oder für malware, die das Opfer herunterladen kann. Um Sicherheitslösungen zu umgehen und das Vertrauen der Benutzer zu gewinnen, nutzen Angreifer häufig Filesharing-Dienste mit bekannten Marken, um bösartige Inhalte zu verbreiten (siehe Abbildung 8).

Der führende Dienst für Filesharing-Websites in den letzten drei Quartalen war der Notiz- und Austauschdienst Evernote. Microsoft SharePoint liegt deutlich an zweiter Stelle, gefolgt vom ShareFile Managed Storage Service auf dem dritten Platz.

Abbildung 8. Evernote führt die beliebtesten Domains für Phishing-Angriffe an

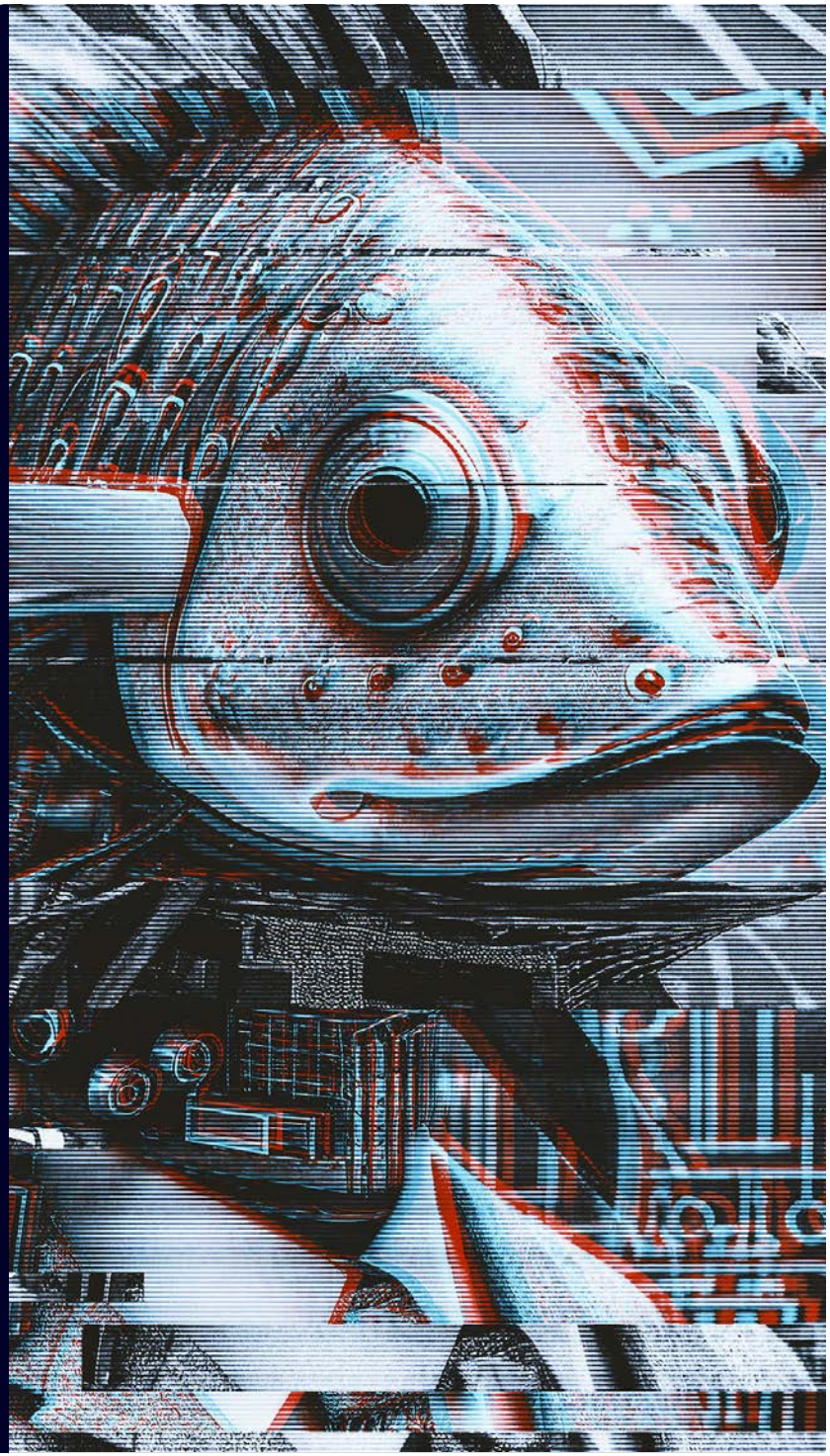


BEDROHUNGS ANALYSE

Angreifer haben ihre Techniken zur Umgehung von Multifaktor-Authentifizierungsmechanismen (MFA) weiterentwickelt. Die Phishing-as-a-Service (PhaaS)-Plattform EvilProxy beispielsweise richtete einen Angriff auf die Finanz- und Versicherungsbranche mit einem Proxy ein, um MFA zu umgehen. Eine andere Gruppe nutzte die DadSec PhaaS-Plattform, um Opfer über einen Proxy zu leiten, der als Man-in-the-Middle fungierte, um MFA-Anfragen abzufangen und die Microsoft 365-Konten der Opfer zu kompromittieren.

Die Betreiber von Ransomware haben sich im 4. Quartal weiter verstärkt auf Energieunternehmen konzentriert. Initial Access Broker (IABs) suchten aktiv nach Zugangsdaten und kompromittierten Systemen in den Netzwerken der Energiebetreiber.

Aufgrund des Terroranschlags der Hamas auf israelische Zivilisten und der darauf folgenden militärischen Reaktion Israels im Gazastreifen haben sich die Cyberkonflikte zwischen den beteiligten Nationalstaaten verschärft. Zusätzlich zu den laufenden Online-Operationen im Rahmen des russisch-ukrainischen Konflikts sind staatlich gesponserte Cyberangriffe nun häufiger geworden.



WICHTIGE EREIGNISSE Q4

1 Okt

Phishing-Angriffe auf das Gastgewerbe gehen weiter

Angreifer führten im Gastgewerbe raffinierte Phishing-Angriffe durch, die zu schwerwiegenden Sicherheitsverletzungen bei Unternehmen wie MGM und Caesars führten. Mimecasts Daten zeigen, dass das Gastgewerbe im vierten Quartal 2023 das zweithäufigste Ziel von Angriffen war.

ARTIKEL

3 Okt

EvilProxy Phishing-Angriff zielt auf US-Firmen

Forscher haben einen Angriff dokumentiert, bei dem E-Mails, die als Benachrichtigungen von der Jobbörse Indeed.com getarnt waren, eine Umleitungsschwachstelle aufwiesen. Der Angriff wurde über die Phishing-as-a-Service (PhaaS)-Plattform EvilProxy gestartet und richtete sich gezielt gegen Führungskräfte in der Banken- und Versicherungsbranche.

ARTIKEL

9 Okt

Hacktivisten beteiligen sich aktiv an beiden Seiten des Konflikts zwischen Israel und Hamas

Es kam zu Dutzenden, möglicherweise sogar Hunderten von Angriffen auf Websites und Netzwerke, als die Cyberoperationen nach dem Terroranschlag der Hamas auf Israel und der anschließenden militärischen Reaktion Israels verstärkt wurden. Das Internationale Komitee vom Roten Kreuz hat Richtlinien für den Einsatz ziviler Hacker veröffentlicht, um den Schaden für die Zivilbevölkerung während des Konflikts zu minimieren.

ARTIKEL

17 Okt

Angreifer kombinieren DadSec Phishing, Cloudflare

In einem typischen Szenario zur Umgehung der Zwei-Faktor-Authentifizierung kombinieren Angreifer verschiedene Taktiken: Sie starten einen AitM-Phishing-Angriff mit gefälschten E-Mails, die Links enthalten, nutzen das Turnstile-Tool von Cloudflare zur menschlichen Verifizierung und erstellen eine gefälschte Microsoft 365-Website, um Benutzer zur Preisgabe ihrer Anmeldedaten und Zwei-Faktor-Codes zu verleiten.

ARTIKEL

18 Okt

Staatlich geförderte Akteure nehmen WinRAR Flw ins Visier

Der mit Russland verbundene Bedrohungsakteur Sandworm, auch bekannt als FrozenBarents und Black Energy, gab sich als ukrainische Schule für Drohnenkriegsführung aus und verschickte eine bösartige ZIP-Datei, die eine Sicherheitslücke im Archivierungsprogramm WinRAR ausnutzte.

ARTIKEL

6 Nov

Iranische Gruppe zielt auf israelische Sektoren

Die mit dem Iran verbundene Gruppe Agonizing Serpens setzte eine fortlaufende Kampagne von Datendiebstahl und Löschangriffen gegen Israels Hochschul- und Technologiesektor fort. Diese Angriffe zielen darauf ab, massive Datenverluste zu verursachen und stehen nicht im Zusammenhang mit Lösegeldforderungen.

ARTIKEL

12 Nov

Der Energiesektor sieht sich im Winter zunehmenden Angriffen ausgesetzt

Die IABs sind aktiv darin, gestohlene Zugangsdaten zu suchen und andere Methoden zu verwenden, um Energienetzwerke zu kompromittieren. Bis Ende 2023 haben die gemeldeten Ransomware-Angriffe auf den Energiesektor zugenommen, insbesondere in Nordamerika, Asien und der Europäischen Union (EU).

ARTIKEL

29 Nov

Finanzdienstleistungs-Phishing liefert LUMMA-Malware

Phishing-E-Mails mit gefälschten Rechnungen führten zu einer bösartigen Website, die Benutzer dazu verleitet, eine JavaScript-Datei herunterzuladen, die die informationsdiebstahlende LUMMA-Malware installiert.

ARTIKEL

6 Dez

ChatGPT-Schutzmaßnahmen können umgangen werden, um Phishing-E-Mails zu erstellen

Die BBC nutzte die kostenpflichtige Version von ChatGPT und spezielle Anpassungen, um einen privaten Bot namens Crafty Emails zu entwickeln. Dieser Bot wurde vom Nachrichtendienst verwendet, um eine Vielzahl von bösartigen Phishing-Aufgaben auszuführen. Der Dienst generierte Variationen beliebter Betrugsmaschen wie die “Hi Mum”-Täuschung, bei der ein Elternteil um Geld gebeten wird, sowie Spear-Phishing-E-Mails. Der Bot ermöglichte es auch, kulturell unterschiedliche Versionen dieser Angriffe zu erstellen.

ARTIKEL

19 Dez

Strafverfolgungsbehörden schließen ALPHV-Website

Die Datenleck- und Verhandlungsplattformen der ALPHV/BlackCat-Ransomware-Bande verschwanden aus dem Internet, nachdem die Strafverfolgungsbehörden aktiv wurden. Das US-Justizministerium gab an, die Websites abgeschaltet zu haben und bot 500 Opfern ein Entschlüsselungstool an. Berichten zufolge erlangte die Gruppe jedoch später wieder Zugang zu den Websites.

ARTIKEL

TOP-BEDROHUNGSKAMPAGNEN Q4

Jedes Quartal wählen wir eine Auswahl der Bedrohungen aus, die wir in diesem Bericht analysieren. Einige Kampagnen zeigen ein signifikantes Volumen, wie aus den Sparklines (siehe unten) hervorgeht, die die Anzahl der im Quartal entdeckten Bedrohungen darstellen. Andere heben interessante Angriffstechniken oder Ziele hervor.

Microsoft QR-codes

Seit Beginn der Pandemie sind QR-Codes zunehmend populär geworden, und Mimecast blockiert regelmäßig Kampagnen, die diese neuen Barcodes nutzen, um Links zu verschleiern. Verbraucher und Arbeitnehmer verwenden QR-Codes nun häufig, sei es um eine digitale Speisekarte in einem Restaurant aufzurufen, Informationen über eine Veranstaltung zu erhalten oder Software durch einen einfachen Linkklick zu installieren. Dadurch ist das Misstrauen der Benutzer gegenüber solchen verschleierten Links gesunken, was dazu führt, dass sie eher bereit sind, die Codes zu scannen, ohne auf die Sicherheitsrichtlinien ihrer Organisation zu achten.

Im vierten Quartal stieß Mimecast auf einen Phishing-Versuch, bei dem sich die E-Mail als Unternehmen ausgab und das Opfer dazu aufforderte, die Microsoft-Authentifizierung einzurichten. Da der Inhalt der E-Mail als Bild eingebettet war und der Benutzer nichts anklicken musste, wurden viele Sicherheitslösungen nicht auf den Angriff aufmerksam. Wenn jedoch der Link hinter dem QR-Code gescannt wurde, gelangte der Benutzer auf eine Seite, die versuchte, die Anmeldedaten für Microsoft Office 365 zu stehlen.

DocuSign QR-Codes

Angriffsakteure bevorzugen nicht nur QR-Codes für Microsoft-gebrandmarktes Phishing; sie missbrauchen auch gerne andere Infrastrukturen. Mimecast stieß im vierten Quartal auf eine Kampagne, die sich auf den sicheren Dokumentenaustauschdienst DocuSign konzentriert. Die Kampagne tarnt einen bösartigen Link als QR-Code, der angeblich zu einem Dokument führt, das von der Gehaltsabteilung geteilt wurde.

Spam-Kampagne für Bankbetrug in Mexiko

Eine Gruppe für Bankbetrug hat im Dezember eine bedeutende URL-basierte Kampagne gestartet, die hauptsächlich Lateinamerikanische Länder, insbesondere Mexiko, zum Ziel hat. Die Gruppe verwendet bescheidene Spam-Kampagnen, bestehend aus 1.000 bis 6.000 E-Mails, die von Domänen gesendet werden, die vom Bedrohungsakteur registriert wurden. Opfer, die auf die in den E-Mails enthaltenen Links klicken, laden Malware auf ihre Systeme herunter. Mimecast hat zwei URL-Formate identifiziert, die von der Gruppe in ihren Kampagnen verwendet werden, die bis April 2023 zurückreichen.

Google App Script-Angriffe

Angreifer führten mehrere Kampagnen durch, bei denen Google App Script verwendet wurde, eine Plattform für die schnelle Anwendungsentwicklung, die dazu dient, Geschäftsanwendungen für die Integration in Google Workspace zu erstellen. Basierend auf JavaScript kann Google App Script auf Daten aus Gmail, dem Kalender und persönlichen Speicherplätzen von Google zugreifen. Angreifer haben diese Technologie missbraucht, indem sie Software-Schwachstellen ausnutzten, um Phishing-Seiten zu erstellen und über die verknüpften Anwendungen Malware zu verbreiten.

Meta Instagram-Impersonation

Eine weitere bedeutende Kampagne imitiert Meta Instagram mit einer Benachrichtigung, die darauf hinweisen soll, dass ein Urheberrechtsverstoß vorliegt. Die ersten Versionen der Warnung sind nicht überzeugend, da sie grammatikalische Fehler enthalten und einen sehr informellen Ton verwenden. Die Angreifer nutzen jedoch legitime Cloud-Infrastrukturdienste wie Salesforce, um die Benachrichtigungen zu senden, wodurch es den Nachrichten gelingt, anfängliche Filter zu umgehen. Das Ziel der Gruppe hinter den Angriffen ist es, es den Angreifern zu ermöglichen, die Zwei-Faktor-Authentifizierung zu umgehen und Zugang zu Konten zu erlangen.

TOP RATSCHLÄGE

Im Verlauf des Quartals haben Regierungsquellen zahlreiche Sicherheitshinweise für Unternehmen herausgegeben. Dazu zählen Warnungen vor der anhaltenden Verwendung von Spear-Phishing durch den russischen Bedrohungsakteur Star Blizzard sowie vor der zunehmenden Nutzung unsicherer Drittanbieter zur Kompromittierung von Zielen.

Zusätzlich haben die NSA und die CISA eine Liste mit zehn häufigen Fehlkonfigurationen im Bereich der Cybersicherheit erstellt, die zu Sicherheitsverstößen führen können.

5 Okt [NSA/CISA] NSA und CISA Red und Blue Teams teilen die Top Ten der Cybersecurity-Fehlkonfigurationen

Die Nationale Sicherheitsbehörde (NSA) und die Agentur für Cybersicherheit und Infrastruktursicherheit (CISA) haben eine Top-10-Liste der häufigsten Fehlkonfigurationen im Bereich der Cybersicherheit in großen Unternehmen veröffentlicht. Dazu gehören beispielsweise das Belassen von Anwendungen in ihrer Standardkonfiguration und die fehlende Netzwerksegmentierung. Für jede dieser Fehlkonfigurationen haben die Agenturen auch die am häufigsten von Angreifern verwendeten Taktiken, Techniken und Verfahren aufgelistet. **REFERENZ**

7 Nov [FBI] Ransomware-Akteure verschaffen sich weiterhin Zugang über Drittanbieter und legitime System-Tools

Die Angriffe richteten sich auf Drittanbieter und Management-Tools, um bestimmte Unternehmen zu kompromittieren, insbesondere in den Bereichen Glücksspiel und Gastgewerbe. Die Angriffe auf Drittanbieter im Glücksspielsektor zielten häufig auf kleine und Stammescasinos ab. Dabei führten Callback-Phishing-Angriffe zu Datendiebstahl und zur Installation von Ransomware auf Unternehmenssystemen. **REFERENZ**

16 Nov [FBI/CISA] Datendiebstahl und Erpressung zielt auf Unternehmen durch IT-Drittanbieter

Das Federal Bureau of Investigation (FBI) und die CISA haben eine Analyse über die Scattered Spider-Gruppe veröffentlicht. Diese Gruppe gibt sich als IT-Helpdesk-Mitarbeiter aus und instruiert Angestellte, kommerzielle Fernzugriffs-Tools auszuführen, um die mehrstufige Authentifizierung zu umgehen. **REFERENZ**

7 Dez [NCSC/NSA/FBI/CISA/ACSC/CCCS] Russischer FSB Cyber-Akteur Star Blizzard setzt weltweite Spear-Phishing-Kampagnen fort

Die mit Russland verbundene Gruppe Star Blizzard hat eine Vielzahl von Organisationen mit Spear-Phishing-Angriffen ins Visier genommen. Diese Angriffe basieren auf gut recherchierten Lockvögeln, die auf sozialen und beruflichen Kontakten beruhen und in der Regel mit einem bösartigen Link enden. Obwohl die Gruppe hauptsächlich auf Organisationen in den Vereinigten Staaten und Großbritannien abzielt, wurden auch Kampagnen gegen Organisationen in NATO-Ländern und den Nachbarländern Russlands durchgeführt. **REFERENZ**

19 Dez [CISA/FBI] #StopRansomware : ALPHV Blackcat

Das FBI und die CISA haben ein gemeinsames Advisory veröffentlicht, das die Indikatoren für Kompromittierung (IoCs) der neuesten Version der Ransomware beschreibt, die von der ALPHV/BlackCat-Gruppe veröffentlicht wurde, bekannt als ALPHV Blackcat Ransomware 2.0 Sphynx. Bis September 2023 hatte die Gruppe mehr als 1.000 Unternehmen kompromittiert, wobei drei Viertel dieser Unternehmen in den Vereinigten Staaten ansässig waren. Die Gruppe erhielt fast 300 Millionen Dollar an Lösegeldzahlungen. **REFERENZ**

WIE SIE AKTIV WERDEN KÖNNEN

Cyberkriminelle und Bedrohungsakteure haben oft das Ziel, Schlüsselpositionen, ungepatchte Schwachstellen sowie unsichere Lieferketten und Drittanbieter auszunutzen. Unternehmen sollten Maßnahmen ergreifen, um ihre hochrangigen Benutzer zu schützen und Strategien zu entwickeln, um Angreifer zu verlangsamen.

- Bedrohungsspezifische Gegenmaßnahmen
- Allgemeine Empfehlungen zurBekämpfung von Bedrohungen
- Schritte speziell für Mimecast-Kunden

Bedrohungsspezifische Gegenmaßnahmen

Bedrohungsspezifische Gegenmaßnahmen Schützen Sie Schlüsselpositionen

Angreifer haben es vor allem auf bestimmte Unternehmensrollen abgesehen. Daher sollten Unternehmen bestimmte Mitarbeiter von potenziell bösartigen Inhalten wie ausführbaren Dateien und Skripten in Dokumenten fernhalten. Vertriebsmitarbeiter und Führungskräfte sollten beispielsweise keinen Code erhalten oder ausführen, während IT-Administratoren mithilfe der Erkennung von anormalem Verhalten überwacht werden sollten.

Verlangsamen Sie Angreifer durch Segmentierung und Täuschung

Einige Angreifer - insbesondere Ransomware-Gruppen, wie Cl0p - entwickeln ihre eigenen Zero-Day-Exploits, um bisher unbekannte Schwachstellen anzugreifen . Netzwerksegmentierung kann sensible Teile des Netzwerks vor Angreifernabschirmen, während Täuschungstechniken wie Honeytokens sowohl die Angreifer verlangsamen als auch die Verteidiger alarmieren können.

Entwickeln Sie eine Strategie für eine sichere Lieferkette

Angreifer haben es zunehmend auf Drittanbieter und professionelle Dienste abgesehen, die als alternative Zugangswege zu den Zielnetzwerken dienen. Unternehmen sollten Mindestanforderungen an die Sicherheit ihrer Partner und Dienstleister aufstellen und Wege finden, um deren Einhaltung zu messen. Es wird auch empfohlen, dass Transaktionen über spezielle oder authentifizierte Systeme abgewickelt werden, was das Misstrauen der Benutzer schürt, wenn Zahlungsaufforderungen per E-Mail eingehen.

Benutzer aufklären und bösartige QR-Codes blockieren

QR-Codes gewinnen an Bedeutung, da Angreifer versuchen, ihre Links in Spam, Phishing und andere E-Mail-basierte Angriffe durch die Verwendung von Bildern zu verschleiern. Unternehmen sollten nicht nur standardmäßig das Laden von Bildern verhindern, sondern auch ihre Mitarbeiter über die Risiken aufklären, die von QR-Codes ausgehen können. Mimecast bietet die Möglichkeit, festzustellen, ob ein QR-Code zu einer bösartigen Nutzlast führt, und blockiert solche, die dies tun.

Hinweis: CyberGraph-Benutzer sollten die vertrauenswürdigenSeiten nutzen, um sicherzustellen, dass die Banner korrekt geladen werden.

Allgemeine Empfehlungen zur Bekämpfung der Bedrohung

Bewerten Sie Ihre Angriffsflächen
Da viele Unternehmen auf Cloud-Dienste umsteigen, ist die Angriffsfläche insgesamt größer geworden. Unternehmen sollten einen Zero-Trust-Ansatz für den Zugriff ihrer Mitarbeiter auf Unternehmensressourcen verfolgen, indem sie bei Bedarf eine erneute Authentifizierung verlangen und strengen Einblick in alle Vermögenswerte gewähren.

Minimieren Sie Ihre Angriffsfläche, indem Sie ungenutzte Dienste blockieren
Wenn eine Organisation bestimmte Webhosts und Websites nicht verwendet oder erwartet, diese zu verwenden, sollten diese blockiert werden. Wenn Dropbox zum Beispiel nicht zum Unternehmensstandard gehört, sollte es nicht erlaubt sein. Wenn Excel-Dokumente nicht per E-Mail verschickt werden sollen, müssen entsprechende Kontrollen eingerichtet werden, um solche Aktionen zu verhindern.

Priorisieren Sie Schwachstellen für Patches
Angreifer verkürzen weiterhin die Zeit zwischen der Veröffentlichung einer Schwachstelle und der Ausnutzung durch Exploits und Angriffe. Die Liste der bekannten ausgenutzten Schwachstellen (Known Exploited Vulnerabilities, KEVs), die von der US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) geführt wird, ist bis zum Ende des 4. Quartals 2023 auf 1.053 Software-Schwachstellen angewachsen. Es ist jedoch nicht ausreichend, jede Schwachstelle im KEV-Katalog zu patchen. Unternehmen sollten verschiedene Schwachstellenmetriken nutzen und ihr Wissen über kritische Systeme einsetzen, um Prioritäten für das Patchen festzulegen.

Machen Sie Ihre Anmeldedaten resistent gegen Phishing
Unsere Daten (siehe Abbildung 3) zeigen, dass Phishing nach Spam die zweithäufigste Angriffsmethode ist, bei der Angreifer typischerweise E-Mail-Angriffe nutzen, um die Anmeldedaten von Benutzern zu stehlen. Aus diesem Grund sollten sich Unternehmen darauf konzentrieren, die Auswirkungen eines erfolgreichen Phishing-Angriffs zu minimieren. Die Einführung eines zusätzlichen Authentifizierungsfaktors, insbesondere einer Phishing-resistenten Technologie, kann im Rahmen eines Zero-Trust-Ansatzes erheblich zur Reduzierung von Angriffen führen, die auf Anmeldeinformationen basieren. Unternehmen, die sowohl ihre Cloud- als auch ihre interne Infrastruktur mit durchgängiger Multifaktor-Authentifizierung ausstatten, können ihr Risiko deutlich reduzieren.

Schritte speziell für Mimecast-Kunden

- Es wird empfohlen, eine Single Sign-On-Lösung mit Ihrem Identitätsanbieter zu verwenden oder die integrierte Multi-Faktor-Authentifizierung von Mimecast zu nutzen. Diese Maßnahmen helfen, die Möglichkeiten von Angreifern zu verringern, E-Mails als Angriffsvektor zu nutzen. **MEHR ERFAHREN**

- Stellen Sie sicher, dass DNS-Authentifizierungsrichtlinien DMARC-Einträge korrekt erkennen. Eine zweite Richtlinie, die einer Richtliniengruppe zugeordnet ist und bei der die Aktion für DMARC-Fehlschläge auf Ignorieren/Verwalten und für zugelassene Absender eingestellt ist, bietet eine effektive Umgehung für alle legitimen E-Mails, die aufgrund von DMARC-Fehlern abgelehnt oder gekennzeichnet werden. **MEHR ERFAHREN**

- Optimieren Sie den Identitätsschutz gemäß bewährten Richtlinien, indem Sie zwei Richtlinien für die Markierung von Betreff/Body mit 2 Treffern erstellen und eine separate C-Level/VIP-Richtlinie basierend auf der Namensübereinstimmung mit einer Sperrung zur Überprüfung durch den Administrator hinzufügen. Erstellen Sie zusätzlich eine weitere Richtlinie für alle Erkennungen von 3 Treffern oder mehr mit der Aktion “Admin-Hold”. **MEHR ERFAHREN**

- Wenn Sie eine strikte Neuschreibung von URLs aktivieren, stellen Sie sicher, dass alle URLs beim Anklicken gescannt werden. Beachten Sie jedoch, dass auch andere Formate wie IP-Adressen und interne Links, die wie URLs aussehen, umgeschrieben werden könnten. **MEHR ERFAHREN**

- Ziehen Sie in Erwägung, die Auto-Allow-Richtlinien auf ‘strict’ statt ‘allow’ einzustellen, um sicherzustellen, dass die Überprüfung von spam auf Unternehmensebene für externe E-Mail-Empfänger nicht umgangen wird. Diese Einstellung sollte in Verbindung mit ‘Auto Allow spam Detection’ vorgenommen werden, um die zur Überprüfung, um sicherzustellen, dass keine potenziell bösartigen Nachrichten die Überprüfung umgehen. **MEHR ERFAHREN**

- Nutzen Sie vorgefertigte Integrationen mit den meisten SIEM- und XDR-Anbietern, um Protokollerfassung und -analyse zur Durchsetzung von Sicherheitsrichtlinien zu ermöglichen. **MEHR ERFAHREN**

- Verwenden Sie Ihre eigene Bedrohungsintelligenz, um einen Threat Feed von Drittanbietern automatisch für die Ablehnung übereinstimmender Indikatoren zu nutzen. **MEHR ERFAHREN**

- Es wird empfohlen, Endbenutzer-Tools zu verwenden, um potenziell bösartige Nachrichten an das Mimecast Security Operations Center (SOC) zur weiteren eingehenden Analyse zu melden. **MEHR ERFAHREN**

Wenn Sie sich über die Auswirkungen der vorgeschlagenen Einstellungen nicht sicher sind, wenden Sie sich bitte an Ihren Mimecast-Kundenbetreuer, Ihren Customer Success Manager oder rufen Sie den Mimecast-Support an.

RESSOURCEN

Hier finden Sie eine Liste von Regierungsressourcen (Webinare, Papiere, Empfehlungen), die Sicherheitsgruppen besuchen können, um die Bedrohungen und Abwehrmaßnahmen besser zu verstehen.

- **CISA/NSA** NSA und CISA Red and Blue Teams Anteil Top Zehn Cybersecurity Fehlkonfigurationen.
  5 Oktober 2023
- **CISA** CISA Veröffentlichungen Neue Ressourcen Identifizierung Bekannte ausgenutzte Schwachstellen und Fehlkonfigurationen im Zusammenhang mit Ransomware.
  12 Oktober 2023
- **CISA** Phishing-Leitfaden: DenAngriff stoppen Zyklus in der ersten Phase
  18. Oktober 2023
- **CISA/NSA** CISA, NSA, und Partner Veröffentlichung Neue Leitfaden zur Sicherung der Software Lieferkette.
  9 November 2023
- **CISA/NCSC** CISA und UK NCSC Enthüllen Gemeinsame Richtlinien für Sicheres KI System Entwicklung.
  26 November 2023
- **CISA/NCSC /ACSC/FBI** Russisch FSB cyber actor Star Blizzard geht weltweit weiter Speer-Phishing-Kampagnen.
  7 Dezember 2023

SCHLUSSFOL-GERUNG

Im vierten Quartal 2023 haben sich viele der Trends aus den vorangegangenen Quartalen verstärkt. Angreifer nutzen zunehmend Marken, um Nutzer dazu zu verleiten, Spam und Phishing zu vertrauen. Oft verknüpfen sie die Marke mit einem QR-Code oder einem Link zu einem vermeintlich legitimen Dateidienst. Die geopolitischen Spannungen verschärften sich nach dem Angriff der Hamas auf israelische Zivilisten und der darauf folgenden Vergeltungsmaßnahme Israels. Dies führte zu einer Zunahme von Angriffen im Zusammenhang mit diesem Konflikt und neuen Themen für Phishing-Köder.

Im vierten Quartal 2023 haben die Angreifer leicht ihre Zielsektoren angepasst und sich verstärkt auf den Finanzsektor konzentriert, einschließlich Banken und anderen Finanzdienstleistungen, sowie auf professionelle Dienstleistungen wie Personalwesen und Buchhaltung. Auch der Reise-, Hotel- und Gaststättensektor war vermehrt betroffen. Obwohl die Angriffskampagnen gegen den Sektor der Personal- und Rekrutierungsdienstleistungen leicht zurückgingen, bleibt dieser Sektor einer der am dritthäufigsten angegriffenen Branchen.

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®