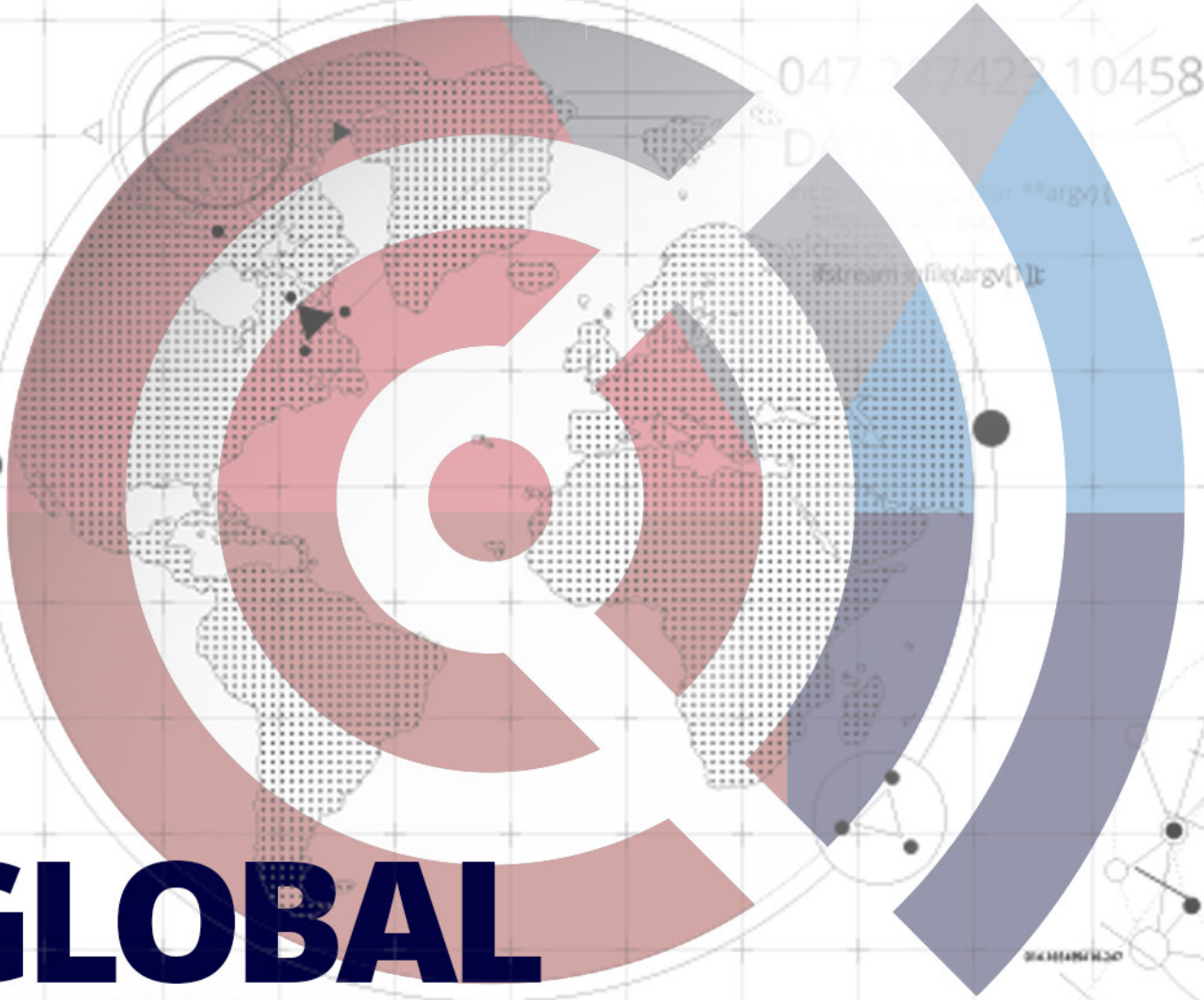
mimecast

RISK RADAR

DETECTION | ANALYSIS | ACTION



GLOBAL THREAT INTELLIGENCE REPORT

JULI BIS DEZEMBER 2024

INHALT.

1.

Einführung.

2.

Zusammenfassung.

3.

Wichtigste Erkenntnisse.

4.

Bedrohungslandschaft.

4.1 Die Bedrohungslandschaft in Diagrammen
4.2 Top-Bedrohungen und -Kampagnen
4.3 Mimecast Risk Radar
4.4 Zeitleiste der wichtigen Ereignisse

5.

Empfehlungen.

5.1 Bedrohungsspezifische Gegenmaßnahmen
5.2 Best Practices und Warnungen
5.3 Spezifische Empfehlungen für Mimecast-Kunden

6.

Fazit.

EINFÜHRUNG.

Moderne Unternehmen brauchen verlässliche Informationen zu aktuellen Bedrohungen, um sich gegen äußerst agile Angreifer verteidigen zu können. Um zu verhindern, dass ihre Geschäftskommunikation und ihre Mitarbeiter gegen sie eingesetzt werden, sollten Unternehmen jeder Größe die folgenden Empfehlungen beachten: Sie sollten immer über die neuesten Bedrohungstrends informiert sein; sie sollten die spezifischen Bedrohungen ihrer Branche und Zulieferer im Auge behalten; sie sollten ihre Abwehrmaßnahmen verstärken; und sie sollten ihre Prozesse entsprechend anpassen.

01

In der zweiten Hälfte des Jahres 2024 verarbeitete Mimecast mehr als 90 Milliarden Datenpunkte für seine fast 43.000 Kunden und identifizierte dabei mehr als 5 Milliarden Bedrohungen. Die Gesamtzahl an Interaktionen, die in diesem sechsmonatigen Zeitraum durch Mimecast geschützt wurden, überstieg diese Zahl noch einmal um ein Vielfaches. E-Mails und Tools für die Zusammenarbeit sind weiterhin die beiden Kanäle, über die die meisten gezielten Angriffe auf Unternehmen ihren Anfang nehmen. Bei Mimecast haben wir daher die Möglichkeit, viele Bedrohungen zu erkennen und zu analysieren, noch bevor sie allgemein bekannt werden.

In der zweiten Hälfte des Jahres 2024 verarbeitete Mimecast mehr als 90 Milliarden Datenpunkte für seine fast 43.000 Kunden und identifizierte dabei mehr als 5 Milliarden Bedrohungen. Die Gesamtzahl an Interaktionen, die in diesem sechsmonatigen Zeitraum durch Mimecast geschützt wurden, überstieg diese Zahl noch einmal um ein Vielfaches.

Unser Global Threat Intelligence Report für das zweite Halbjahr 2024 enthält: Daten aus unseren Systemen – mit denen wir unzählige Millionen Benutzer schützen –; Erkenntnisse von unseren Sicherheitsanalysten; Open-Source-Informationen zu den neuesten Bedrohungen; eine Analyse der aktuellen Bedrohungsaktivitäten; Statistiken zu Angriffstrends; und eine Reihe von Empfehlungen für kleine und große Unternehmen, die ihre Mitarbeiter schützen und die Auswirkungen riskanter Benutzer minimieren möchten.

Wir hoffen, dass Sie aus dem vorliegenden Bericht zur Bedrohungslage des zweiten Halbjahres 2024 wertvolle Insights für die Sicherheitsstrategie Ihres Unternehmens gewinnen können, und wir freuen uns darauf, in Zukunft weitere Erkenntnisse mit Ihnen teilen zu können.

ZUSAMMEN-FASSUNG.

IN DER ZWEITEN HÄLFTE DES JAHRES 2024 MISSBRAUCHTEN BEDROHUNGSAKTEURE ZUNEHMEND LEGITIME DIENSTE, UM IHRE ANGRIFFE ZU VERSCHLEIERN UND ABWEHRSYSTEME ZU UMGEHEN.

Dieser Angriffstrend, bei dem Angreifer sich vertrauenswürdiger Dienste bedienen – das sogenannte Living Off Trusted Services oder LOTS –, bedeutet, dass Unternehmen sich nicht mehr nur auf die Reputation eines Dienstes bzw. auf Authentifizierungssysteme verlassen können, um sich vor Messaging-basierten und menschenorientierten Angriffen zu schützen. Darüber hinaus verstecken sich einige Bedrohungsakteure hinter Drittanbietern – etwa Dienstanbieter oder Softwareprodukte –, um leichter in anvisierte Netzwerke einzudringen.

02

AKTUELLE GEOPOLITISCHE ENTWICKLUNGEN HABEN BEDROHUNGSAKTEUREN NICHT NUR DEN IMPULS ZUR AUSWEITUNG IHRER KOMPROMITTIERUNGSVERSUCHE GELIEFERT, SONDERN AUCH EINE REICHE QUELLE VON THEMEN, AUF DENEN SIE IHRE ANGRIFFE BASIEREN KÖNNEN.

Staatliche Akteure führten weiterhin Cyberangriffe und Cyberspionage aus, um verschleierte Aktionen gegen ihre Rivalen durchzuführen. China kompromittierte die Infrastruktur der USA und Kanadas[1], der Iran und Israel nahmen die Infrastruktur des jeweils anderen Landes ins Visier[2], und Russland hatte es weiterhin auf europäische und amerikanische Organisationen abgesehen –[3]auch nachdem seine Invasion der Ukraine ins Stocken geriet.

1. Tunney, Catharine. „China ‚compromised' Canadian government networks and stole valuable info: spy agency." CBC. 30. Oktober 2024. https://www.cbc.ca/news/politics/cse-cyber-threats-china-1.7367719
2. Lemos, Robert. „As Geopolitical Tensions Mount, Iran's Cyber Operations Grow." Dark Reading. Nachrichtenartikel. 18. September 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow
3. Eddy, Nathan. „Ukraine-Russia Cyber Battles Tip Over Into the Real World." Dark Reading. Nachrichtenartikel. 3. Oktober 2024. https://www.darkreading.com/cyberattacks-data-breaches/ukraine-russia-cyber-battles-tip-over-into-real-world

KI-TECHNOLOGIEN BIETEN WEITERHIN SOWOHL ANGREIFERN ALS AUCH VERTEIDIGUNGSSPEZIALISTEN EINZIGARTIGE VORTEILE.

Cybersicherheitsanalysten können mithilfe von KI-Assistenten potenzielle Sicherheitsereignisse schneller analysieren. Vorfallbearbeiter können KI nutzen, um Angriffe schneller und umfassender abzuwehren und zu beheben. Aber auch Angreifer profitieren: Forschung von Mimecast, bei der wir linguistische Analysen einsetzten, zeigte, dass etwa 12 % aller E-Mails – einschließlich Phishing-Angriffen – Anzeichen dafür aufwiesen, dass sie von großen Sprachmodellen (Large Language Models; LLM) verfasst wurden. Auch Deepfake-Audio und -Video wurden erfolgreich eingesetzt, um CEOs zu imitieren und auf diese Weise Mitarbeiter anzuweisen, Zahlungen auf Konten von Cyberkriminellen zu leisten.

ALLE DIESE TRENDS WERDEN SICH AUCH IM JAHR 2025 FORTSETZEN.

Die Anzahl der Angriffe, bei denen die Cloud auf irgendeine Weise zum Einsatz kam, hat sich im Jahr 2024 mehr als verdoppelt. Außerdem wird unsere geopolitische Lage immer chaotischer: Sowohl Frankreich als auch Deutschland bereiten sich auf neue Wahlen vor, US-Präsident Donald Trump tritt für eine zweite, nicht aufeinanderfolgende Amtszeit an, und Russland und China plustern sich weiterhin mit ihren Militärs auf. Sowohl Sicherheitsforscher als auch Bedrohungsakteure entwickeln neue Wege, um von KI-Systemen zu profitieren, indem sie entweder Sicherheitslücken ausnutzen oder ihre eigenen Angriffsstrategien verbessern.

4. Lee, Evonne. „New Mimecast Threat Intelligence: How ChatGPT Upended Email." Mimecast Threat Intelligence Blog. 30. September 2024. https://www.mimecast.com/blog/how-chatgpt-upended-email/.

WICHTIGSTE ERKENNTNISSE.

Während die Aktivitäten von Bedrohungsakteuren in fast allen Bereichen zugenommen haben, stechen die folgenden fünf Trends besonders hervor.

03

OCTO

SPEZIES

Mit ihrem hochentwickelten Nervensystem und dem großen Gehirn sind sie Meister der **Analyse**. Sie können sich sehr gut an ihre Umgebung anpassen und verschiedenartige Herausforderungen überwinden, was sie zu Spezialisten in der Bedrohungsaufklärung macht.

K-1 ONE

ANGREIFER MISSBRAUCHEN IMMER ÖFTER VERTRAUENSWÜRDIGE DIENSTE (LIVING OFF TRUSTED SERVICES; LOTS).

Die Cloud-Dienste von Microsoft, Google und Evernote werden von Bedrohungsakteuren häufig als Hosts für Payloads und Landing-Pages genutzt. Aber auch andere Cloud-Dienste werden öfter für spezifische Komponenten der Angriffsinfrastruktur missbraucht: Cloudflares Turnstile-CAPTCHAs beispielsweise werden regelmäßig eingesetzt, um Bedrohungsanalysen zu verhindern; DocuSign, TeamViewer und Wave Compliance hosten unwissentlich Inhalte von Angreifern; und Google Gmail sowie Microsoft Outlook (früher Hotmail) werden zum Versand von Phishing-E-Mails missbraucht.

K-2 TWO

GEOPOLITISCHE SPANNUNGEN ERHÖHEN DIE WAHRSCHEINLICHKEIT VON CYBERANGRIFFEN.

Die französischen und deutschen Wahlen sowie die anhaltende Unberechenbarkeit des Russland-Ukraine-Kriegs werden die politischen Spannungen innerhalb der Europäischen Union noch weiter erhöhen. Auch die Abkehr der US-Regierung von vorhersehbaren Normen könnte eine Steigerung der Cyberaktivitäten mit sich ziehen. Experten aus Wirtschaft, Politik und Cybersicherheit warnen zunehmend davor, dass geopolitische Spannungen und Cybersicherheitsrisiken Hand in Hand gehen. In der jährlichen Systemic Risk Barometer Survey der Depository Trust and Clearing Corporation für 2025 gingen geopolitische Risiken und Cyberrisiken als größte Risiken hervor. [5]

K-3 THREE

E-MAIL-AUTHENTIFIZIERUNGSTECHNOLOGIEN ERSCHWEREN ANGREIFERN IHRE ARBEIT, WÄHREND KÜNSTLICHE INTELLIGENZ DIE HÜRDEN FÜR CYBERKRIMINALITÄT GESENKT HAT.

Durch die Nutzung vertrauenswürdiger Dienste können Angreifer immer höhere Authentifizierungsanforderungen von E-Mail-Technologien – wie SPF, DKIM und DMARC – erfüllen und sich so als vertrauenswürdige Quellen ausgeben. Während Angreifer sich also aufgrund moderner Technologien immer komplexere Angriffsmethoden ausdenken müssen, finden sie doch immer noch entsprechende Dienste, um Authentifizierungs- und Abstimmungsprüfungen zu bestehen. Darüber hinaus können sich aufgrund der Verbreitung von KI-Chatbots selbst angehende Cyberkriminelle die für das Hacken notwendigen Fähigkeiten aneignen.

5. „Geopolitical and Cyber Risks Remain Top Threats to the Financial Services Sector in 2025." DTCC. https://www.dtcc.com/news/2024/december/04/geopolitical-and-cyber-risks-remain-top-threats-to-the-financial-services-sector-in-2025

K-4 FOUR

DIE KATEGORIEN „MEDIEN & VERLAGSWESEN“, „KUNST, UNTERHALTUNG & FREIZEIT“ SOWIE „RECHTSDIENSTLEISTUNGEN“ VERZEICHNETEN IN DER ZWEITEN JAHRESHÄLFTE 2024 DIE MEISTEN BEDROHUNGEN PRO BENUTZER.

Die meisten Branchen wiesen ein für sie charakteristisches Bedrohungsprofil auf: In den Bereichen „Kunst, Unterhaltung & Freizeit“ wurde ein höherer Anteil an schädlichen Dateien verzeichnet, während Beschäftigte in der Kategorie „Medien & Verlagswesen“ eine größere Anzahl schädlicher Links erhielten. Angriffe mit Identitätsmissbrauch dominierten das Bedrohungsprofil für den Bereich „Software & SaaS“.

K-5 FIVE

BEI DEN MEISTEN SICHERHEITSVERSTÖSSEN IST DER MENSCH WEITERHIN DIE GRÖSSTE SCHWACHSTELLE.

Da der Großteil dieser Angriffe durch eine Handlung eines Insiders erfolgen, der Angreifern Zugang zu sensiblen oder geschützten Ressourcen gewährt. Aus dem Data Breach Investigations Report (DBIR) von 2024 ging hervor, dass mehr als zwei Drittel (68 %) der Sicherheitsverletzungen im Jahr 2023[6] einen „nicht bösartigen menschlichen Faktor“ aufwiesen. Eine Umfrage aus dem Jahr 2024 unter 1.000 Mitarbeitern ergab, dass ein Drittel (34 %) befürchtet, von Angreifern als Schwachstelle ausgenutzt zu werden, obwohl die große Mehrheit (86 %) sich selbst als sachkundig in Bezug auf Cybersicherheit betrachtete.[7] Mehr als die Hälfte der Befragten fürchteten, ihren Arbeitsplatz zu verlieren, wenn sie ihre Organisation einem Cyberangriff aussetzten.

6. Verizon Data Breach Investigations Report, 2024
https://www.verizon.com/business/resources/reports/dbir/#takeaways
7. Why AI fuels cybersecurity anxiety, particularly for younger employees,
https://www.ey.com/en_us/consulting/human-risk-in-cybersecurity

04

DIE BEDROHUNGSLANDSCHAFT.

- BEDROHUNGSLANDSCHAFT IN DIAGRAMMEN →
- TOP-BEDROHUNGEN & -KAMPAGNEN →
- MIMECAST RISK RADAR →
- ZEITLEISTE DER WICHTIGEN EREIGNISSE →

BAT

SPEZIES

Sie sind spezialisiert auf die **Bedrohungserkennung**. Anhand der Echolotung – also der Aussendung hochfrequenter Töne, die von Objekten abprallen – erhalten sie eine detaillierte Karte ihrer Umgebung. Dies hilft ihnen dabei, Hindernisse zu vermeiden – selbst in völliger Dunkelheit.

04
.1

DIE BEDRO-HUNGSLANDSCHAFT IN DIAGRAMMEN.

Eine Analyse der Bedrohungslandschaft in der zweiten Hälfte des Jahres 2024 zeigte, dass Angreifer zunehmend verbraucher- und unternehmensorientierte Cloud-Dienste verwenden, um der Entdeckung zu entgehen. Mehrere große Cloud-Dienste werden missbraucht, um Inhalte von Angreifern zu hosten, und es werden zunehmend Hyperlinks zur Verbreitung von Schadcode verwendet.

In der zweiten Hälfte des Jahres 2024 verlagerten die Angreifer ihren Fokus auf Nutzer in den Kategorien „Kunst, Unterhaltung & Freizeit“, „Rechtsdienstleistungen“ sowie „Software & SaaS“ – im Gegensatz zur ersten Hälfte des Jahres 2024, als die Branchen „Banking“, „Reisen & Gastgewerbe“ sowie „Kunst & Unterhaltung“ die Liste der Ziele anführten. Über alle Branchen hinweg wurde eine hohe Anzahl von Angriffen mit Massen-E-Mails aus Quellen mit geringer Reputation verzeichnet. Nutzer in der Kategorie „Kunst & Unterhaltung“ wurden verstärkt mit schädlichen Dateien angegriffen, während in der Kategorie „Rechtsdienstleistungen“ vermehrt Fälle von Identitätsmissbrauch auftraten.

Im Folgenden sehen Sie eine Übersicht der Bedrohungslandschaft basierend auf unseren Daten.

W 41°24'12.2 "
E 23°44'54.4"
PE-3 Nvgt B

MISSBRAUCH VON CLOUD-DIENSTEN

#01

Angreifer nutzen zunehmend vertrauenswürdige Dienste (LOTS), um diejenigen Verteidigungsmaßnahmen zu umgehen, die gefährlichen Code sowie schädliche Ressourcen und Online-Dienste als nicht vertrauenswürdig identifizieren und somit abweisen. Bei einigen der Infrastruktur-Hosts, die von Angreifern missbraucht werden, handelt es sich um bekannte Plattformen wie Google Docs, Evernote und Dropbox DocSend. Andere Dienste sind jedoch weniger bekannt, wie Publuu (eine Seite zur Erstellung interaktiver Online-Flipbooks), Wave Compliance (ein Online-Webinar-Host) und Gamma (eine Seite zur Erstellung von Präsentationsfolien).

Eine weitere Angriffsstrategie bestand darin, unterschiedliche Plattformen für verschiedene Angriffsphasen zu nutzen: Für den Versand von Phishing-E-Mails nutzten Angreifer eine bestimmte Gruppe von Plattformen und für das Hosting der Payloads eine bestimmte Reihe von Websites, die oft nur aus einem Webformular oder einer Datei mit einem Link bestehen. Die All-in-one-Marketing-Website GetResponse beispielsweise war eine wichtige Quelle für Phishing-E-Mails, obwohl viele davon nicht unbedingt schädlich, sondern „nur" unerwünscht waren. Obwohl Adobe-Websites nicht zu den größten Payload-Hosts gehören, werden mindestens zwei dieser Websites von Angreifern genutzt, um Landing-Pages zu hosten.

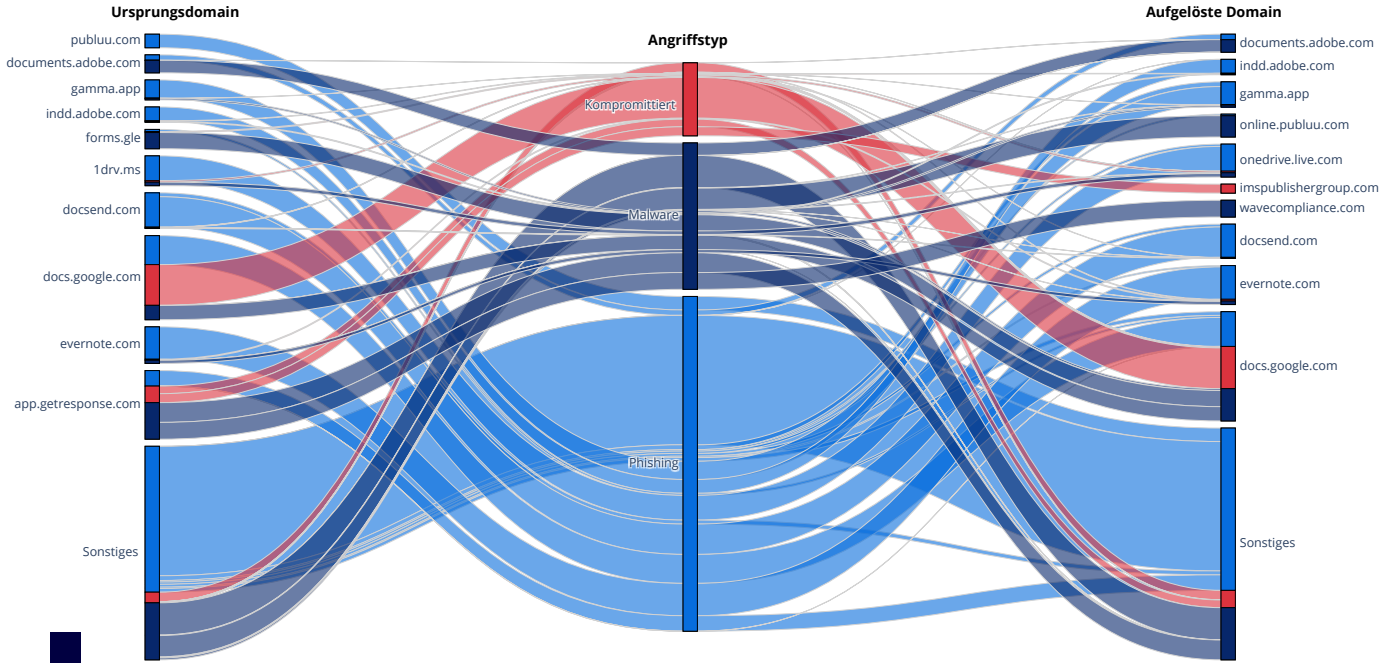


Diagramm 1: Die meisten Ursprungsdomains verweisen auf ähnliche Enddomains. Zum Beispiel hosten die meisten Angreifer, die Evernote als Ursprungsdomain verwenden, dort auch ihre Payloads. Dennoch gibt es einige Ausnahmefälle, bei denen eine Plattform die Weiterleitungsseite hostet (z. B. eine große Menge an Spam vom Marketingdienst GetResponse.com) und eine zweite Plattform die Landing-Page (wie der Schulungs- und Webinardienst Wave Compliance).

BPBS NACH ANGRIFFSTYP

#02

In der zweiten Hälfte des Jahres 2024 machte Spam weiterhin den Großteil der von Mimecast blockierten Nachrichten aus. Über den Sommer hinweg verzeichneten wir einen Anstieg von E-Mail-Nachrichten in der Kategorie „Unerwünscht“, der gegen Ende des Jahres jedoch wieder nachließ. Phishing-Angriffe – die typischerweise eine URL zu einer Website oder einem Dienst enthalten, die von einem Angreifer kontrolliert werden – zeigten im zweiten Halbjahr ein langsames Wachstum.

Mimecast klassifiziert schädliche und unerwünschte Aktivitäten nach dem Stadium, in dem die Erkennung erfolgt.

SPAM fängt Massen-E-Mails von nicht vertrauenswürdigen Domains ab sowie E-Mails, die weit verbreitete Inhalte enthalten.

VERDÄCHTIGE NACHRICHTEN sind solche, die potenziell schädliche Nachrichten, Dateien oder URLs darstellen bzw. enthalten. Das heißt, dass zwar keine schädlichen Inhalte erkannt wurden, dass es aber Anzeichen gibt, dass die Nachricht mit Vorsicht behandelt werden sollte, wie zum Beispiel, wenn sie von einem häufig missbrauchten Dienst oder einer Quelle mit einem schlechten Ruf stammen.

UNERWÜNSCHT schließt Nachrichten ein, die vom Benutzer blockiert wurden.

PHISHING-BEDROHUNGEN zielen darauf ab, Opfer zur Preisgabe sensibler Informationen zu verleiten, wie z. B. Anmeldedaten oder Zahlungsinformationen. Dies umfasst auch Phishing-Links, BEC, Identitätsmissbrauch oder HTML-Anhänge, die Anmeldeseiten imitieren.

MALWARE-NACHRICHTEN enthalten Anhänge, die als schädlich erkannt wurden, oder Links, die zu Malware führen.

Der signifikante Anstieg des Spam-Aufkommens zwischen der ersten und der zweiten Jahreshälfte 2024 ist nicht auf einen Trend im Spam-Volumen zurückzuführen, sondern auf die Weiterentwicklung des Erkennungssystems und der Datenerfassungsstrategie von Mimecast. Mimecast erkennt nun nicht nur E-Mails als Spam, die mit hoher Zuversicht abgelehnt wurden, sondern auch Spam, der vom Gateway zurückgehalten wurde, nachdem Administratoren entsprechende Konfigurationen vorgenommen hatten.

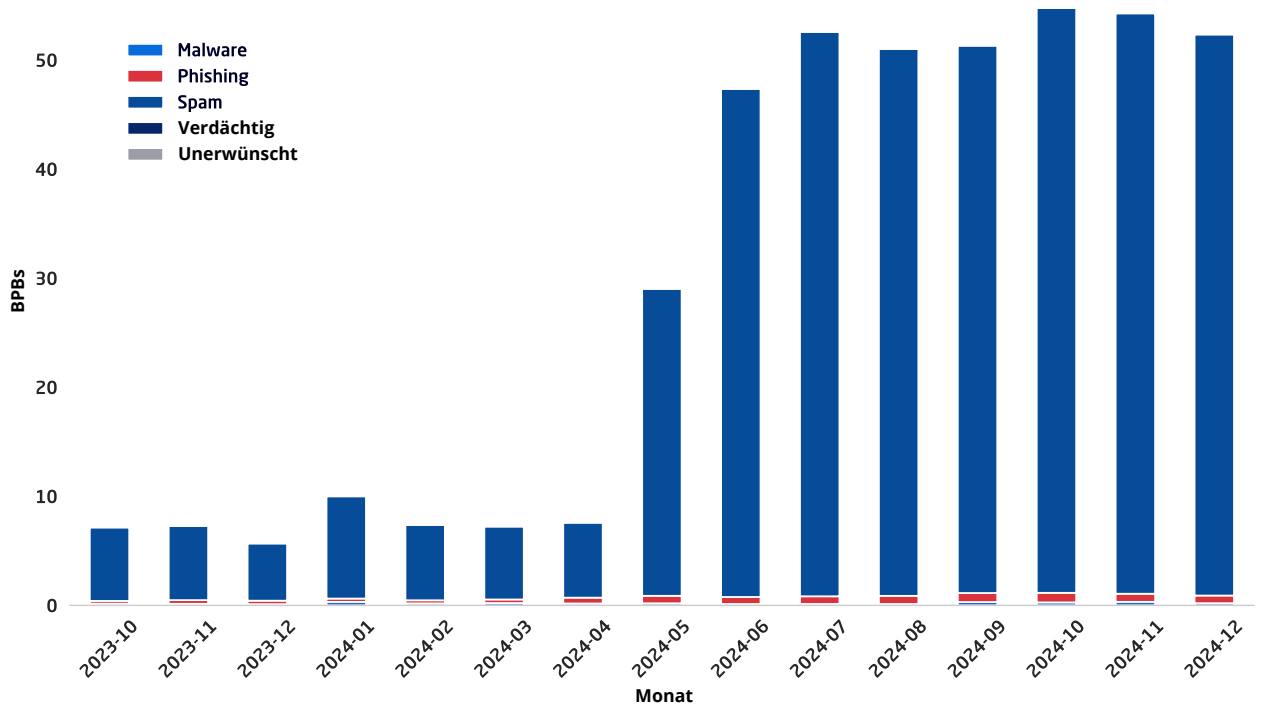


Diagramm 2a: Der signifikante Anstieg an Spam-Vorfällen ist darauf zurückzuführen, dass wir nicht nur Spam-Nachrichten registriert haben, die abgelehnt wurden, sondern auch Nachrichten, die am Gateway zurückgehalten wurden. Mit dieser Änderung profitieren Admins von zusätzlichen Konfigurationsmöglichkeiten für die Zurückhaltung von Spam-Nachrichten.

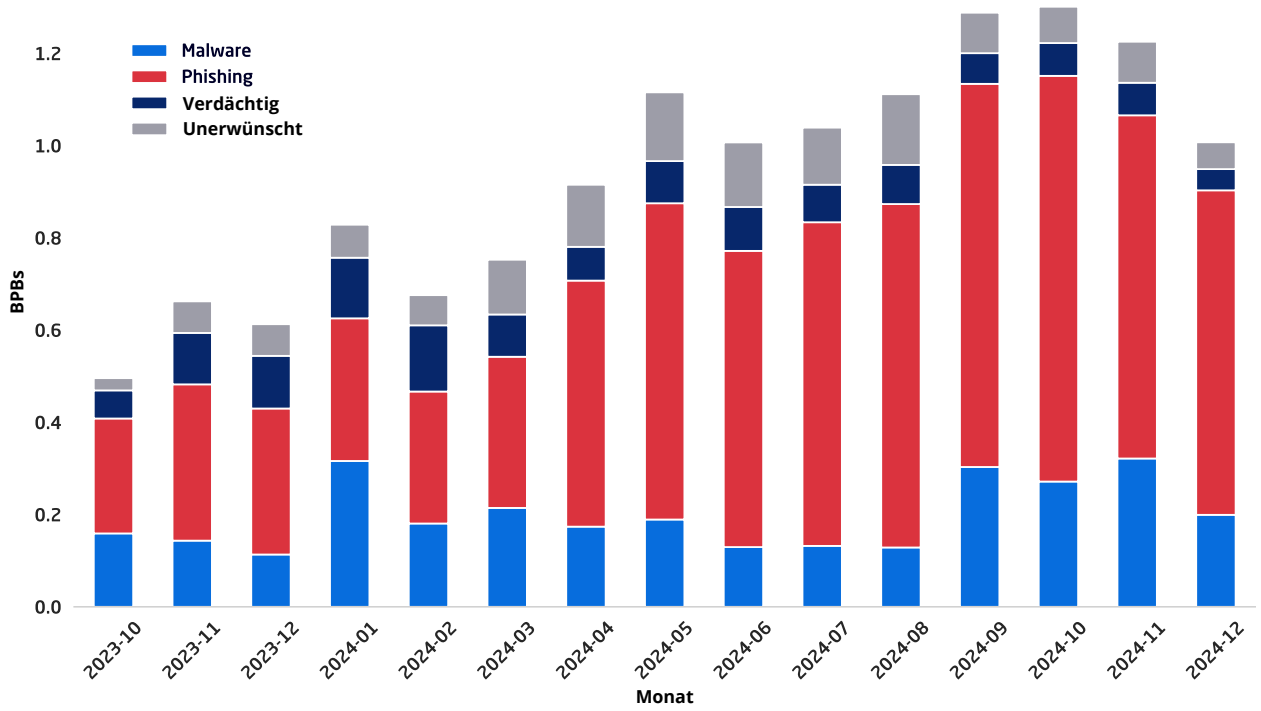


Diagramm 2b: Ignoriert man die enorme Anzahl an Spam in unserem Datensatz, wird deutlich, dass es tendenziell zu immer mehr Phishing-Vorfällen kommt. Gegen Ende der zweiten Jahreshälfte 2024 verzeichneten wir außerdem einen Anstieg der Malware-Angriffe. Im Dezember 2024 stiegen die Malware-Vorfälle in Subsahara-Afrika um 42,14 % – eine deutliche Erhöhung gegenüber dem Vorjahr. Diese Steigerung ist bedingt durch die politische Instabilität in der Region und eine Verstärkung der Cyberaktivitäten. Zusätzlich dazu verzeichnete die Region einen Anstieg von Ransomware-Angriffen, die zunehmend opportunistisch werden. Diese Angriffe nutzen oft Schwachstellen aus und treten als Sekundärinfektionen auf, was einen besorgniserregenden Trend in der Bedrohungslandschaft darstellt.

TOP-ZIELINDUSTRIEN NACH BPBS

#03

Angreifer neigen dazu, unterschiedliche Arten von Angriffen für unterschiedliche Branchen zu nutzen, wodurch jeder Branche ein unverwechselbares Bedrohungsprofil zugewiesen werden kann. Die Kategorie „Kunst, Unterhaltung & Freizeit“ ist der am stärksten betroffene Bereich (nach Entfernung der Spam-Daten) und verzeichnete die größte Anzahl von Bedrohungen pro Benutzer (BPB), wobei die meisten Angriffe aus E-Mails und Nachrichten mit schädlichen Anhängen bestanden.

Die Bereiche „Professional Services: Rechtsdienstleistungen“ sowie „Medien & Verlagswesen“ verzeichneten die nächsthöhere Bedrohungsintensität, mit jeweils fast 9 BPB. In der Kategorie „Professional Services: Rechtsdienstleistungen“ trat eine größere Anzahl von Identitätsmissbrauchsangriffen auf, während in der Kategorie „Medien & Verlagswesen“ eine hohe Anzahl schädlicher URLs verschickt wurde.

Alle Branchen verzeichneten ein erhebliches Volumen an Spam sowie Bedrohungen, die nur deswegen erkannt wurden, weil die Angreifer Infrastruktur mit geringer Reputation nutzten. Bei der Auswertung unserer Analysen entfernten wir die Daten zu Massen-E-Mails, die als Spam bzw. als E-Mails von Absendern mit niedriger Reputation erkannt wurden – diese machten jeweils 17 BPB und 5 BPB aus.

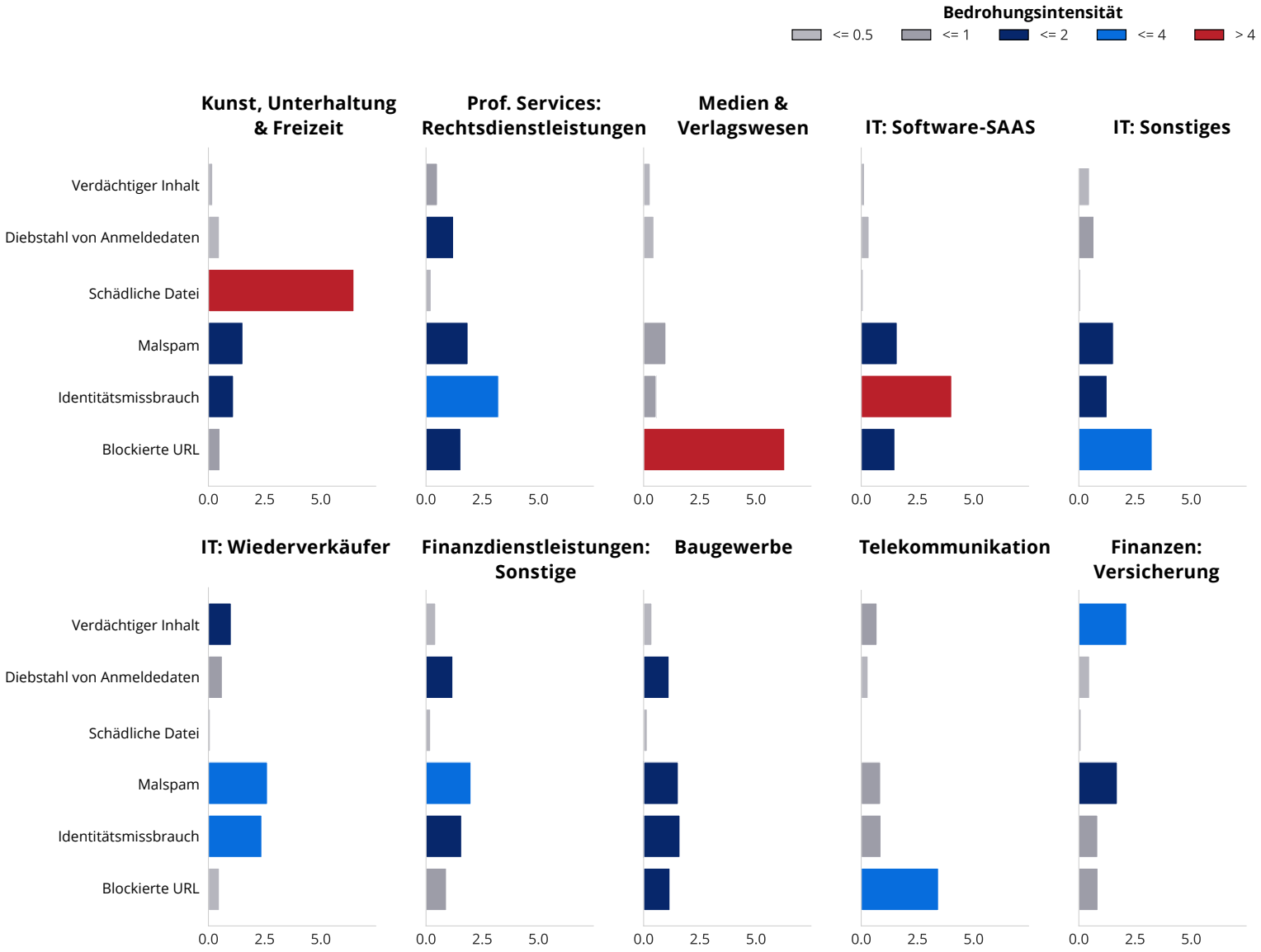


Diagramm 3: Bedrohungsprofil der Top-10-Branchen, ohne die Kategorien „Spam“ und „Geringe Reputation“ (zur Reduzierung der Datenlast). Die BPB-Angaben (x-Achse) sind im Logarithmusformat angegeben.

BEDROHUNGSGRUPPEN #04

Die Zuordnung von Cyberbedrohungen ist ein komplexes Unterfangen, insbesondere da viele Bedrohungsakteure eine Mischung aus Taktiken anwenden und es mittlerweile auch verschiedene Cybercrime-as-a-Service-Modelle gibt, wie zum Beispiel Ransomware-as-a-Service (RaaS), Phishing-as-a-Service (PhaaS) und Initial Access Brokers (IABs). Diese Dienste ermöglichen es mehreren Bedrohungsakteuren, dieselben Werkzeuge und Infrastrukturen wiederzuverwenden, was dazu führt, dass ähnliche Kampagnen von völlig unterschiedlichen Gruppen gestartet werden. Bedrohungsakteure verwenden häufig eine Kombination von Techniken aus verschiedenen Angriffsvektoren und ändern regelmäßig ihre Methoden. Das macht es so schwierig, einen einzelnen Akteur oder ein einzelnes Motiv zu identifizieren.

Traditionelle Zuordnungsmethoden, die auf Infrastruktur- oder Malware-Signaturen basieren, werden zunehmend unzuverlässig. Stattdessen konzentrieren wir uns bei Mimecast auf die Analyse von Taktiken, Techniken und Verfahren, um Bedrohungsoperationen systematisch zu kategorisieren und zu referenzieren. Indem wir die Vorgehensweise von Angreifern nachverfolgen, können wir über unzählige Kampagnen hinweg Bedrohungen gruppieren und Muster identifizieren, selbst wenn herkömmliche Zuordnungsmethoden versagen. Dieser Ansatz bietet uns ein klareres und zuverlässigeres Verständnis davon, wie sich die Fähigkeiten dieser Angreifer weiterentwickeln. Im Folgenden sind die erfolgreichsten Bedrohungsoperationen aufgelistet (mit Mimecast-internen Attributionsnamen). Die Tabelle zeigt auch verbundene Kampagnen, um das Verhalten und die potenziellen Auswirkungen dieser Operationen besser zu beschreiben.

Bedrohungsakteur

MCTA1014

Erstmalig beobachtet: 2020

ZIEL

INFORMATIONSDIEB-
STAHL UND SPIONAGE

ZIELREGION

NORDAMERIKA,
EUROPA UND DER
NAHE OSTEN

Zielsektoren

LUFTFAHRT
RAUMFAHRT
TRANSPORT

OKT. 2024

Neueste Kampagnen

Bedrohungsakteur

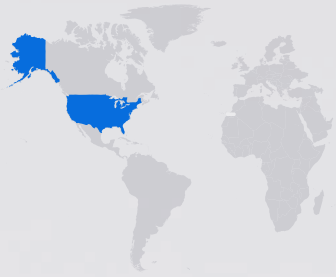
MCTA1003

Erstmalig beobachtet: 2018

ZIEL

DATENDIEBSTAHL

ZIELREGION



VORWIEGEND
IN DEN USA

Zielsektoren

IT
BILDUNGSWESEN

OKT. 2024

Neueste Kampagnen

Bedrohungsakteur

MCTA3010

Erstmalig beobachtet: 2018

ZIEL

ERHEBUNG VON
ANMELDEDATEN ZUR
WEITERGABE

ZIELREGION

SÜDAFRIKA

Zielsektoren

ALLE

NOV. 2024

Neueste Kampagnen

Bedrohungsakteur

MCTA5004

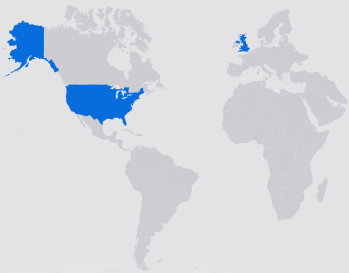
Erstmalig beobachtet: 2024

ZIEL

FINANZEN

Kampagneninformationen

ZIELREGION



GLOBAL
(HAUPTSÄCHLICH USA
UND UK)

Zielsektoren

FERTIGUNG
IMMOBILIEN
EINZELHANDEL

DEZ. 2024

Neueste Kampagnen

Bedrohungsakteur

MCTA3028

Erstmalig beobachtet: 2018

ZIEL

DIEBSTAHL VON ANMELDEDATEN UND PHISHING

Kampagneninformationen

ZIELREGION

GLOBAL

Zielsektoren

ALLE

DEZ 2021

Neueste Kampagnen

Bedrohungsakteur

MCTA3001

Erstmalig beobachtet: 2023

ZIEL

DIEBSTAHL VON ANMELDEINFORMATIONEN UND DATEN

ZIELREGION

AUSTRALIEN

Zielsektoren

HAUPTSÄCHLICH BILDUNGSWESEN

DEZ 2021

Neueste Kampagnen

Bedrohungsakteur

MCTA5005

Erstmalig beobachtet: 2020

ZIEL

FINANZEN

ZIELREGION

GLOBAL

Zielsektoren

ALLE

DEZ 2021

Neueste Kampagnen

Bedrohungsakteur

MCTA3022

Erstmalig beobachtet: 2021

ZIEL

DIEBSTAHL VON ANMELDEDATEN UND PHISHING

ZIELREGION

VORWIEGEND UK

Zielsektoren

ALLE

DEZ 2021

Neueste Kampagnen

TOP-SICHERHEITSLÜCKEN IM ZEITVERLAUF

#05

Während sich die überwiegende Mehrheit der Angreifer, die Software-Schwachstellen ausnutzen, zweier beliebter Sicherheitslücken bedienen (CVE-2017-0199 und CVE-2022-42889), wurden in der zweiten Jahreshälfte 2024 89 verschiedene Schwachstellen genutzt. Beim Vergleich der Top-10-Schwachstellen, die von Mimecast entweder innerhalb einer E-Mail entdeckt oder als Link zugestellt wurden, erzielten sieben einen Exploitability-Prediction-Scoring-System(EPSS)-Wert von mindestens 0,88. Das entspricht einer 88-%igen Wahrscheinlichkeit einer Ausnutzung innerhalb der darauffolgenden 30 Tage. Zwei Schwachstellen – beide im Jahr 2024 entdeckt – wurden noch nicht als ausgenutzt registriert.

Diese Vergleichsübersicht zeigt auch die Divergenz zwischen den Bewertungen des EPSS und des CVSS (Common Vulnerability Scoring System) auf. Die CVSS-Bewertung korreliert tendenziell eher mit dem späteren Schweregrad der Schwachstelle.

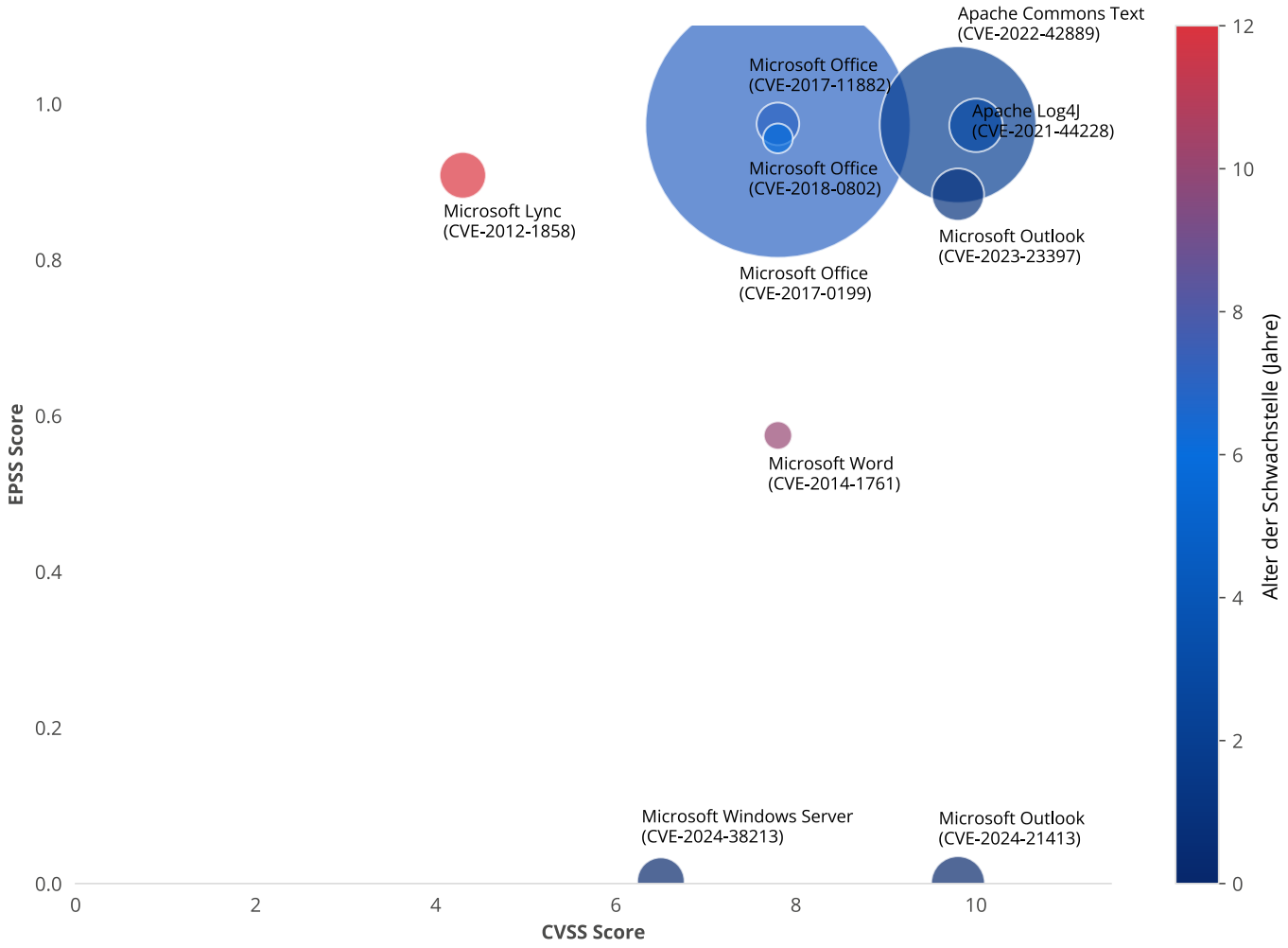


Diagramm 5: Die Top-10-Schwachstellen in Nachrichten, verglichen nach EPSS- und CVSS-Werten. Zwei beliebte Schwachstellen sind mindestens 10 Jahre alt. Stand der EPSS-Daten: 15. Januar 2025.

TOP-BEDROHUNGEN UND -KAMPAGNEN.

04.2

01
OPEN SPOOFING

02
URHEBERRECHTSVERLETZUNG/ABONNEMENT-BENACHRICHTIGUNG

03
BENUTZER SOLL LINKS KOPIEREN UND EINFÜGEN – BETRUG MIT KREDITORENBUCHHALTUNG

04
GEZIELTER BEC-BETRUG MIT AUDIO-DEEPFAKE

05
VERPASSTE LIEFERUNG

06
ÜBERNAHME EINES FACEBOOK-KONTOS

W 41°24'12.2 "
E 23°44'54.4"
PE-3 Nvgt B

PPO-399. 3

#01 OPEN SPOOFING

TECHNIK Kompromittierte Verbraucher-Router leiten gefälschte Phishing-E-Mails über ISP-Dienste weiter

VERWENDETE DIENSTE Zimbra, MagicMail

ZIELE Global – alle Branchen

Link zur Benachrichtig¬ung

Bedrohungsakteur

↓

Verbraucher-ISP-Router werden durch Schwachstellen oder schwache Passwörter ausgenutzt

↓

Router konfiguriert, um als Proxy verwendet zu werden

↓

Phishing-E-Mails werden über die Mailserver von Internetdienstanbietern weitergeleitet

↓

Bösartige Links werden auf verschiedenen Cloud-Diensten gehostet

↓

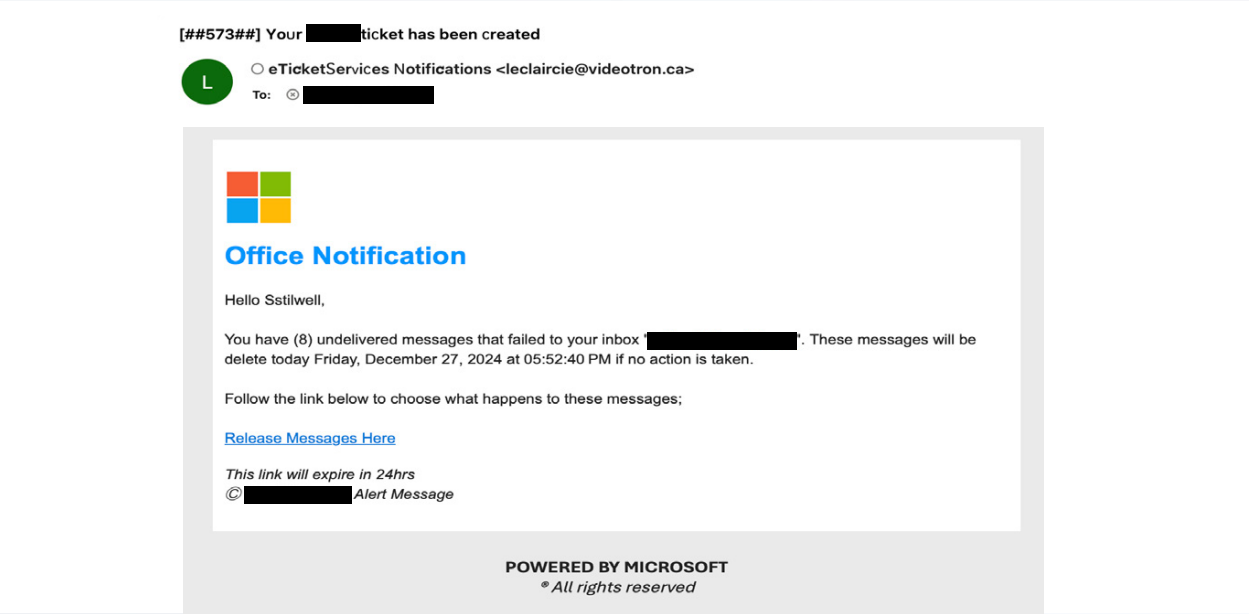
Aufforderung zur Eingabe von M365-Benutzernamen und -Passwort

↓

Anmeldedaten abgegriffen und Benutzer auf die echte M365-Anmeldeseite weitergeleitet

Bedrohungsakteure nutzen kompromittierte Verbraucher-Router als Proxys, um groß angelegte Phishing-Kampagnen über die E-Mail-Dienste von ISPs zu versenden, wodurch sie die eigene Infrastruktur verschleiern und E-Mail-Authentifizierungsmaßnahmen umgehen. Indem sie ISPs mit schwachen oder fehlenden Maßnahmen zur ausgehenden E-Mail-Authentifizierung missbrauchen, können Bedrohungsakteure in großem Umfang Nachrichten versenden und uneingeschränktes Absender-Spoofing betreiben.

Die betroffenen ISPs, die wir bei unserer Untersuchung identifizierten, verwenden E-Mail-Lösungen wie Zimbra und MagicMail und verfügen offenbar nicht über effektive Maßnahmen zur Bekämpfung von ausgehendem Spam. Die Kombination aus unzureichenden Authentifizierungsmaßnahmen und gelockerten Kontrollmechanismen ermöglicht es Angreifern, hohe Versandraten zu erreichen und groß angelegte Spam-Kampagnen ohne wesentliche Unterbrechungen aufrechtzuerhalten.


[##573##] Your [redacted] ticket has been created

L eTicketServices Notifications <leclaircie@videotron.ca>

To: [redacted]

Office Notification

Hello Sstilwell,

You have (8) undelivered messages that failed to your inbox '[redacted]'. These messages will be delete today Friday, December 27, 2024 at 05:52:40 PM if no action is taken.

Follow the link below to choose what happens to these messages;

Release Messages Here

This link will expire in 24hrs

© [redacted] *Alert Message*

POWERED BY MICROSOFT

® All rights reserved

#02 URHEBERRECHTSVERLETZUNG/ABONNEMENT-BENACHRICHTIGUNG

TECHNIK Imitation von Anwaltskanzleien zum Versand gefälschter Copyright-Hinweise zwecks Informationsdiebstahl

VERWENDETE DIENSTE Gmail, Serien-E-Mails

ZIELE Global, aber vorwiegend UK – Einzelhandel, Großhandel, Reise- und Gastgewerbe

Link zur Benachrichtig¬ung

Bedrohungsakteur

↓

Phishing-E-Mails werden über einen Serien-E-Mail-Dienst versendet

↓

Sie enthalten Links zu Inhalten, die auf Dropbox gehostet werden

↓

Laden Sie die ZIP-Datei herunter, die eine ausführbare Datei enthält

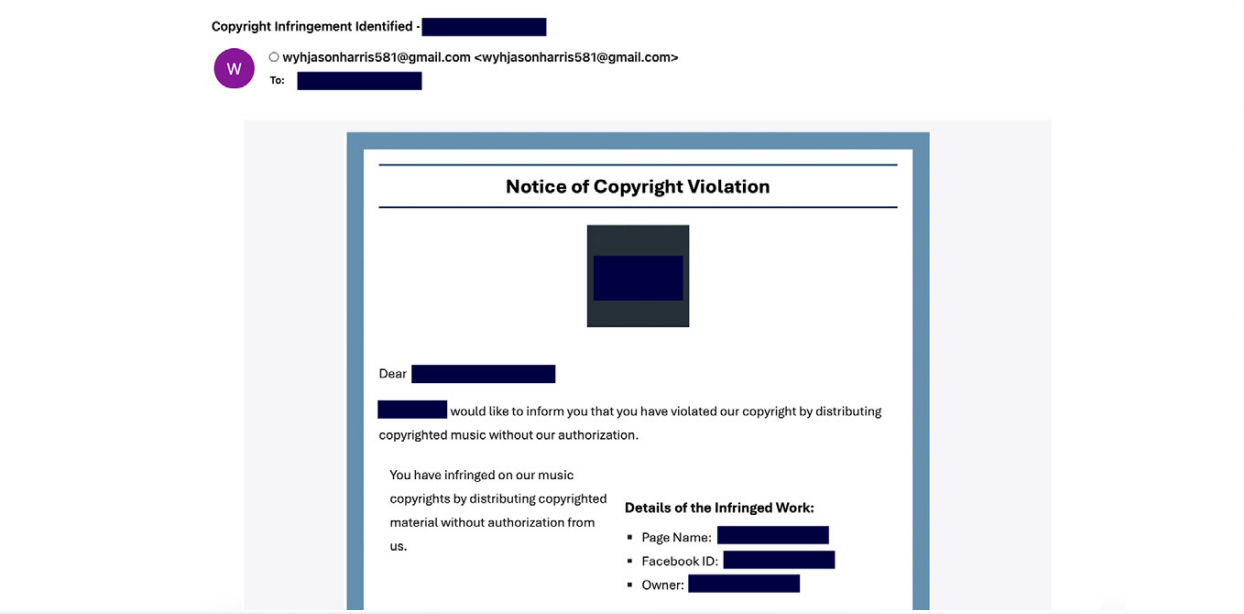
↓

Eine ausführbare Datei lädt einen Infostealer von Github herunter

↓

Vertrauliche Daten werden abgeführt

Angreifer geben sich in E-Mails, die über einen Serien-E-Mail-Dienst via Gmail versendet werden, als renommierte Anwaltskanzleien aus und behaupten, dass das Unternehmen des Empfängers irgendwelche Urheberrechte verletzt habe. Die E-Mail enthält einen direkten Dropbox-Link oder eine Weiterleitung zu Dropbox, die zum Herunterladen einer Zip-Datei mit einer ausführbaren Datei führt. Ziel dieser Kampagnen ist es, mithilfe verschiedener Infostealer sensible Informationen wie Anmeldedaten und Finanzinformationen von infizierten Maschinen zu stehlen.


Copyright Infringement Identified - [redacted]

W wyhjasonharris581@gmail.com <wyhjasonharris581@gmail.com>

To: [redacted]

Notice of Copyright Violation

Dear [redacted]

[redacted] would like to inform you that you have violated our copyright by distributing copyrighted music without our authorization.

You have infringed on our music copyrights by distributing copyrighted material without authorization from us.

Details of the Infringed Work:

- Page Name: [redacted]
- Facebook ID: [redacted]
- Owner: [redacted]

#03 BENUTZER SOLL LINKS KOPIEREN UND EINFÜGEN – BETRUG MIT KREDITORENBUCHHALTUNG

TECHNIK Benutzer davon überzeugen, einen Link zu kopieren und einzufügen, um Abwehrmaßnahmen zu umgehen

VERWENDETE DIENSTE Amazon Simple Email Service, Python-Mailer

ZIELE Vorwiegend USA – Fertigung, Einzelhandel und Rechtsdienstleistungen

Link zur Benachrichtig¬ung

Bedrohungsakteur

↓

Phishing-E-Mail über AWS mit Python-Mailer

↓

Benutzer wird dazu aufgefordert, eine fehlerhafte URL in seinen Browser einzufügen

↓

Weiterleitung zu einer freigegebenen Datei, die auf einem gefälschten SharePoint-Server gehostet wird

↓

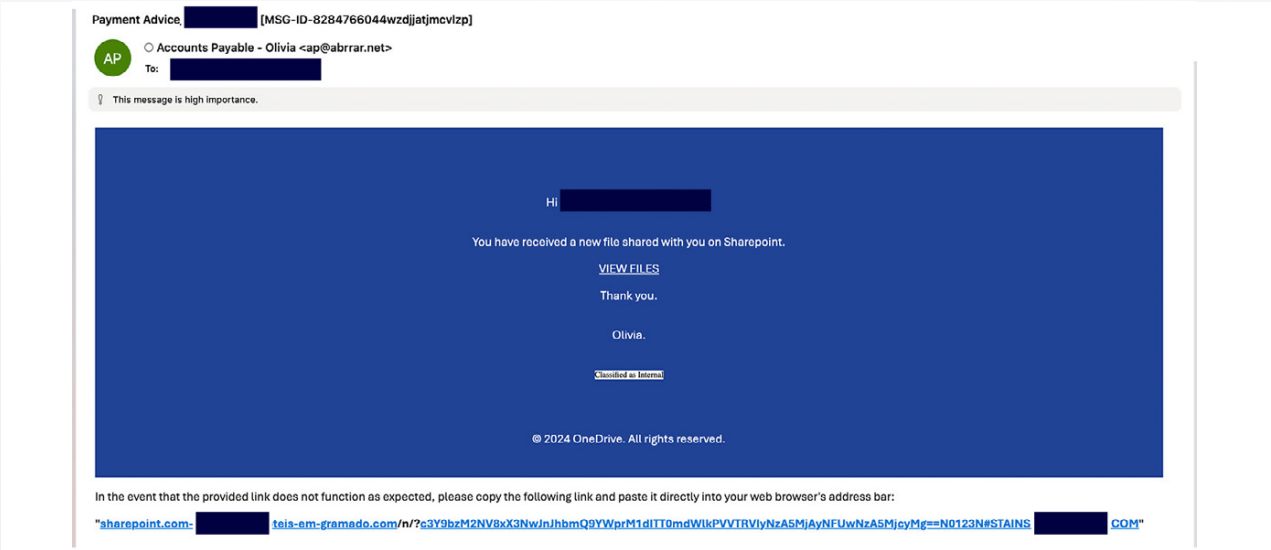
Aufforderung zur Eingabe von M365-Benutzernamen und -Passwort

↓

Verwendung oder Verkauf von Kreditkarte auf illegalen Marktplätzen

Um technische Erkennungssoftware und -dienste zu umgehen, versuchen viele Bedrohungsakteure Benutzer dazu zu verleiten, fehlerhafte Links aus einer E-Mail zu kopieren – in der Regel fehlt in diesen URLs das Präfix „http://“ – und diese in ihren Browser einzufügen. Die von Mimecast analysierten Köder enthielten üblicherweise eine Schaltfläche mit einem defekten Link und einem Text nach dem Muster: „Sollte der Link nicht funktionieren, kopieren Sie bitte die unten stehende URL und fügen Sie sie in Ihren Browser ein.“

Diese Technik geht Hand in Hand mit anderen Verschleierungstaktiken, wie etwa der Verwendung von QR-Codes (um Links für Menschen unlesbar zu machen), sowie Angstmacherei in Verbindung mit der Angabe von Telefonnummern (damit Opfer ein von Angreifern betriebenes Callcenter anrufen). Das Ziel von Kampagnen, die diese Angriffsstrategie nutzen, besteht typischerweise darin, Anmeldedaten der Opfer zu sammeln.


Payment Advice [redacted] [MSG-ID-8284766044wzdjjatjmcvlzp]

AP Accounts Payable - Olivia <ap@abrrar.net>

To: [redacted]

This message is high importance.

Hi [redacted]

You have received a new file shared with you on Sharepoint.

VIEW FILES

Thank you.

Olivia.

Classified as Internal

© 2024 OneDrive. All rights reserved.

In the event that the provided link does not function as expected, please copy the following link and paste it directly into your web browser's address bar:

"sharepoint.com- [redacted] teis-em-gramado.com/n/?c3Y9bzM2NV8xX3NwJnJhbmQ9YWprM1dlTT0mdWlkPVVTRVIyNzA5MjAyNFUwNzA5MjcyMg==N0123N#STAINS [redacted] COM"

#04 GEZIELTER BEC-BETRUG MIT AUDIO-DEEPFAKE

TECHNIK Audio-Deepfake, Business Email Compromise (BEC)
VERWENDETE DIENSTE Adobe Sign, DocuSign
ZIELE Global – überwiegend Finanzsektoren

Link zur Benachrichtig¬ung

Bedrohungsakteur

↓

BEC-E-Mail über Docusign oder AdobeSign

↓

Benutzer unterzeichnet eine digitale Geheimhaltungsvereinbarung

↓

Benutzer ruft eine gefälschte Nummer zur Verifizierung der Geheimhaltungsvereinbarung an

↓

E-Mail-Interaktion führt zur Ausstellung einer Rechnung

↓

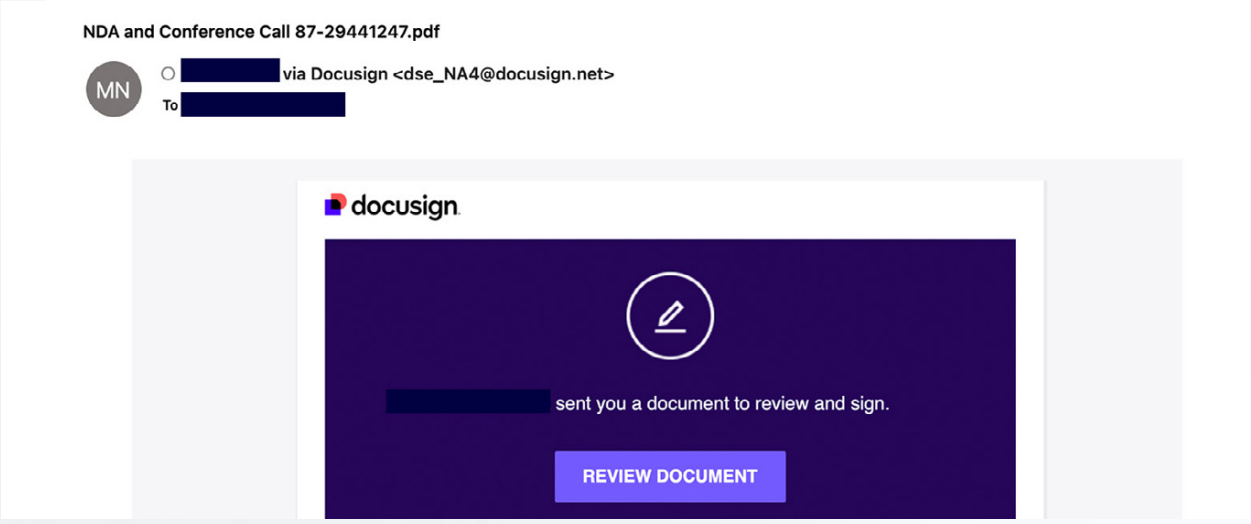
Deepfake-Audio von einem leitenden Angestellten zur Bestätigung der Zahlung

↓

Zahlung auf das Bankkonto eines Bedrohungsakteurs

Mitarbeiter im Bankwesen, Versicherungswesen und anderen Finanzsektoren erhalten Spear-Phishing-E-Mails von einer angeblichen Anwaltskanzlei, die über einen vertrauenswürdigen Dienst wie DocuSign oder Adobe Sign versendet wurden.

Diese Nachrichten fordern Mitarbeiter dazu auf, eine Vertraulichkeitsvereinbarung zu unterschreiben und dann eine Nummer anzurufen, die angeblich von einer Anwaltskanzlei stammt, die jedoch vom Angreifer kontrolliert wird. Der Bedrohungsakteur gibt sich als Mitarbeiter der Anwaltskanzlei aus und nutzt dabei Deepfake-Audiotechniken, um seine Stimme zu verstellen. Er sendet eine E-Mail von einer von ihm kontrollierten Domain, die der Domain der nachgeahmten Anwaltskanzlei ähnelt. Der Angreifer sendet dann eine Rechnung, die auch wieder angeblich von der Anwaltskanzlei stammt. Schließlich folgt ein Deepfake-Anruf, in dem der Angreifer sich als CEO des Unternehmens oder eine andere Führungskraft ausgibt.



#05 VERPASSTE LIEFERUNG

TECHNIK Missbrauch vertrauenswürdiger Dienste (LOTS)
VERWENDETE DIENSTE S3-Buckets auf AWS zum Hosten von HTML-Dateien
ZIELE UK – gemeinnützige Organisationen und Wohnungswirtschaft

Link zur Benachrichtig¬ung

Bedrohungsakteur

Phishing-E-Mail über Biglobe ISP

Umgeleitet zu einer auf AWS gehosteten HTML-Datei

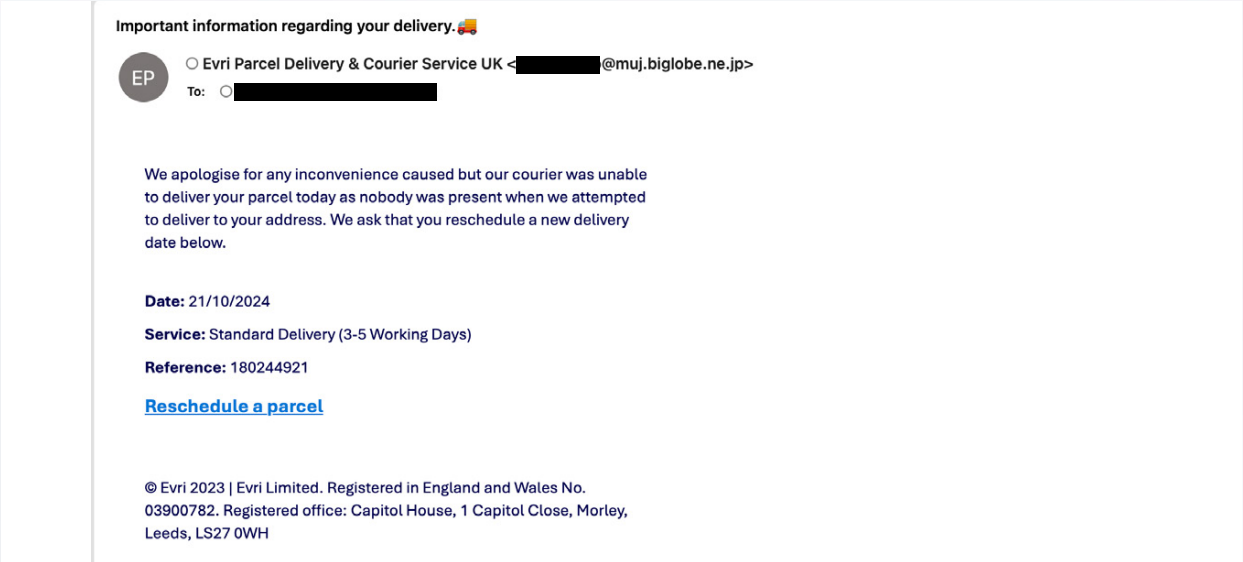
HTML-Datei täuscht EVRI-Seite für eine verpasste Zustellung vor

Personenbezogene Daten und Kreditkarteninformationen werden für die aktualisierte Lieferung bereitgestellt

Verwendung oder Verkauf von Kreditkarte auf illegalen Marktplätzen

Mithilfe von BIGLOBE – einem japanischen Dienst, der häufig von Bedrohungsakteuren missbraucht wird – werden Nachrichten an gemeinnützige Organisationen und Wohnungsbaugesellschaften im Vereinigten Königreich gesendet. Darin werden Empfänger über eine verpasste Lieferung informiert.

Viele asiatische ISPs lassen den Missbrauch ihrer Netzwerke zu – oder wissen nicht, zu welchen Zwecken ihre Dienste missbraucht werden. Bedrohungsakteure nutzen diese ISPs (und andere) aus: Sie erwerben authentifizierte Konten über Untergrundmarktplätze, sodass sie legitimen Zugang zu deren Infrastruktur erhalten und schädliche E-Mails versenden können, die die meisten E-Mail-Authentifizierungsprotokolle umgehen.



Important information regarding your delivery.🚚

EP Evri Parcel Delivery & Courier Service UK <[redacted]@muj.biglobe.ne.jp>
To: [redacted]

We apologise for any inconvenience caused but our courier was unable to deliver your parcel today as nobody was present when we attempted to deliver to your address. We ask that you reschedule a new delivery date below.

Date: 21/10/2024

Service: Standard Delivery (3-5 Working Days)

Reference: 180244921

Reschedule a parcel

© Evri 2023 | Evri Limited. Registered in England and Wales No. 03900782. Registered office: Capitol House, 1 Capitol Close, Morley, Leeds, LS27 0WH

#06 ÜBERNAHME EINES FACEBOOK-KONTOS – MARKENIMITATION

TECHNIK Jobköder in sozialen Medien, bei denen Angreifer sich als Marken wie Victoria's Secret, Red Bull und Coca-Cola ausgeben

VERWENDETER DIENST Recruitee

ZIELE Größtenteils UK und USA – vorwiegend Medien, Verlagswesen und Einzelhandel

Bedrohungsakteur

↓

Phishing-E-Mail, die über das Recruitee CMS gesendet wurde

↓

Anmeldeseite auf einer Lookalike-Domain der nachgeahmten Marke

↓

Anmeldung über eine gefälschte Facebook-Seite zur Einreichung von Bewerbungen

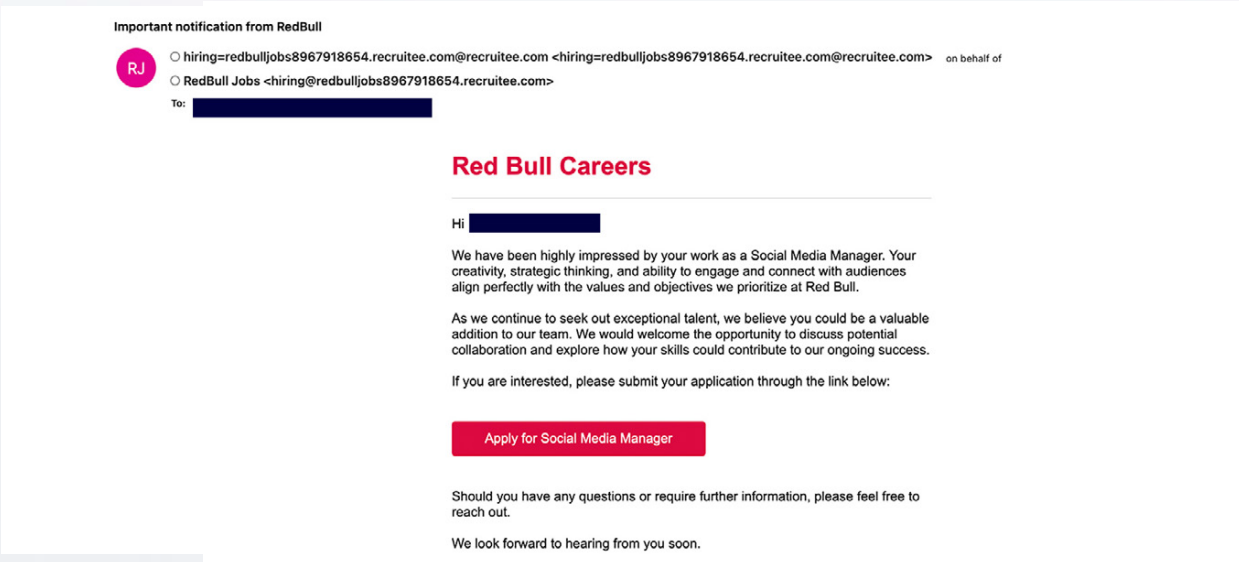
↓

Zur Vervollständigung der Anwendung sind MFA-Codes erforderlich

↓

Facebook-Anmeldedaten wurden über einen Telegram-Logger erlangt und weitergegeben

Eine kürzlich durchgeführte Phishing-Kampagne nutzte Recruitee, ein legitimes Drittanbieter-CMS für die Personalbeschaffung, um betrügerische E-Mails mit Jobangeboten zu versenden. Bedrohungsakteure registrieren Lookalike-Domains, um sich als bekannte Marken auszugeben und ihren betrügerischen Tätigkeiten Glaubwürdigkeit zu verleihen. Die Phishing-Seiten verwenden CAPTCHAs und IP-Filter, um eine automatisierte Erkennung zu verhindern, und zielen darauf ab, Facebook-Anmeldedaten zu erbeuten.



Important notification from RedBull

RJ hiring=redbulljobs8967918654.recruitee.com@recruitee.com <hiring=redbulljobs8967918654.recruitee.com@recruitee.com> on behalf of
RedBull Jobs <hiring@redbulljobs8967918654.recruitee.com>
To: [redacted]

Red Bull Careers

Hi [redacted]

We have been highly impressed by your work as a Social Media Manager. Your creativity, strategic thinking, and ability to engage and connect with audiences align perfectly with the values and objectives we prioritize at Red Bull.

As we continue to seek out exceptional talent, we believe you could be a valuable addition to our team. We would welcome the opportunity to discuss potential collaboration and explore how your skills could contribute to our ongoing success.

If you are interested, please submit your application through the link below:

Apply for Social Media Manager

Should you have any questions or require further information, please feel free to reach out.

We look forward to hearing from you soon.

04
.3

MIMECAST RISK RADAR.

ANGREIFER NUTZEN HÄUFIGER VERTRAUENSWÜRDIGE DIENSTE (LOTS)

Angreifer missbrauchen immer öfter seriöse Dienstanbieter, um gezielt reputations- und vertrauensbasierte Abwehrmaßnahmen zu umgehen. Für ihre Tätigkeiten nutzen sie legitime E-Mail-Anbieter, File-Sharing-Websites, Webinar-Hosting-Dienste und viele weitere vertrauenswürdige Angebote. Angriffe erfolgen häufig über große E-Mail-Dienste wie Google Gmail und Microsoft Outlook (früher Hotmail), während Links in E-Mail-Nachrichten oft auf einen legitimen Hosting-Dienst weiterleiten, wie Google Docs, Evernote oder die Microsoft-Dienste OneDrive und SharePoint.

Während die großen Anbieter legitimer Dienste nach Wegen suchen, um einen solchen Missbrauch zu verhindern, nehmen Angreifer nun auch kleinere Anbieter ins Visier. Bei Mimecast konnten wir beispielsweise große Kampagnen nachverfolgen, die Anbieter wie Airtable, Publuu und Wave Compliance nutzten.

GEOPOLITISCHE RISIKEN NEHMEN ZU

Angesichts weltweit steigender geopolitischer Spannungen verändert sich auch die Bedrohungslandschaft. Cyberangreifer sind aktiver geworden. Sie nutzen den Cyberbereich zur Informationssammlung, zur Kompromittierung der Assets konkurrierender Nationen sowie zur Einkommensgenerierung. Der scheinbare Mangel an handfesten Konsequenzen für Cyberoperationen hat einige Nationen dazu ermutigt, ihre Tätigkeiten noch auszuweiten. Und auch Cyberkriminelle führen immer dreistere Angriffe durch.

Auf der anderen Seite gelingt es Strafverfolgungsbehörden jedoch auch, die Infrastruktur von Cyberkriminellen zu stören. Und die Bemühungen der Verteidigungsspezialisten führen dazu, dass Angriffsziele nicht mehr so leicht zu hacken sind. Nach dem Einmarsch Russlands in die Ukraine nutzten beide Länder ihre Bestände an Zero-Day- und N-Day-Exploits, was zeitweise zu einem sprunghaften Anstieg von Angriffen führte (siehe Abbildung 1), der inzwischen jedoch wieder abgeklungen ist. Im Jahr 2024 blieb die Gesamtzahl der über den Known-Exploited-Vulnerability(KEV)-Katalog gemeldeten ausgenutzten Schwachstellen konstant, jedoch auf niedrigem Niveau.

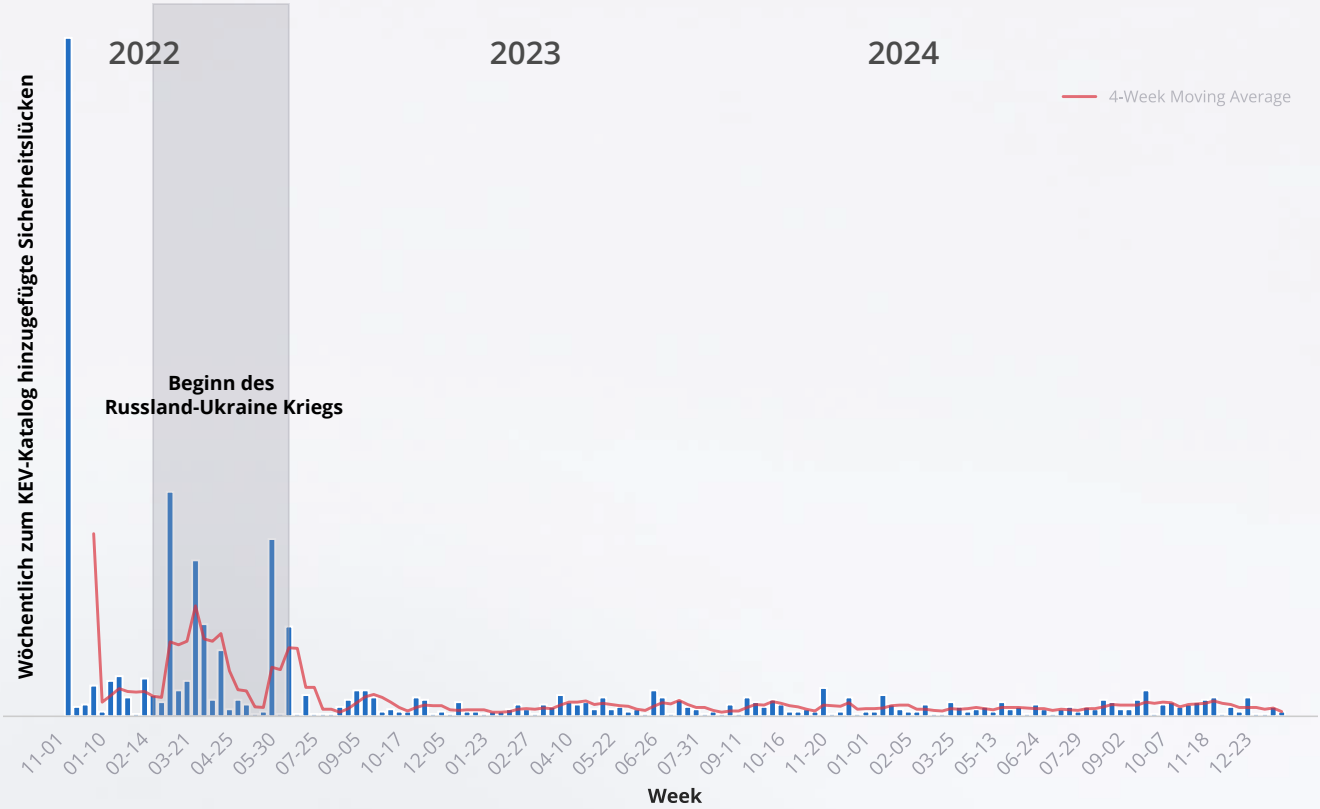


Abbildung 1: Die CISA (Cybersecurity and Infrastructure Security Agency) gibt an, dass sie dem KEV-Katalog zwischen Mitte 2022 und Ende 2024 etwa 4 Schwachstellen pro Woche hinzugefügt hat. Die Daten zeigen einen starken Anstieg bei der Erstveröffentlichung der Liste, sowie signifikante Aktivitäten in den ersten Monaten der russischen Invasion.

Das Niveau heutiger Cyberbedrohungen wurde angesichts unserer globalen geopolitischen Lage weiter angehoben. Zudem schaffen Ereignisse mit weltweiten Auswirkungen eine noch größere Vielfalt von Ködern für Bedrohungsakteure, die menschliche Schwächen ausnutzen möchten.

W 41°24'12.2 "
E 23°44'54.4 "
PE-3 NVGT B

Die wichtigsten geopolitischen Lockmittel, die von Mimecast beobachtet wurden:

01
CHINA–TAIWANCHINA-SOUTH

02
CHINA-SÜDCHINESISCHES MEER

03
CHINA-CUT-KABEL

04
RUSSLAND-UKRAINE-KRIEG

05
ISRAEL-GAZA-KONFLIKT

06
GESETZGEBUNG DER EUROPÄISCHEN UNION

07
RUSSLAND–US-WAHLEN

08
IRAN–US-WAHLEN

09
WETTEREREIGNISSE IN DEN USA

AM HÄUFIGSTEN ANGEGRIFFENE BRANCHEN

Die Branchen mit den größten Bedrohungsintensitäten umfassen „Kunst, Unterhaltung & Freizeit“ – mit mehr als 10 Bedrohungen pro Benutzer (BPB) –, sowie die Kategorien „Professional Services: Rechtsdienstleistungen“ und „Medien & Verlagswesen“, die fast 9 Bedrohungen pro Benutzer verzeichneten.

Die meisten Branchen wiesen ein für sie charakteristisches Bedrohungsprofil auf. Die Kategorie „Kunst, Unterhaltung & Freizeit“ verzeichnete einen weitaus höheren Anteil an Angriffen mit schädlichen Dateien, während die Mitarbeiter von Anwaltskanzleien eine beträchtliche Anzahl von Identitätsmissbrauchsangriffen erlebten. Mitarbeiter im Medien- und Verlagswesen wurden vor allem mit schädlichen Links angegriffen, während der Software- und SaaS-Sektor mit vielen Identitätsmissbrauchsangriffen zu kämpfen hatte.

Bei der Auswertung unserer Analysen entfernten wir die Daten zu Massen-E-Mails, die als Spam bzw. als E-Mails von Absendern mit niedriger Reputation erkannt wurden – diese machten jeweils 17 BPB und 5 BPB aus.

01	KUNST, UNTERHALTUNG & FREIZEIT	10.322010 BPB
02	RECHTSDIENSTLEISTUNGEN	8.613564 BPB
03	MEDIEN & VERLAGSWESEN	8.622578 BPB

ZEITLEISTE DER WICHTIGEN EREIGNISSE IN DER 2. JAHRESHÄLFTE.

04.2

JUL.

10 MILLIARDEN PASSWÖRTER GELEAKT

SEPT.

ASIATISCHE KRYPTOWÄHRUNGSBÖRSEN VON DIEBSTÄHLEN BETROFFEN

INTERNET ARCHIVE GEHACKT

OKT.

SALZ-TAIFUN SORGT FÜR WACHSENDE BESORGNIS

NOV.

IRANISCHE „FAKE-ARBEITER“ NEHMEN SENSIBLE BRANCHEN INS VISIER

DEZ.

US-FINANZMINISTERIUM ÜBER DRITTE GEHACKT

PHISHING VON ENTWICKLERN ERMÖGLICHT BROWSER-ERWEITERUNGSKOMPROMITTIERUNG

PPO-399. 3

JULI

10 MILLIARDEN PASSWÖRTER GELEAKT

SCHWACHSTELLE Geleakte Passwörter

AUSWIRKUNGEN Credential-Stuffing- und Brute-Force-Angriffe

RockYou2024 ist das größte Leak von Anmeldedaten aller Zeiten – mit 9.948.575.739 offengelegten eindeutigen Klartextpasswörtern. Diese riesige Datei, die in einem Hackerforum veröffentlicht wurde, ist deswegen so Besorgnis erregend, da die enthaltenen Passwörter über die letzten zwei Jahrzehnte hinweg gesammelt wurden, sodass viele Benutzer potenziellen Angriffen durch Credential-Stuffing und andere Sicherheitsbedrohungen ausgesetzt sind.

SEP.

ASIATISCHE KRYPTOWÄHRUNGSBÖRSEN VON DIEBSTÄHLEN BETROFFEN

SCHWACHSTELLE Netzwerkverletzungen
AUSWIRKUNGEN Mehr als 70 Millionen US-Dollar an Verlusten

Zwei Kryptowährungsbörsen – die in Singapur ansässige BingX und die indonesische Indodax – erlitten nach separaten Sicherheitsverletzungen massive Verluste. Indodax versprach, seine Nutzer für ihren Verlust von 22 Millionen US-Dollar zu entschädigen, während BingX einen Verlust von 44 Millionen US-Dollar in Kauf nehmen musste. In den USA gab das US-Justizministerium die Verhaftung von zwei Personen bekannt, nachdem einem US-Bürger Kryptowährungen im Wert von 230 Millionen US-Dollar gestohlen wurden.

HACKERANGRIFF AUF DAS INTERNET ARCHIV

SCHWACHSTELLE Unbekannt
AUSWIRKUNGEN Informationen zu 31 Millionen einzigartigen Konten offengelegt

Das Internet Archiv erlitt über einen Zeitraum von 22 Tagen gleich mehrere Sicherheitsverletzungen. Um den 28. September herum stahl ein Bedrohungsakteur die Datenbankdatei der Wayback Machine des Internet Archiv und konnte so Benutzernamen, E-Mail-Adressen und verschlüsselte Passwörter stehlen. Obwohl der Gründer der Website danach erklärte, dass die Systeme bereinigt und die Sicherheitsmaßnahmen verbessert wurden, erfolgten im Oktober mehrere Denial-of-Service-Angriffe und ein zweiter Sicherheitsvorfall.

OKT.

ZUNEHMENDE SORGEN UM SALT TYPHOON

SCHWACHSTELLE Infiltration der US-amerikanischen Telekommunikation
AUSWIRKUNGEN Chinesische Akteure erhalten umfangreichen Zugang zu Kommunikationssystemen

Die vom chinesischen Staat gesponserte Bedrohungsgruppe Salt Typhoon verschaffte sich Zugang zu hochsensiblen Informationen über US-Bürger und US-Regierungsbeamte, indem sie wichtige Telekommunikations- und Internetdienstanbieter in den USA kompromittierte (darunter Verizon und AT&T). Berichten zufolge sind bis zu neun verschiedene Anbieter betroffen, ebenso wie die gerichtlich genehmigte Abhörinfrastruktur einiger Anbieter, was als „Spionageabwehrversagen höchsten Ranges“ bezeichnet wurde.

NOV.

IRANISCHE „SCHEINARBEITER“ ZIELEN AUF SENSIBLE BRANCHEN AB

SCHWACHSTELLE Social-Engineering, LinkedIn-Missbrauch

AUSWIRKUNGEN Luftfahrt-, Raumfahrt- und Verteidigungsindustrien in Israel und den Vereinigten Arabischen Emiraten; auch die Türkei, Indien und Albanien sind mögliche Ziele

Mutmaßliche iranische Hacker nutzten gefälschte Rekrutierungswebsites, um sich als Personalvermittler auf LinkedIn auszugeben und Kontakt zu Raumfahrt-, Verteidigungs- und Luftfahrtunternehmen in Israel, den VAE, der Türkei, Indien und Albanien aufzunehmen. Hacker geben sich seit 2023 auf LinkedIn als Personalvermittler aus, um über gefälschte lukrative Jobangebote Malware an Opfer zu verteilen und dadurch verschiedene Ziele auszuspionieren und sensible Daten zu stehlen. Diese Malware und die Taktiken ähneln denen einer nordkoreanischen Hackergruppe, die es auf börsengehandelte Kryptowährungsfonds abgesehen hatte.

DEZ.

US-FINANZMINISTERIUM ÜBER DRITTANBIETER GEHACKT

SCHWACHSTELLE Drittanbieter; kritische Rolle von Sicherheitssoftware

AUSWIRKUNGEN Angreifer erhielten über einige Workstations Zugriff auf nicht klassifizierte Daten

Das US-Finanzministerium gab bekannt, dass sich ein Sicherheitsvorfall beim Identitätssicherheitsanbieter BeyondTrust auf die Systeme des Ministeriums ausgeweitet hatte. Dies führte zur Kompromittierung mehrerer Workstations und der Offenlegung nicht klassifizierter Daten. Obwohl die Ermittlungen noch andauern, zeigen die Vereinigten Staaten den Finger auf eine vom chinesischen Staat gesponserte Hackergruppe, die sich Berichten zufolge Zugang zu einem API-Schlüssel für den Fernsupport verschafft hatte. BeyondTrust hat bislang noch nicht bekannt gegeben, wie die Angreifer Zugang zu diesem kritischen Schlüssel erlangten.

PHISHING-ANGRIFFE AUF ENTWICKLER ERMÖGLICHEN KOMPROMITTIERUNG VON BROWSER-ERWEITERUNGEN

SCHWACHSTELLE Spear-Phishing-Angriff verleiht Chrome-Erweiterungen umfangreiche Berechtigungen

AUSWIRKUNGEN Schädliche Erweiterungen sammeln Anmeldedaten und Informationen von Endbenutzern

Bedrohungsgruppen haben im vergangenen Jahr mehr als 30 Browser-Erweiterungen kompromittiert, indem sie Spear-Phishing-E-Mails, die angeblich von Google stammten, an die Kontaktperson oder -gruppe der angezielten Chrome-Browser-Erweiterung schickten. In diesen E-Mails werden Entwickler gebeten, einer harmlos erscheinenden Anwendung Rechte zu gewähren. Tatsächlich geben sie damit jedoch Angreifern die Möglichkeit, die echte Erweiterung durch eine schädliche Anwendung zu ersetzen. Das Datensicherheitsunternehmen Cyberhaven berichtete erstmals im Dezember über diese Taktik, nachdem einer seiner eigenen Entwickler dem Angriff zum Opfer gefallen war und der Anwendung „Privacy Policy Extension“ (Erweiterung für Datenschutzrichtlinie) Berechtigungen erteilt hatte. Schätzungsweise 2,6 Millionen Benutzer könnten von dem Angriff betroffen sein.

EMPFEHLUNGEN.

05

BEDROHUNGSSPEZIFISCHE GEGENMASSNAHMEN

BEST PRACTICES & WARNUNGEN

EMPFEHLUNGEN FÜR MIMECAST KUNDEN

A5

CROW

SPEZIES

Sie sind bekannt für ihre Fähigkeit, Wissen zu vermitteln und Probleme zu lösen. Allzeit dazu bereit, in **Aktion** zu treten, sind sie Ihre erste Anlaufstelle für Strategien zur Minderung von Cybersecurity-Risiken.

BEDROHUNGSSPEZIFISCHE GEGENMASSNAHMEN.

05.1

Organisationen sollten konkrete Maßnahmen ergreifen, um ihre Abwehr zu verbessern und den Kostenaufwand von Angreifern zu erhöhen.

HUMAN RISK MANAGEMENT

Um Human Risk in einer Organisation effektiv zu handhaben, sollte ein Rahmenwerk eingeführt werden, das die Sicherheitsziele mit den Geschäftszielen in Einklang bringt. Wenn Organisationen sich bewusst machen, wie menschliche Risikofaktoren zu potenziell negativen Ergebnissen führen, können sie ein mehrstufiges Reaktionssystem entwickeln, das zwischen unbeabsichtigten Fehlern und böswilligen Handlungen unterscheidet. Die Hauptbedenken sind der Verlust von geistigem Eigentum oder anderen wettbewerbsrelevanten Informationen, die Exfiltration sensibler Daten und der Missbrauch von Unternehmensressourcen.

Organisationen sollten sowohl positive Verstärkungsmaßnahmen („Nudges“) als auch korrigierende Gegenmaßnahmen in einem phasenweisen Ansatz integrieren. Um diese Maßnahmen erfolgreich umzusetzen, ist es entscheidend, funktionsübergreifende Arbeitsgruppen zu etablieren, um die Zustimmung der Stakeholder und ein effektives Change-Management sicherzustellen. Gleichzeitig sollten klare Kommunikationskanäle zur Führungsebene bestehen, um über Risikometriken, potenzielle Vorfälle und Strategien zur Schadensbegrenzung zu informieren.

BIETEN SIE SENSIBILISIERUNGSSCHULUNGEN AN

Angesichts einer komplexen Bedrohungslandschaft, in der sich geopolitische Spannungen häufig als Cyberbedrohungen manifestieren, werden umfassende Sensibilisierungsschulungen unerlässlich. Mitarbeiter müssen nicht nur über allgemeine Cyberrisiken aufgeklärt werden, sondern auch darüber, wie globale Ereignisse Phishing-Kampagnen, Insider-Bedrohungen und Social-Engineering-Versuche beeinflussen können, die auf ihre Organisation abzielen. Durch die Implementierung effektiver Schulungsprogramme zur Sensibilisierung der Belegschaft sowie Plattformen zur Absicherung von Benutzern können Organisationen ihre menschliche Firewall sowohl gegen konventionelle Cyberangriffe als auch gegen

solche mit geopolitischen Motiven stärken. Dieser am Menschen orientierte Sicherheitsansatz hilft Mitarbeitenden dabei, Bedrohungen zuverlässig zu identifizieren und effektiv darauf zu reagieren, unabhängig davon, ob Angriffe per E-Mail, über soziale Medien, Tools für die Zusammenarbeit oder andere Vektoren erfolgen, bei denen die menschliche Psychologie ausgenutzt wird.

VERLANGEN SIE MEHR SICHERHEIT VON DRITTANBIETERN

Angriffe auf Unternehmen in den Bereichen Fertigung, Transport, Lagerung und Auslieferung sowie im Einzelhandel und Großhandel stellen ein erhebliches Risiko für die Kompromittierung der Lieferkette durch Dritte dar. Unternehmen sollten ihre Service-Level-Agreements überprüfen, um Mindeststandards für die Daten- und Cybersicherheit festzulegen. Zudem sollten sie nach Möglichkeiten suchen, ihre Lieferanten enger zu überwachen, etwa durch die Nutzung externer Ratingdienste oder durch eine genauere Prüfung von Akquisitionen.

SCANNEN SIE IHRE UMGEBUNG AUF FEHLKONFIGURATIONEN ODER EXTERNE GEÖFFNETE PORTS

Unternehmen sollten ihre Infrastruktur regelmäßig auf bekannte ausnutzbare Schwachstellen überprüfen, z. B. unsichere offene externe Netzwerkports oder öffentliche Cloud-Umgebungen. Mit Tools wie Cloud Security Posture Management können Unternehmen Fehlkonfigurationen in ihrer öffentlichen Cloud schnell identifizieren. Dadurch wird sichergestellt, dass alle öffentlich zugänglichen Server-Ports geschlossen oder angemessen gesichert und geschützt sind.

Als Beispiel hat Mimecast eine anhaltende Zunahme von Angriffen auf Remote Desktop Protocol (RDP)-Ports festgestellt, auf die 80 % der effektiven Ransomware-Angriffe entfallen. Angreifer werden weiterhin nach offenen RDP-Ports suchen, um Organisationen anzugreifen.

BILDER IN E-MAIL-NACHRICHTEN BLOCKIEREN

Angreifer nutzen immer häufiger bildbasierte Dateitypen, um Phishing-Köder und schädlichen Code in Zielunternehmen einzuschleusen, ohne die jeweiligen Erkennungsmechanismen zu triggern. Unsere Analysen haben zudem ergeben, dass Bedrohungsakteure zu diesem Zweck auch Verschlüsselungstaktiken und fremdsprachigen Text in Bildern verwenden. Unternehmen sollten ihre E-Mail-Clients so konfigurieren, dass sie das Laden von Bildern in Nachrichten verhindern und Bilder, die von Benutzern explizit markiert wurden, isolieren.

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

SEGMENTIEREN SIE DAS NETZWERK UND PROTOKOLLIEREN SIE DEN INTERNEN DATENVERKEHR

Angreifer können sich, insbesondere während eines Ransomware-Angriffs, schnell lateral durch ein Netzwerk bewegen. Die Segmentierung des internen Netzwerks und die Unterbringung kritischer Ressourcen in eigenen Enklaven kann den durch Ransomware und andere Angriffe verursachten Schaden verringern. Die Überwachung des internen Datenverkehrs, insbesondere die Segmentierung der Kommunikation, kann zu einer früheren Erkennung von Bedrohungen führen.

NUTZEN SIE SOLIDE MECHANISMEN FÜR BENUTZERANMELDEINFORMATIONEN UND IMPLEMENTIEREN SIE MFA

Bei Malware-Bedrohungen werden häufig gängige Passwörter ausgenutzt, um in Netzwerke einzudringen. Aktuelle Angriffe zeigen, wie schwache Passwörter zu Sicherheitsverletzungen beitragen. Stärken Sie jedes Netzwerk, indem Sie Richtlinien zu sicheren Passwörtern durchsetzen, insbesondere für Benutzer mit umfangreichen Zugriffsberechtigungen. Die IT-Sicherheit muss standardmäßige Administratorkennwörter abschaffen. Das Erfordernis einer mehrstufigen Authentifizierung kann die Kompromittierung gestohlener Konten oder Anmeldeinformationen drastisch reduzieren.

05.2 BEST PRACTICES UND WARNUNGEN.

WARNUNGEN ZU APT40: DAS MSS IN AKTION

8. Juli 2024 Mehr erfahren >

Organisationen: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK, BND und andere

Die für die Cybersicherheit und Strafverfolgung zuständigen Regierungsbehörden in Australien, Kanada, Neuseeland, Deutschland, Südkorea, dem Vereinigten Königreich und den Vereinigten Staaten haben die Taktiken des vom chinesischen Staat gesponserten Bedrohungsakteurs APT40 (auch bekannt als Gingham Typhoon) dargelegt, der „wiederholt australische Netzwerke sowie Netzwerke der Regierung und des privaten Sektors in der Region ins Visier genommen hat“. Die Gruppe kann den Proof-of-Concept-Code für neue Schwachstellen schnell anpassen, ausnutzen und in Angriffe umwandeln, um diese Tools in Kampagnen einzusetzen.

ERKENNUNG UND BESCHRÄNKUNG VON ACTIVE DIRECTORY-KOMPROMITTIERUNGEN

September 2024 Mehr erfahren >

Organisationen: ASD, CISA, NSA, CCCS, NCSC-NZ, NCSC-UK

Die Cybersicherheitsbehörden der Five-Eyes-Staaten beschreiben 17 verschiedene Techniken für Angriffe auf Microsoft Active Directory, die am häufigsten verwendete Identitäts- und Zugriffslösung in Unternehmen. Da Active Directory eine zentrale Rolle bei der Authentifizierung und Autorisierung spielt und gleichzeitig aufgrund von Standardeinstellungen und der Komplexität der Installation anfällig für Kompromittierungen ist, zielen böswillige Akteure häufig darauf ab.

RUSSISCHE MILITÄR-CYBERAKTEURE ZIELEN AUF KRITISCHE INFRASTRUKTUREN IN DEN USA UND WELTWEIT

5. September 2024 Mehr erfahren >

Organisationen: CISA, FBI, NSA

Mehrere russische Bedrohungsgruppen, die mit militärischen Einrichtungen in Verbindung stehen, griffen ukrainische Regierungsbehörden und andere Ziele von NATO-Verbündeten mit der zerstörerischen WhisperGate-Malware an. Die Angreifer nutzen typischerweise Schwachstellen in Netzwerkgeräten aus, um sich Zugriff darauf zu verschaffen.

DIE AM HÄUFIGSTEN AUSGENUTZTEN SCHWACHSTELLEN 2023

12. November 2024 Mehr erfahren >

Organisationen: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK

Vielleicht etwas verspätet haben die führenden Behörden der Five-Eyes-Staaten (Australien, Kanada, Neuseeland, das Vereinigte Königreich und die Vereinigten Staaten) Informationen über die 15 am häufigsten ausgenutzten Schwachstellen des Jahres 2023 veröffentlicht. Elf der 15 Schwachstellen wurden in Zero-Day-Angriffen ausgenutzt, verglichen mit nur zwei Zero-Day-Angriffen für die zwölf Schwachstellen, die 2022 auf der Liste standen.

VERBESSERUNG DER CYBER-RESILIENCE: DAS RED TEAM VON CISA TEILT SEINE BEWERTUNG EINER US-ORGANISATION AUS DEM SEKTOR DER KRITISCHEN INFRASTRUKTUR

21. November 2024 Mehr erfahren >

Organisationen: CISA

Die Cybersecurity and Infrastructure Security Agency (CISA) identifizierte während einer Red-Team-Evaluierung erhebliche Schwachstellen in den Cybersicherheitsmaßnahmen einer Organisation aus dem Bereich der kritischen Infrastruktur. Das Team drang über eine Web-Shell in die Organisation ein, die noch von einer früheren Evaluierung übrig geblieben war. Danach konnte das Red Team aufgrund unzureichender Netzwerkschutzmaßnahmen und einer langsamen Abwehr die Domain sowie sensible Systeme kompromittieren.

MIT DER ISLAMISCHEN REVOLUTIONSGARDE VERBUNDENE CYBERAKTEURE NUTZEN SPS IN MEHREREN SEKTOREN, EINSCHLIESSLICH US-EINRICHTUNGEN FÜR WASSER- UND ABWASSERSYSTEME

18. Dezember 2024 Mehr erfahren >

Organisationen: FBI, CISA, NSA, US EPA, INCD, CCCS, NCSC

Die Cybersicherheitsbehörden der USA, Israels, Kanadas und des Vereinigten Königreichs haben eine aktualisierte Warnung herausgegeben. Darin werden schädliche Cyberaktivitäten von Akteuren beschrieben, die mit dem Korps der Islamischen Revolutionsgarde (IRGC) verbunden sind, einschließlich Angriffen auf speicherprogrammierbare Steuerungen (SPS) und kritische Infrastrukturen im Vereinigten Königreich und in Israel.

SPEZIFISCHE EMPFEHLUNGEN FÜR MIMECAST-KUNDEN.

Mimecast-Benutzer können konkrete, praxistaugliche Schritte umsetzen, um ihre Benutzer vor den im Bericht beschriebenen Bedrohungen zu schützen (unter Beachtung mittelschwerer technischer Anweisungen).

CLOUD-GATEWAY FÜR E-MAIL-SICHERHEIT

1. Es wird empfohlen, eine Single Sign-on-Lösung zur Anmeldung bei Ihrem Identitätsanbieterzu verwenden oder die in Mimecast eingebaute Multi-Faktor-Authentifizierung zu nutzen, um die Möglichkeiten eines Angreifers zu verringern, E-Mails als Angriffsvektor zu nutzen.
2. Stellen Sie sicher, dass DNS-Authentifizierungsrichtlinien DMARC-Einträge berücksichtigen. Eine zweite Richtlinie, die auf eine Richtliniengruppe mit der DMARC-Fehleraktion „Ignorieren/Verwaltete und zulässige Absender" festgelegt ist, bietet eine effektive Umgehung für alle legitimen E-Mails, die aufgrund von DMARC-Fehlern abgelehnt/unter Quarantäne gestellt werden.
3. Optimieren Sie den Schutz vor Identitätsbetrug gemäß den Best Practice-Richtlinien von zwei Treffern Setzen Sie die Markierung „Betreff/Text" und schließen Sie eine separate C-Level/VIP-Richtlinie basierend auf Namensübereinstimmung mit einer Sperre zur Überprüfung durch den Administrator ein. Erstellen Sie außerdem eine weitere Richtlinie für alle Erkennungen von drei oder mehr Treffern mit der Sperre durch den Administrator.
4. Ergreifen Sie erweiterte Abwehrmaßnahmen gegen BEC anhand von drei Richtlinien: Moderate Durchsetzung bei der Bedrohungserkennung, Absenderumgehung für vertrauenswürdige Quellen und Empfängerumgehung für interne Ausschlüsse.
5. Das Einrichten eines umfassenden URL Rewriting stellt sicher, dass alle URLs beim Klicken gescannt werden. Seien Sie sich jedoch bewusst, dass das Rewriting alle Elemente umfasst, die einer URL ähneln, z. B. IP-Adressen und interne Links.
6. Nutzen Sie vorgefertigte Integrationen, die mit den meisten SIEM- und XDR-Anbietern kompatibel sind, um Protokollierung und Analyse zur Durchsetzung von Sicherheitsrichtlinien bereitzustellen.
7. Nutzen Sie Ihre eigenen Bedrohungsdaten, um alle Bedrohungsdaten von Drittanbietern für die automatische Zurückweisung von übereinstimmenden Indikatoren zu nutzen.
8. Endbenutzer sollten dem Mimecast SOC potenziell gefährliche Nachrichten über Mimecast-Benutzertools zur weiteren Analyse melden.

CLOUD INTEGRATED

1. Aktivieren Sie die Browser-Isolierung, um das Risiko zu minimieren, dass Benutzer potenziell verdächtige Websites besuchen.
2. Passen Sie Ihre Zulassungs- und Blockierungsregeln genau an, um festzulegen, wer auf Ihre Umgebung zugreifen darf und wer nicht.
3. Sehen Sie sich wöchentliche Berichte an, um Einblicke in die Bedrohungen zu erhalten, die in Ihrer Umgebung erkannt wurden.
4. Endbenutzer sollten dem Mimecast SOC potenziell gefährliche Nachrichten über Mimecast-Benutzertools zur weiteren Analyse melden.

Wenn Sie sich hinsichtlich der Auswirkungen der vorgeschlagenen Einstellungen nicht sicher sind, wenden Sie sich bitte an Ihren Mimecast-Kundenbetreuer bzw. Ihren Customer Success Manager oder loggen Sie einen Anruf beim Mimecast-Support.

FAZIT.

In der zweiten Hälfte des Jahres 2024 zeigten Bedrohungsanalysen eine Intensivierung ausgeklügelter Desinformationskampagnen und koordinierter Hacktivismus-Operationen. Diese gingen einher mit eskalierenden geopolitischen Spannungen, die es den Bedrohungsakteuren ermöglichten, globale Ereignisse für gezielte Angriffe zu instrumentalisieren. Ihre fortschrittlichen Taktiken umfassen nun die systematische Datenexfiltration, den gezielten Einsatz von Ransomware, orchestrierte DDoS-Angriffe sowie die Ausnutzung menschlicher Schwachstellen durch ausgeklügelte Social-Engineering-Kampagnen, die sich auf bedeutende geopolitische Entwicklungen konzentrieren. Zusammengenommen stellen diese Taktiken erhebliche Risiken für die Geschäftskontinuität und Systemverfügbarkeit dar.

Die Identifizierung gefährlicher Aktivitäten ist heute technisch äußerst komplex geworden, da Angreifer schädliche Handlungen mit legitimen Operationen vermischen, einschließlich der Ausnutzung vertrauenswürdiger Dienste und gängiger System-Binärdateien. Bedrohungsakteure nutzen zunehmend legitime Red-Team-Tools, was es den Sicherheitskontrollen erheblich erschwert, zwischen autorisierten und nicht autorisierten Aktivitäten zu unterscheiden. Dies erfordert verbesserte Überwachungsfunktionen, einschließlich fortschrittlicher Verhaltensanalysen und Anomalieerkennungssystemen.

In anderen Bereichen der Bedrohungslandschaft weisen Social-Engineering-Angriffe weiterhin hohe Erfolgsquoten auf. Sie werden durch die Integration automatisierter KI-Technologien immer raffinierter. Advanced Persistent Threats nutzen heute ausgeklügelte Deepfake-Technologien und KI-generierte Inhalte für gezielte Angriffe aus, was den Einsatz traditioneller Erkennungs- und Präventionsmechanismen erheblich erschwert. Die technische Raffinesse dieser Angriffe verrät, dass dahinter eine komplexe Social-Engineering-Forschung und Analyse der Kommunikationsmuster in der Lieferkette steckt.

Die Sicherheit am Perimeter bleibt ein kritisches Anliegen, da Bedrohungsakteure kontinuierlich Schwachstellen in der Edge-Infrastruktur ausnutzen – darunter VPN-Anwendungen, Firewalls und internetgestützter Dienste. Zero-Day-Exploits in Verbindung mit einer verzögerten Umsetzung von Patches

schaffen verlängerte Fenster der Verwundbarkeit, insbesondere in Hochverfügbarkeitsumgebungen, die umfangreiche Patch-Tests erfordern. Diese Herausforderung wird durch komplexe Netzwerkarchitekturen und wachsende Angriffsflächen verstärkt, die durch die Migration zu Cloud-Infrastrukturen und die Weiterentwicklung von Betriebstechnologien bedingt sind. Organisationen benötigen spezielle Fähigkeiten zur Vorfallreaktion, einschließlich fortschrittlicher forensischer Werkzeuge, Netzwerkanalysesysteme und automatisierter Erkennungsmechanismen.

Sicherheitslücken, die dieses Jahr wahrscheinlich ausgenutzt werden:

VPN

Zu sehen in der kürzlichen Ergänzung des CISA-Katalogs der bekannten ausnutzbaren Schwachstellen um CVE 2025 0282 (bzgl. des Ivanti Connect Secure VPN)

AUTHENTIFIZIERUNG

Zuletzt beobachtet bei Sicherheitslücken, bei denen Umgehungen über einen alternativen Pfad oder Kanal ohne Authentifizierungscode ausgenutzt werden

DENIAL-OF-SERVICE (DOS)

Eine immer beliebter werdende bösartige Aktivität, die darauf abzielt, den Geschäftsbetrieb zu stören, z. B. CVE-2024-3393 PAN-OS-Firewall-Dienstverweigerung (DoS)

RESSOURCEN:

Webinar
Translating Threat Intelligence into Practical Security Strategies

Forschungsbericht
Stand der E-Mail- und Kollaborationssicherheit

TI HUB.

Mimecast TI Hub

Community.

Mimecast central

mimecast