mimecast

RISK RADAR

DETECTION | ANALYSIS | ACTION

GLOBAL THREAT INTELLIGENCE REPORT

JULY - DECEMBER 2024

CONTENTS.

INTRODUCTION.

01

Strong threat intelligence has become critical for companies and organizations to defend against attackers' increasing agility. Organizations of every size should educate themselves on the latest trends, track the threats targeting their industry and suppliers, and harden defenses and update their processes to prevent their business communications and people from being used against them.

In the second half of 2024, Mimecast processed more than 90- billion data points for its over 42,000 customers, flagging more than 5- billion threats during the six-month period. The total number of protected interactions greatly exceeded that by many multiples. Email and collaboration tools continue to be the channels through which most attackers start their effort to compromise targeted organizations, allowing Mimecast to detect and analyze many threats before they become widely known.

In the second half of 2024, Mimecast processed more than 90- billion data points for its nearly 43,000 customers, flagging more than 5- billion threats during the six-month period.

In our H2 2024 Global Threat Intelligence report, Mimecast has accumulated data from our systems protecting tens of millions of users, provided insights from our intelligence analysts, and added open-source intelligence on the latest threats. The report includes analysis of threat activity, statistics revealing attack trends, and a series of recommendations for small businesses and large enterprises to protect their employees and mitigate the impact of risky users.

We invite you to explore our H2 2024 threat intelligence report and look forward to sharing more insights in the future.

EXECUTIVE SUMMARY.

IN THE SECOND HALF OF 2024, THREAT ACTORS INCREASINGLY USED LEGITIMATE SERVICES AS A WAY TO OBSCURE THEIR ATTACKS AND ATTEMPT TO EVADE DEFENSES.

The trend of living off trusted services (LOTS) means that businesses will have to rely on more than just reputation and authentication systems to protect themselves from messaging and human-centered attacks. In addition, threat actors are exploiting third-party suppliers — whether a service provider or a software product — to more easily slip into a targeted network.

02

GEOPOLITICS HAVE GIVEN THREAT ACTORS BOTH MOTIVE FOR MORE FREQUENT ATTEMPTED COMPROMISES AND A FERTILE SUPPLY OF SUBJECT MATTER WITH WHICH TO CRAFT ATTACKS.

Nation-state actors continued to resort to cyberattacks and cyber -espionage to pursue deniable actions against their rivals. China compromised US and Canadian[1] infrastructure, Iran and Israel each targeted the other nation's infrastructure[2], and Russia continued to target European and US organizations[3] after its invasion of Ukraine stalled.

1. Tunney, Catharine. "China 'compromised' Canadian government networks and stole valuable info: spy agency." CBC. 30 October 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. News article. 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. News article. 3 October 2024. https://www.darkreading.com/cyberattacks-data-breaches/ukraine-russia-cyber-battles-tip-over-into-real-world

AI TECHNOLOGIES CONTINUE TO OFFER UNIQUE BENEFITS TO BOTH DEFENDERS AND ATTACKERS.

Cybersecurity analysts can more quickly analyze potential security events with the help of AI assistants, while incident responders can use AI to block and remediate an attack more quickly and completely. Attackers are benefiting as well: Mimecast research[4] using linguistic analysis found that about 12% of emails — including phishing attacks — showed signs of being written by large language models (LLM). Deepfake audio and video have been effectively used to imitate CEOs and instruct employees to make fraudulent payments into cybercriminal accounts.

ALL THESE TRENDS WILL CONTINUE IN 2025.

The number of attacks that used the cloud to some degree more than doubled in 2024, while geopolitics continues to become more chaotic with France and Germany both facing elections in Europe, U.S. President Donald Trump seated for a second, non-consecutive term, and Russia and China continuing to flex their militaries on the world stage. Both security researchers and attackers are pioneering new ways to exploit AI systems, either taking advantage of security weaknesses or augmenting their own attack strategies.

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/.

KEY FINDINGS.

While threat actor activity has increased across almost all metrics, some trends stand out.

03

OCTO

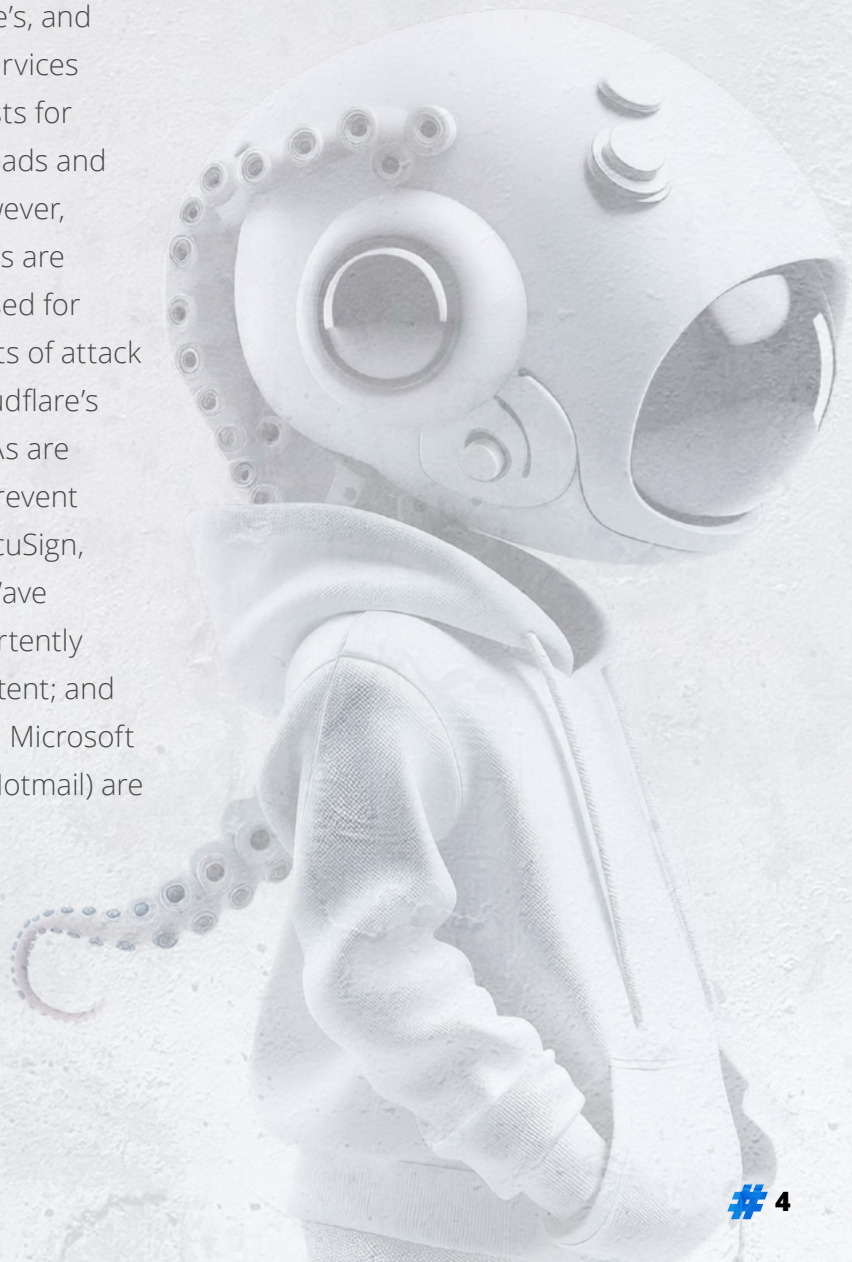
SPECIES

Masters of **analysis** with highly developed nervous system and large brain. They excel in adapting to their environment and overcoming challenges, making them a standout in threat intelligence.

K-1 ONE

ATTACKERS ARE INCREASINGLY LIVING OFF TRUSTED SERVICES (LOTS).

Microsoft's, Google's, and Evernote's cloud services commonly play hosts for threat actors' payloads and landing pages. However, other cloud services are frequently being used for specific components of attack infrastructure: Cloudflare's Turnstyle CAPTCHAs are regularly used to prevent threat analysis; DocuSign, TeamViewer, and Wave Compliance inadvertently host attackers' content; and Google's Gmail and Microsoft Outlook (formally Hotmail) are used to send phishing attacks.



K-2 TWO

GEOPOLITICS RAISES THE LIKELIHOOD OF CYBERATTACKS.

The French and German elections, and the continued uncertainty of the Russia-Ukraine war, will raise the tension of European Union politics. The departure of U.S. government from predictable norms could also result in greater activity in the cyber domain. Business, political, and cybersecurity experts have increasingly warned that geopolitical tensions and cybersecurity risks are linked. The top two risks identified for 2025 in the annual Systemic Risk Barometer Survey conducted by the Depository Trust and Clearing Corporation were Geopolitical Risk and Cyber Risk.[5]

K-3 TWO

KEY EMAIL AUTHENTICATION TECHNOLOGIES HAVE INCREASED CHALLENGES FOR ATTACKERS, WHILE AI HAS LOWERED THE BAR FOR CYBERCRIME.

By using trusted services, attackers can meet the increasing authentication requirements of email technologies — such as SPF, DKIM, and DMARC — and appear to come from a trusted source. While the technologies make their attacks more complicated, the attackers continue to find services to pass authentication and alignment checks. In addition, the spread of AI chat bots allows even would-be cybercriminals to gain the skills necessary for hacking.

5. "Geopolitical and Cyber Risks Remain Top Threats to the Financial Services Sector in 2025." DTCC. 4 December 2024. 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

MEDIA & PUBLISHING, ENTERTAINMENT & RECREATION, LEGAL SERVICES, AND THE ARTS INDUSTRIES SAW THE MOST THREATS PER USER IN H2 2024.

Most industries saw a distinctive threat profile, including a greater proportion of malicious files targeting the Arts, Entertainment & Recreation sectors, while workers in the Media & Publishing sector encountered larger number of malicious links. Impersonation attacks dominated the threat profile for the software & SaaS sector.

K-5 FIVE

HUMANS CONTINUE TO HAVE A PRIMARY ROLE IN MOST BREACHES.

Most breaches are enabled by an insider taking an action that allows attackers access to sensitive or protected resources. The 2024 version of the annual Data Breach Investigations Report (DBIR) found that more than two-thirds (68%) of breaches that occurred in 2023[6] had "a non-malicious human element." A 2024 survey of 1,000 employees found that a third (34%) worried that they would be the vulnerability exploited by attackers, even though the vast majority (86%) considered themselves knowledgeable about cybersecurity[7]. More than half of respondents fear they would lose their job if they left their organization open to a cyberattack.

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

THE THREAT LANDSCAPE

- IN CHARTS
- TOP THREATS & CAMPAIGNS
- MIMECAST RISK RADAR
- MAJOR EVENT TIMELINE

BAT

SPECIES

Detecting threats is their craft. Using echolocation, they emit high-frequency sounds that bounce off objects, giving them a detailed map of their surroundings. This helps them avoid obstacles, even in complete darkness.

04
.1

THE THREAT LANDSCAPE IN CHARTS.

The threat landscape in the second half of 2024 showed increasing use of consumer and business cloud services as a way for attackers to avoid detection. As a result, several major cloud services are being used to host attackers' content, and links continue to grow as a mechanism for delivering payloads.

In the second half of 2024, attackers shifted to focus on Arts, Entertainment & Recreation, Legal Services, and Software & SaaS sectors, a shift from the first half of 2024, when the Banking, Travel & Hospitality, and Arts & Entertainment industries topped the list of targets. While every industry encountered a significant number of bulk email attacks from low reputation sources, attackers targeted the Arts & Entertainment sector with more attacks using malicious files, and Legal Services encountered more attacks using impersonation.

Read on to explore how Mimecast data analysis illustrates the threat landscape.

CLOUD SERVICE ABUSE
#01

Attackers are increasingly living off trusted services (LOTS) in their efforts to bypass defenses that rely on identifying attacks by spotting untrusted code, resources, and online services. While some choices to host attackers' infrastructure are obvious — such as Google Docs, Evernote, and Dropbox DocSend — other online services are less well-known, such as interactive publication site Publuu, online webinar host Wave Compliance, and slide-deck presentation site Gamma.

Attackers also used specific platforms to send phishing emails and different sites to host the payload, which is often just a web form or file with a link. All-in-one marketing site GetResponse, for example, was a significant source of phishing emails — although many of those may not be malicious, just unwanted. While Adobe sites are not top hosts of payloads, at least two sites are used by attackers to host initial landing pages used by attackers.

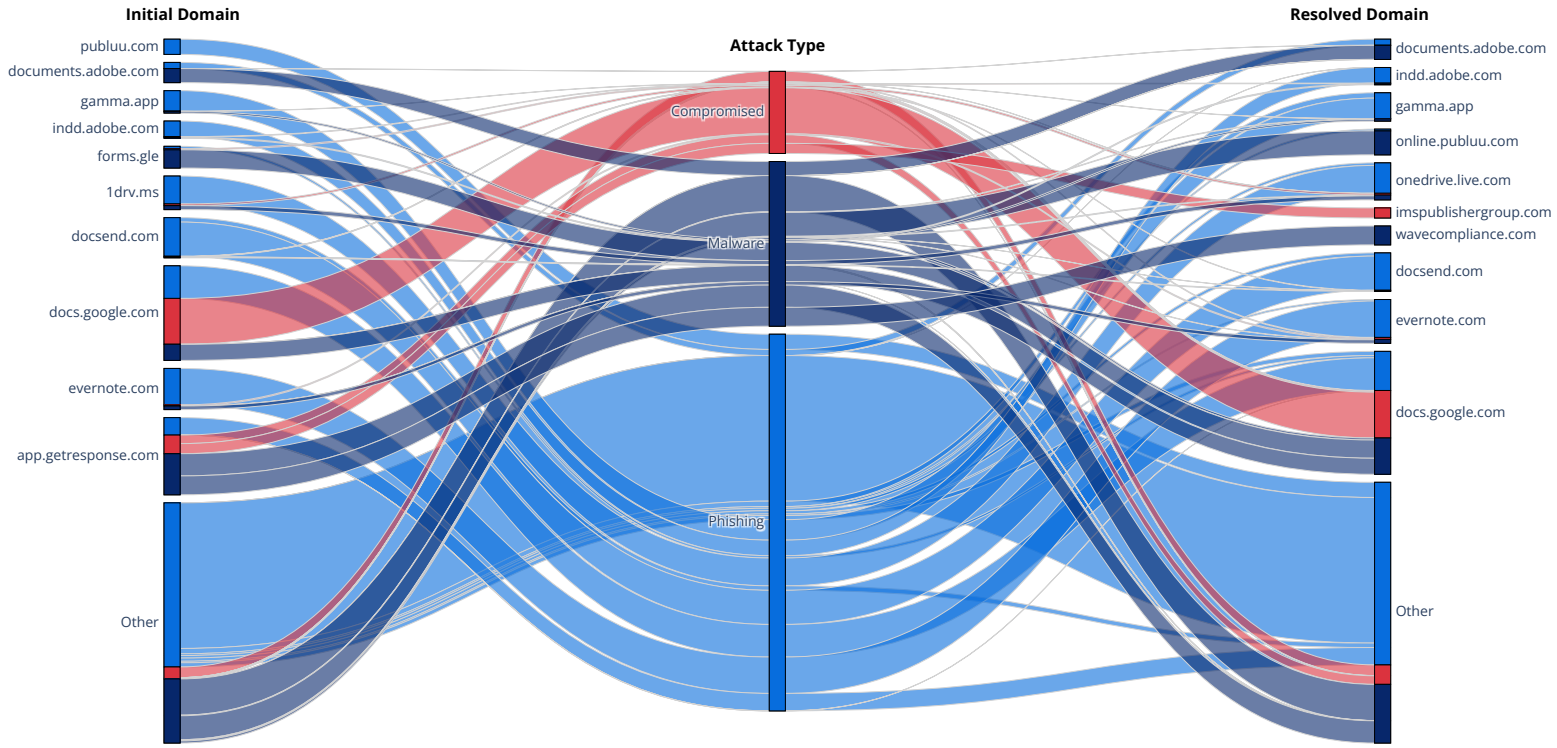


Chart 1: Most initial domains map to similar final domains, such as most attacks using Evernote initially, also hosting a payload there. Yet, there are a number of standouts, where one platform hosts the initial redirect page — such as a large volume of spam coming from marketing service GetResponse.com — and a second platform hosting the landing page, such as the training and webinar service Wave Compliance.

TPUS BY ATTACK TYPE

#02

While spam continues to account for the vast majority of messages blocked by Mimecast in H2 2024, the summer saw a surge in Unwanted email messages. While that surge abated by the end of the year, phishing attacks, which typically include a URL to an attacker-controlled site or service, saw slow growth through the half.

Mimecast classifies malicious and unwanted activity by the stage at which detection occurs.

SPAM catches mass emails from non-trusted domains and those containing widely encountered content.

SUSPICIOUS MESSAGES are potentially malicious messages, files or URLs; harmful content has not been detected, but indicators demonstrate the message should be treated with caution, such as if the message originates from a commonly abused service or a source with a low reputation.

UNWANTED includes messages blocked by the user.

PHISHING are threats designed to trick victims into revealing sensitive information, such as credentials or payment information. This inlcudesincludes phishing links, BEC, impersonation, or html attachments designed to impersinateimpersonate login pages.

MALWARE are those messages with attachments that are detected as malicious or links that lead to malware.

The significant increase in spam between the first and second halves of 2024 is due to Mimecast's evolving detection system and data collection, not a trend in spam volume. The increase in spam detections occurs because Mimecast added spam that was held by the gateway to the detection data, which can be configured by the administrator, rather than just high-confidence rejections.

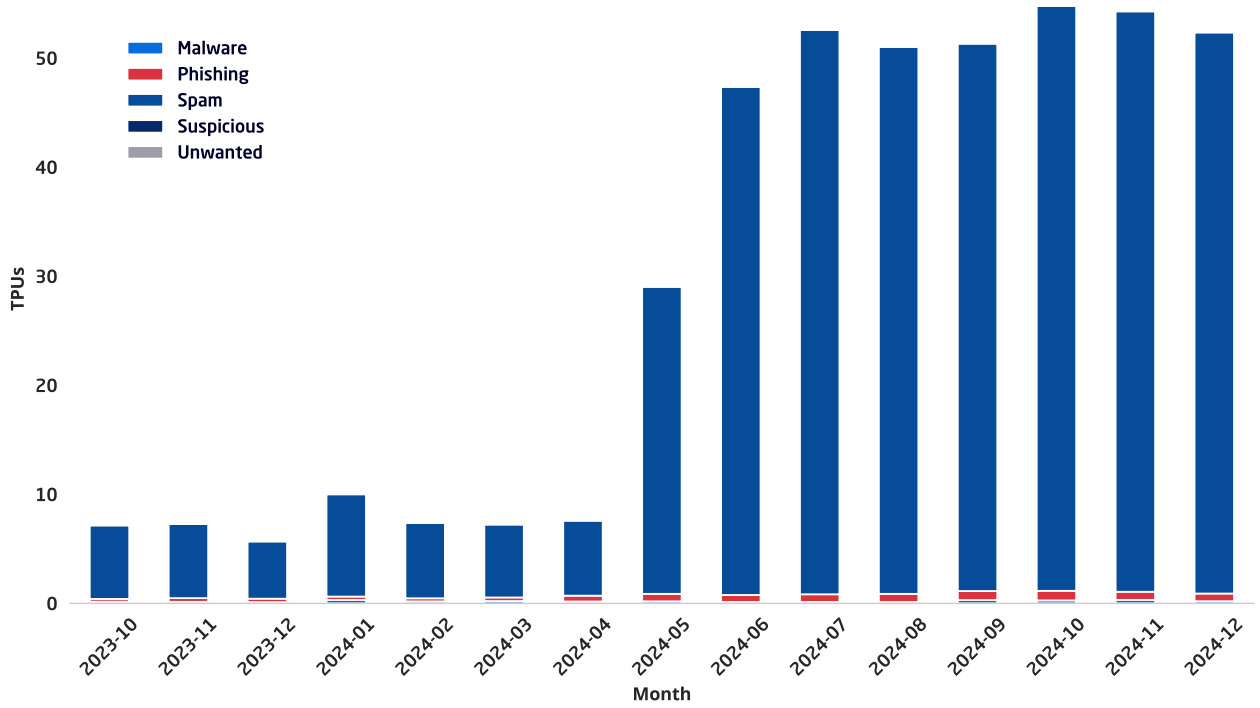


Chart 2a: The significant increase in spam detections follows the integration of spam held at the gateway, as opposed to solely relying on spam rejections; this change also introduces an element of admin configurability in managing spam holds.

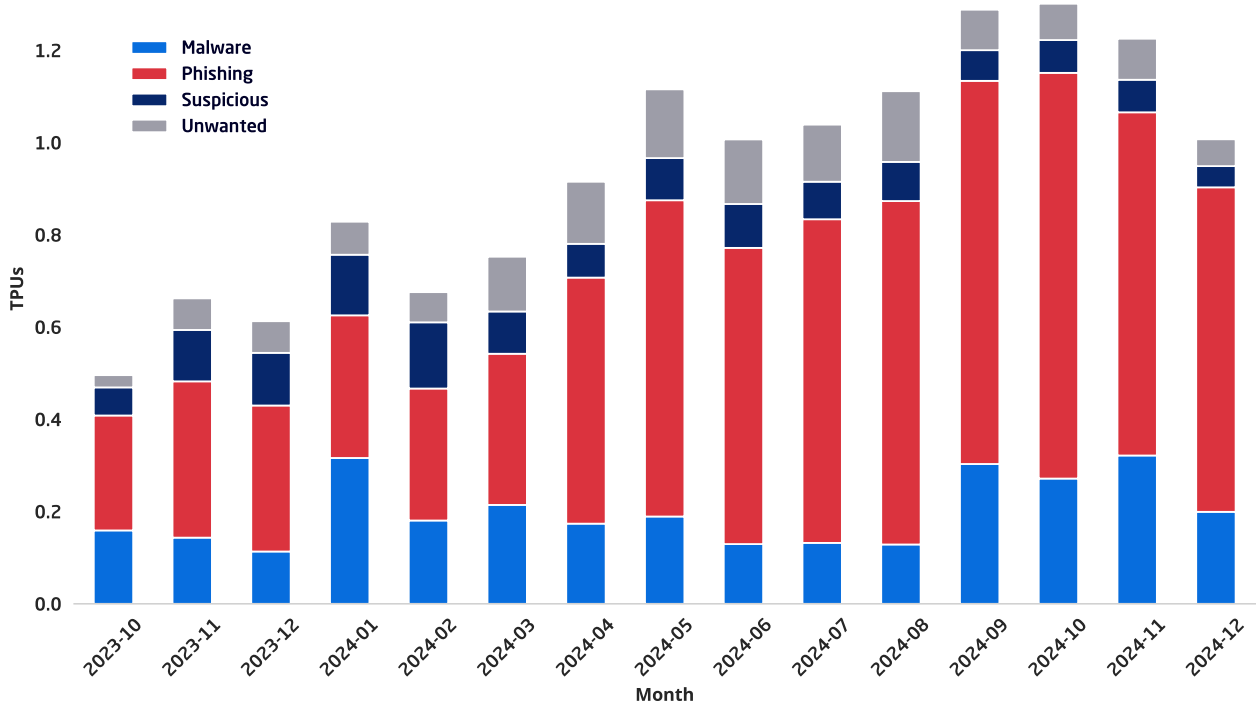


Chart 2b: Removing the overwhelming influence of the spam dataset shows that Phishing is on the rise, and a surge in Malware attacks late in the second half of 2024. In December 2024, malware detection in Sub-Saharan Africa surged by 42.14%, significantly higher than the previous year, driven by political instability and increased cyber activity. Additionally, the region is witnessing a rise in ransomware attacks, which are becoming more opportunistic, often exploiting vulnerabilities and delivered as secondary infections, indicating a concerning trend in the threat landscape.

TOP TARGETED INDUSTRIES BY TPUS

#03

Attackers tend to use different types of attacks to target different industries, giving each industry a distinctive threat profile. The Arts, Entertainment & Recreation sector — the top attacked industry after removing the large volume of spam — encountered the greatest number of threats per user (TPUs), with most attacks consisting of emails and messages with malicious payloads.

The Professional Services: Legal and Media & Publishing sectors saw the next highest threat intensity, with each encountering nearly 9 TPUs. Attackers targeted Professional Services: Legal with a greater number of impersonation attacks, while Media & Publishing encountered a high number of malicious URLs.

Every industry encounters a significant volume of spam as well as threats that are detected because of the attackers' use of low-reputation infrastructure. As part of the analysis, Mimecast removed bulk email messages — detected as Spam or Low Reputation — which accounted for 17 TPUs and 5 TPUs, respectively.

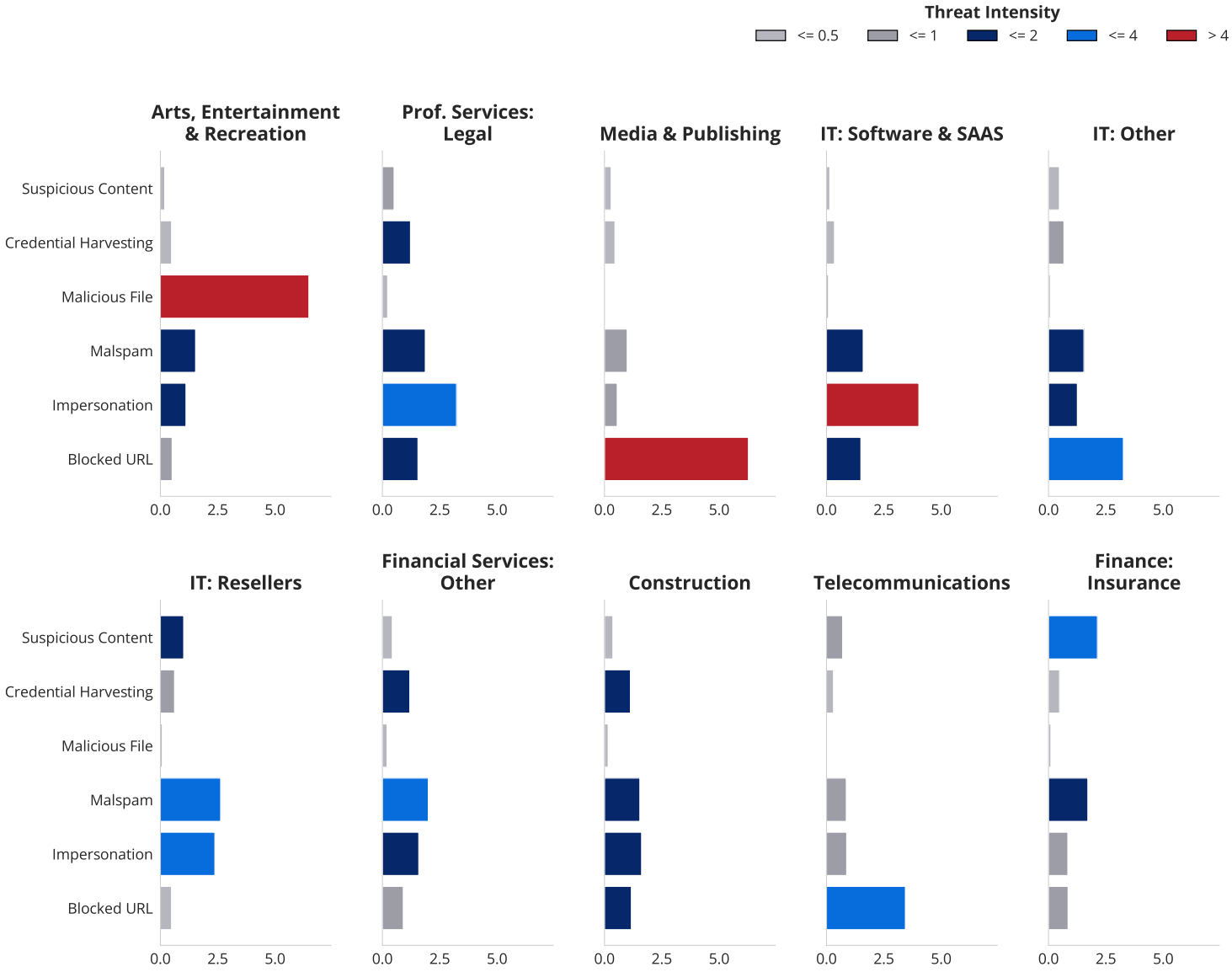


Chart 3: The threat profile for the Top-10 industries, without the Spam and Low Reputation categories since that tends to overwhelm the data. The TPU counts (x-axis) are in log format.

THREAT GROUPS
#04

Attributing cyber threats is inherently complex, especially with the blended tactics many threat actors employ and the rise of cybercrime-as-a-service models like Ransomware-as-a-Service (RaaS), Phishing-as-a-Service (PhaaS), and Initial Access Brokers (IABs). These services allow multiple threat actors to reuse the same tools and infrastructure, resulting in similar campaigns being launched by entirely different groups. Threat actors often employ a combination of techniques from different attack vectors and frequently change their methods, making it difficult to pinpoint a single actor or motive.

Traditional attribution methods, which rely on infrastructure or malware signatures, are increasingly unreliable. Instead, Mimecast focuses on analyzing Tactics, Techniques, and Procedures (TTPs) to categorize and reference threat operations systematically. By tracking how attackers operate, we group threats and identify patterns across campaigns, even when traditional attribution methods fail. This approach provides a clearer and more reliable understanding of their evolving capabilities. The most prolific threat operations with Mimecast internal attribution names are highlighted below with related campaigns to describe their behaviors and potential impact.

Threat operation

TO1014

First observed: 2020

GOAL

INFORMATION THEFT
AND ESPIONAGE

TARGETED

NORTH AMERICA
EUROPE
MIDDLE EAST

Sector

AVIATION
AEROSPACE
TRANSPORTATION

OCT 2024

Latest campaign

Threat operation

TO1003

First observed: 2018

GOAL

DATA THEFT

TARGETED

PREDOMINANTLEY
UNITED STATES

Sector

IT
EDUCATION

OCT 2024

Latest campaign

Threat operation

TO3010

First observed: 2018

GOAL

CREDENTIAL FOR
DISTRIBUTION

TARGETED

SOUTH AFRICA

Sector

ALL

NOV 2024

Latest campaign

Threat operation

TO5004

First observed: 2024

GOAL

FINANCIAL

CAMPAIGN INFO

TARGETED

PREDOMINANTLY
UNITED KINGDOM
UNITED STATES

Sector

MANUFACTURING
REAL ESTATE
RETAIL

DEC 2024

Latest campaign

Threat operation

TO3028

First observed: 2018

GOAL

CREDENTIAL HARVESTING

CAMPAIGN INFO

TARGETED

GLOBAL

Sector

ALL

DEC 2021

Latest campaign

Threat operation

TO3001

First observed: 2023

GOAL

CREDENTIAL AND DATA THEFT

TARGETED

AUSTRALIA

Sector

PREDOMINATELY EDUCATION

DEC 2021

Latest campaign

Threat operation

TO5005

First observed: 2020

GOAL

FINANCIAL

TARGETED

GLOBAL

Sector

ALL

DEC 2021

Latest campaign

Threat operation

TO3022

First observed: 2021

GOAL

CREDENTIAL HARVESTING

TARGETED

PREDOMINATELY UNITED KINGDOM

Sector

ALL

DEC 2021

Latest campaign

TOP VULNERABILITIES OVER TIME

05

While the vast majority of attacks attempting to exploit software issues focused on two popular vulnerabilities (CVE-2017-0199 and CVE-2022-42889), attackers attempted to exploit 89 different issues in the second half of 2024. Comparing the Top 10 vulnerabilities detected by Mimecast as part of an email or delivered as a link, seven issues have an Exploitability Prediction Scoring System (EPSS) score of at least 0.88 which equates to an 88% chance of exploitation within the next 30 days, while two vulnerabilities — both discovered in 2024 — have yet to be registered as exploited.

The mapping also shows the divergence of the EPSS score and the Common Vulnerability Scoring System (CVSS) score, which tends to correlate with the eventual severity of exploitation.

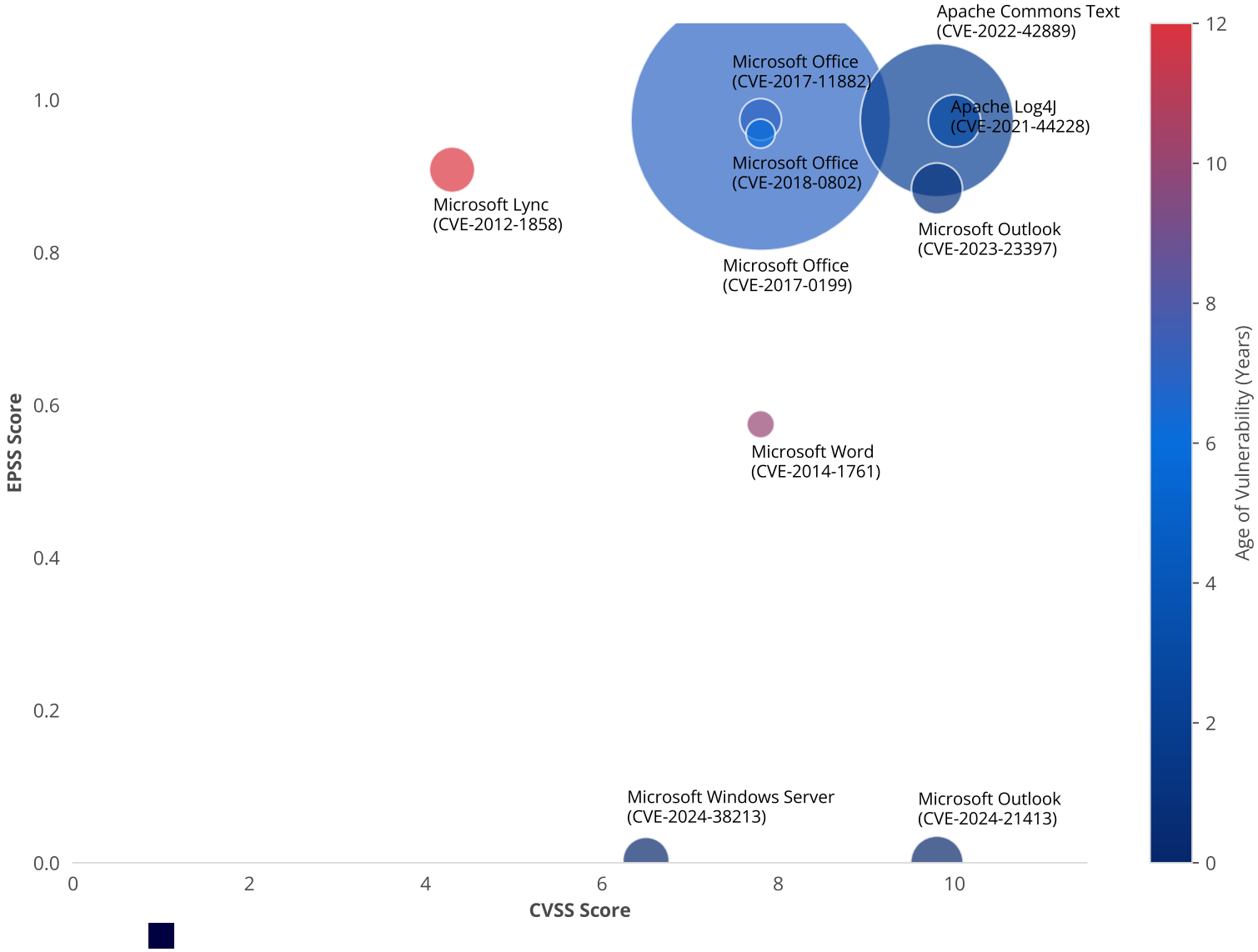


Chart 5: The Top 10 vulnerabilities detected in messages, compared by EPSS and CVSS scores. Two popular vulnerabilities are at least 10 years old. EPSS data collected as of 15 January 2025.

TOP THREATS AND CAMPAIGNS

04.2

01 OPEN SPOOFING

02 COPYRIGHT INFRINGEMENT/SUBSCRIPTION NOTIFICATION

03 USER LINK COPY AND PASTE - ACCOUNT PAYABLE SCAM

04 TARGETED BEC SCAM WITH AUDIO DEEPFAKE

05 MISSING A DELIVERY

06 FACEBOOK ACCOUNT TAKEOVER

#01 OPEN SPOOFING

TECHNIQUE Compromised consumer routers proxying spoofed phishing emails through ISP services

SERVICES USED Zimbra, MagicMail

TARGETS Global - all industries

READ ARTICLE

Threat actor

↓

Consumer ISP routers exploited through vulnerabilities or weak passwords

↓

Router configured to be used as a proxy

↓

Phishing emails relayed through ISP mail servers

↓

Malicious links hosted on various cloud services

↓

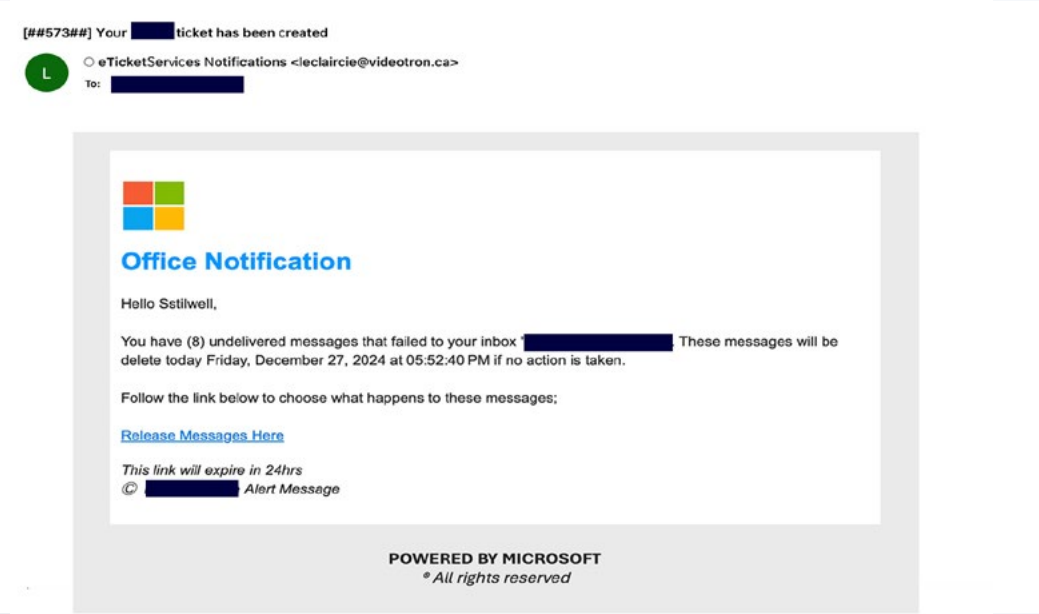
Prompted for M365 username and password

↓

Credentials harvested and user redirected to genuine M365 login page

Threat actors are leveraging compromised consumer routers as proxies to send large scale credential phishing campaigns through ISP email services obscuring their infrastructure and bypassing email authentication. By taking advantage of ISPs with weak or absent outbound email authentication threat actors achieve high-volume distribution and unrestricted sender spoofing capabilities.

The affected ISPs identified from our investigation use email solutions such as Zimbra and MagicMail, and appear to not have robust outbound anti-spam measures. The combination of inadequate authentication and relaxed security controls enables attackers to achieve high sending rates and sustain large-scale spam campaigns without significant disruption.



#02 COPYRIGHT INFRINGEMENT/SUBSCRIPTION NOTIFICATION

TECHNIQUE Impersonating law firms with copyright notice bait for info stealing

SERVICES USED Gmail, Mail Merge

TARGETS Global, but primarily UK-based - retail, wholesale, travel, and hospitality industries

READ ARTICLE

Threat actor

↓

Phishing email through mail merge service

↓

Links to content hosted on Dropbox

↓

Download zip file containing executable file

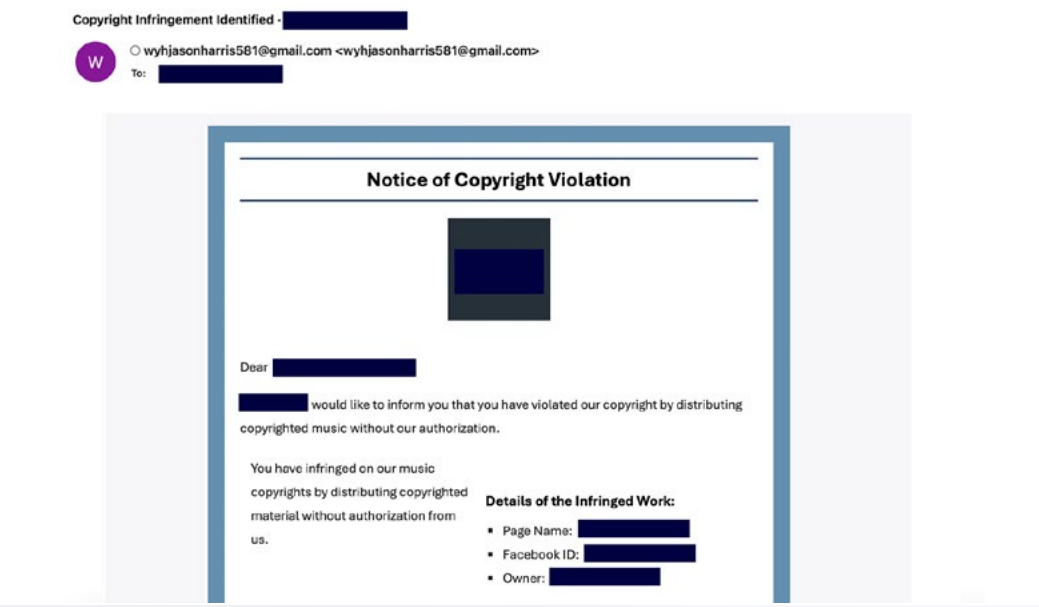
↓

Executable file downloads infostealer from Github

↓

Exfiltrates sensitive data

Malicious emails sent through Gmail via a mail-merge service are impersonating reputable law firms and claiming that companies are infringing copyrights. The email contains a direct Dropbox link or a redirect to Dropbox, which results in a download of a zip file containing an executable. The goal of the campaigns is to use various infostealers to steal sensitive information from infected machines such as credentials and financial details.



#03 USER LINK COPY AND PASTE - ACCOUNT PAYABLE SCAM

TECHNIQUE Convincing users to copy and paste a link to evade defenses

SERVICES USED Amazon Simple Email Service, Python mailers

TARGETS Predominately U.S - manufacturing, retail and legal industries

READ ARTICLE

Threat actor

↓

Phishing email through AWS using Python mailer

↓

User prompted to paste malformed URL into browser

↓

Redirects to a shared file hosted on a fake SharePoint

↓

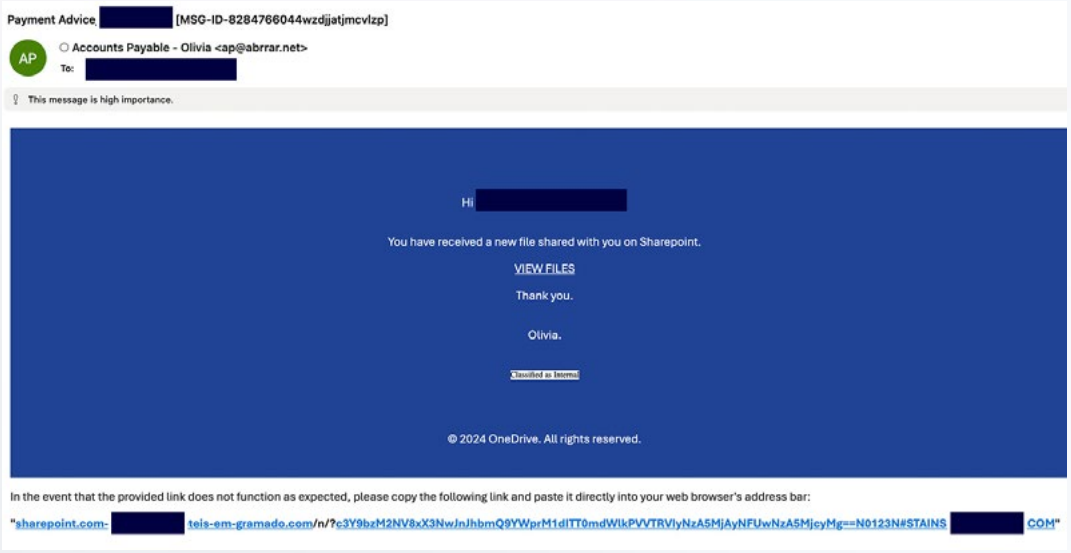
Prompted for M365 username and password

↓

Credit card used or sold in underground marketplaces

In their efforts to evade technical detection software and services, threat actors have moved on to convincing users to copy malformed links from an email — typically, they are missing the prefix "http://" — and paste those links in their browsers. The lures Mimecast analyzed usually included a button with a broken link and text that has some variation on: "If the link does not work, please copy and paste the link below."

This technique is in addition to other approaches to obfuscation, such as using QR codes to make links unreadable by humans and using scare tactics paired with phone numbers to prompt victims to call an attacker-operated call center. The goal of the current campaigns using this attack typically are to gather credentials from the victim.



#04 TARGETED BEC SCAM WITH AUDIO DEEPFAKE

TECHNIQUE Audio deepfake, business email compromise (BEC)
SERVICES USED Adobe Sign, DocuSign
TAGETED Global - predominately financial sectors

READ ARTICLE

Threat actor

↓

BEC email through Docusign or AdobeSign

↓

User signs digital NDA

↓

User calls fake number for NDA verification

↓

Interaction via email results in invoice for payment

↓

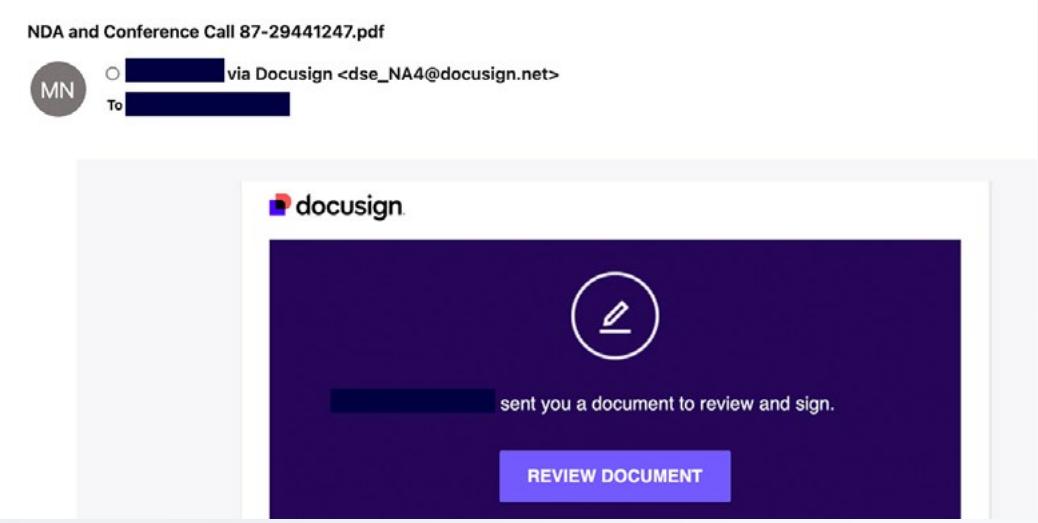
Deepfake audio from executive confirming payment

↓

Payment made to threat actor bank account

Employees in the Banking, Insurance, and other financial sectors are targeted with spear phishing emails that claim to be from a law firm and sent using a trusted service such as DocuSign and Adobe Sign.

The targeted messages ask the employee to sign the NDA and then call a number purportedly from a law firm, but the number is controlled by the attacker. The threat actor impersonates the law firm using deepfake audio techniques to disguise their voice and sends an email from an attacker-controlled domain that appears close to the impersonated law firm.
Finally, the attacker will send an invoice purportedly from the law firm and follow up with a deepfake call that poses as their company CEO or another executive.



#05 MISSING A DELIVERY

TECHNIQUE Living off trusted services (LOTS)
SERVICES USED S3 buckets on AWS to host HTML files
TARGETS UK - not for profit and housing industries

READ ARTICLE

Threat actor

↓

Phishing email through Biglobe ISP

↓

Redirected to HTML file hosted on AWS

↓

HTML file impersonates EVRI missed delivery page

↓

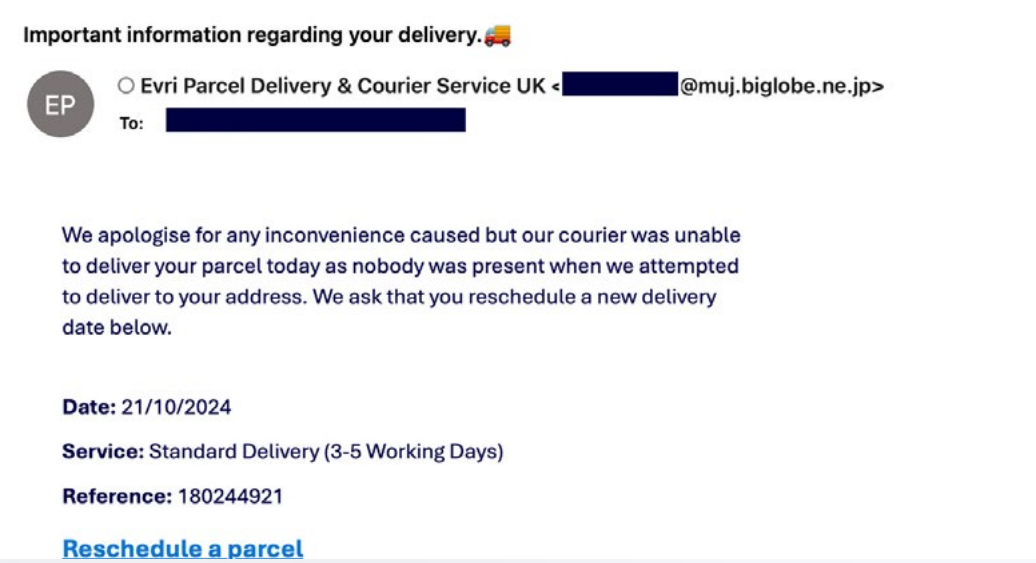
PII and credit card Information provided for updated delivery

↓

Credit card used or sold in underground marketplaces

Messages sent through BIGLOBE, a Japanese service that is often abused by threat actors, target not-for-profit and housing organizations in the UK with messages that indicate a delivery has been missed.

Threat actors take advantage of this and other ISPs by purchasing authenticated accounts through underground marketplaces, granting them legitimate access to their infrastructure and enabling them to send malicious emails that bypass most email authentication protocols.


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

#06 FACEBOOK ACCOUNT TAKEOVER — BRAND IMPERSONATION

TECHNIQUE Job lure impersonating brands such as Victoria's Secret, Red Bull and Coca- Cola
SERVICES USED Recruitee
TARGETS UK and US largely - predominately media & publishing and retail industries

READ ARTICLE

Threat actor

↓

Phishing email sent through Recruitee CMS

↓

Signup page on lookalike domain of impersonated brand

↓

Login via fake Facebook page to submit application

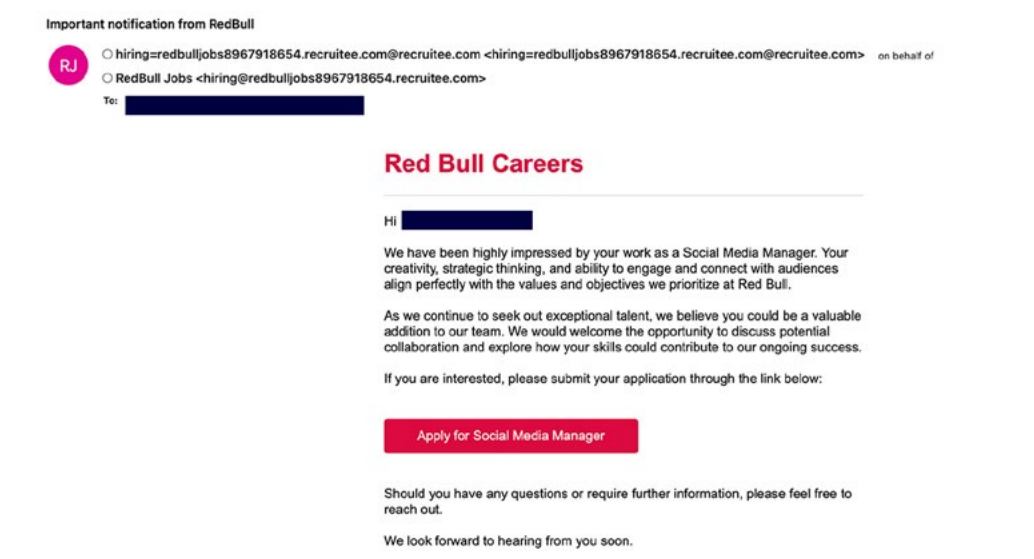
↓

MFA codes are required to complete application

↓

Facebook credentials obtained and shared via a Telegram logger

A recent phishing campaign leveraged Recruitee, a legitimate third-party recruitment CMS to send fraudulent job offer emails. Threat actors register lookalike domains impersonating well-known brands to add credibility to the scam. The phishing pages use CAPTCHAs and IP filtering to deter automated detection and aim to harvest Facebook credentials.


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.

ATTACKERS INCREASINGLY LIVE OFF TRUSTED SERVICES (LOTS)

From legitimate email providers to file-sharing sites to webinar-hosting services, attackers have extended their use of trusted services to bypass defenses that rely on reputation and trust. Attacks commonly use major email providers, such as Google's Gmail and Microsoft's Outlook (formally Hotmail), while links in email messages commonly terminate on a legitimate hosting service, such as Google Docs, Evernote, or Microsoft's OneDrive and SharePoint services.

As legitimate services find ways to deter abuse, attackers are also branching out to smaller providers. Major campaigns tracked by Mimecast, for example, used providers, such as Airtable, Publuu, and Wave Compliance.

GEOPOLITICAL RISKS RISE

As geopolitical tensions rise worldwide, the threat landscape is changing. Cyber attackers have become more active, using the cyber domain for intelligence collection, compromising rival nations' assets, and generating income. The perceived lack of concrete consequences for cyber operations has incentivized nations to expand their operations and cybercriminals to conduct more brazen attacks.

Yet, law enforcement has increasingly had successes in disrupting cybercriminal infrastructure, while defenders' efforts are making easy-to-hack targets rarer. Following Russia's invasion of Ukraine, both countries expended their stockpile of zero-day and n-day exploits, causing a spike (see Figure 1) that has since eased. In 2024, the total number of exploited vulnerabilities reported through the Known Exploited Vulnerability (KEV) catalog had maintained a steady, but low, rate.

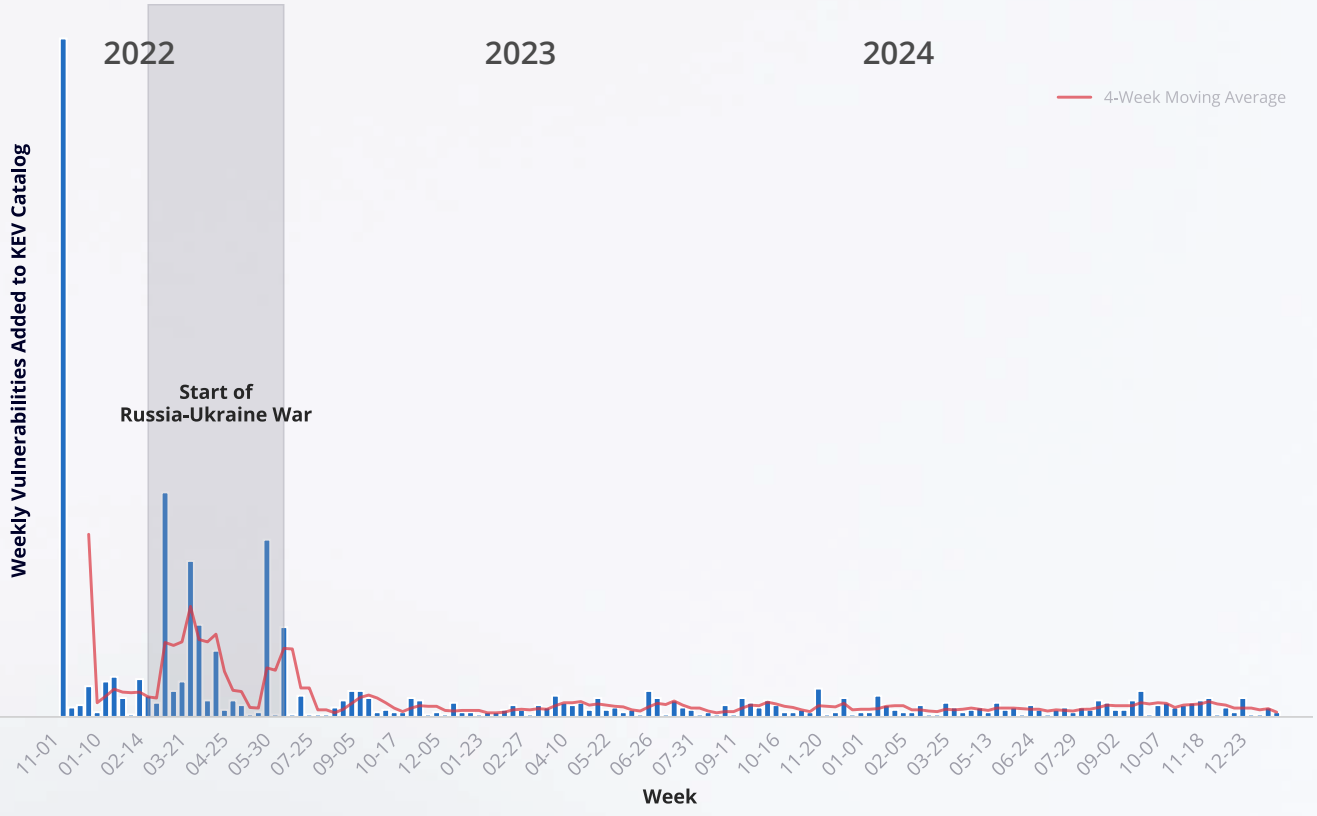


Figure 1: Since mid-year 2022, through the end of 2024, CISA has added about 4 vulnerabilities per week to the KEV catalog, according to data collected by the Cybersecurity and Infrastructure Security Agency (CISA). The data shows a large spike when the list was first published, followed by significant activity during the initial months of Russia's invasion of Ukraine.

While geopolitics has driven increase in the cyber-threat level, global events also give threat actors focused on the vulnerable human element a greater variety of lures.

The top geopolitical lures seen by Mimecast threat researchers:

01
CHINA-TAIWAN

02
CHINA-SOUTH CHINA SEA

03
CHINA-CUT CABLE

04
RUSSIA-UKRAINE WAR

05
ISRAEL-GAZA CONFLICT

06
EUROPEAN UNION LEGISLATION

07
RUSSIA-US ELECTIONS

08
IRAN-US ELECTIONS

09
US WEATHER EVENTS

TOP ATTACKED INDUSTRIES

The industries facing the most significant threat intensities include the Arts, Entertainment & Recreation sector, which saw more than 10 threats per user (TPUs), and the Professional Services: Legal and Media & Publishing sectors, which saw nearly 9 TPUs.

Most industries saw a distinctive threat profile. The Arts, Entertainment & Recreation sector saw a far greater proportion of attacks using malicious files, while law firm employees encountered a significant number of impersonation attacks. Attackers targeted workers in the Media & Publishing sector primarily with malicious links, while the Software & SaaS sector had to deal with many impersonation attacks.

As part of the analysis, Mimecast removed bulk email messages — detected as Spam or Low Reputation — which accounted for 17 TPUs and 5 TPUs, respectively.

01	ARTS, ENTERTAINMENT & RECREATIONAL	10.322010 TPU
02	LEGAL	8.613564 TPU
03	MEDIA & PUBLISHING	8.622578 TPU

MAJOR EVENT TIMELINE.

04.2

JULY
10 BILLION PASSWORDS LEAKED

SEPT.
ASIAN CRYPTOCURRENCY EXCHANGES HIT WITH THEFTS
INTERNET ARCHIVE BREACHED

OCT.
SALT TYPHOON WORRIES GROW

NOV.
IRANIAN "FAKE WORKERS" TARGET SENSITIVE INDUSTRIES

DEC.
U.S. TREASURY HACKED THROUGH THIRD PARTY
PHISHED DEVELOPERS ALLOW BROWSER EXTENSION COMPROMISE

JULY

10 BILLION PASSWORDS LEAKED

VULNERABILITY Passwords leaked
IMPACT Credential stuffing and brute force attacks

The discovery of RockYou2024, the largest password compilation leak in history, containing an astonishing 9,948,575,739 unique plaintext passwords. This massive file, was posted on a hacking forum raises significant concerns, as it includes passwords accumulated over the past two decades, potentially exposing many users to credential stuffing attacks and other security threats.

SEPT

ASIAN CRYPTOCURRENCY EXCHANGES HIT WITH THEFTS

VULNERABILITY Network breaches
IMPACT More than US$70 million in losses

Attacks on two cryptocurrency exchanges, Singapore-based BingX and Indonesian-based Indodax, suffered massive losses after separate breaches. Jakarta-based Indodax pledged to compensate users after a $22 million loss, while BingX claimed a $44 million loss. In the United States, the Department of Justice also announced the arrest of two people connected with stealing $230 million in cryptocurrency from a U.S. citizen.

INTERNET ARCHIVE BREACHED

VULNERABILITY Unknown
IMPACT Information on 31 million unique accounts exposed

The Internet Archive suffered multiple breaches over a period of 22 days. Around Sept. 28, a threat actor stole the database file for the Internet Archive's Wayback Machine, compromising usernames, email addresses, and encrypted passwords. While the site's founder said it had scrubbed systems and upgraded security, multiple denial-of-service attacks and a second breach occurred in October.

OCT

SALT TYPHOON WORRIES GROW

VULNERABILITY Infiltration of U.S. telecommunications
IMPACT Chinese actors gain broad access to communications

Chinese state-sponsored threat group, Salt Typhoon, gained access to highly sensitive information on U.S. citizens and government officials by compromise major U.S. telecommunications and Internet-service providers, including Verizon and AT&T. As many as nine different providers are reportedly affected, including gaining access to the court-authorized wiretap infrastructure at some providers, in what has been called a "counterintelligence failure of the highest order."

NOV

IRANIAN "FAKE WORKERS" TARGET SENSITIVE INDUSTRIES

VULNERABILITY Social engineering, LinkedIn abuse

IMPACT Aerospace, aviation and defense industries in Israel and the United Arab Emirates; Turkey, India and Albania are also possible targets

Suspected Iranian hackers used fake recruiting web sites to pose as recruiters on LinkedIn, contacting aerospace, defense, and aviation companies in Israel, the UAE, Turkey, India, and Albania. Hackers have posed as recruiters on LinkedIn to distribute malware to victims through fake lucrative job offers to spy on targets and steal sensitive data starting in 2023. The malware and tactics are similar to those of a North Korean hacking group that targeted cryptocurrency exchange-traded funds.

DEC

U.S. TREASURY HACKED THROUGH THIRD PARTY

VULNERABILITY Third-party supplier, critical role of security software

IMPACT Attackers gained access to unclassified data on some workstations

The U.S. Treasury Department announced that a breach of identity-security provider BeyondTrust had cascaded down to its own systems leading to the exposure of several workstations and unclassified data. While the investigations continues, the United States pointed to a Chinese state-sponsored hacking group that reportedly gained access to an API key used for remote support. BeyondTrust has not yet revealed how the attackers gained access to the critical key.

PHISHED DEVELOPERS ALLOW BROWSER EXTENSION COMPROMISE

VULNERABILITY Spear phishing attack leading to elevated permissions on Chrome extensions

IMPACT Information collection by malicious extensions of end users' credentials and information

Threat groups have compromised more than 30 browser extensions in the past year by sending spear phishing emails that appear to be from Google to the contact person or group for the targeted Chrome browser extensions. Developers who click on the email are asked to grant privileges to a benignly named application, but actually are giving attackers the ability to replace their extension with a malicious application. Data security firm Cyberhaven first reported the tactics in December, after one of its developers fell prey to the attack and granted permissions to the "Privacy Policy Extension" application. As many as 2.6-million users may have been impacted by the attack.

RECOMMEN-DATIONS

05

THREAT SPECIFIC

BEST PRACTICES & ADVISORIES

STEPS FOR MIMECAST CLIENTS

CROW

SPECIES

Known for their problem-solving and teaching skills. Always educating, and taking **action**. Your go-to for cybersecurity risk mitigation strategies.

THREAT-SPECIFIC COUNTERMEASURES.

05.1

Organizations should be taking specific actions to improve defenses and raise the cost for attackers.

HUMAN RISK MANAGEMENT

Organizations should implement a human risk management framework that aligns security objectives with business goals. By mapping the human risk factors and potential adverse outcomes, companies can develop a multi-tiered response system that differentiates between unintentional mistakes and malicious actions. The primary concerns are loss of intellectual property or other competitive information, exfiltration of sensitive data, and misuse of company resources.

Organizations should incorporate both positive reinforcement "nudges" and corrective remediation measures in a phased approach. To achieve these measures, it's critical to establish cross-functional working groups to ensure stakeholder buy-in and effective change management, while maintaining clear communication channels with leadership about risk metrics, potential incidents, and mitigation strategies.

PROVIDE AWARENESS TRAINING

In today's complex landscape where geopolitical tensions frequently manifest as cyber threats, comprehensive awareness training becomes essential. Staff must be educated not only about general cyber risks but also about how global events can influence phishing campaigns, insider threats, and social engineering attempts targeting their organization. By implementing robust awareness training programs and human risk platforms to guardrail users, organizations can strengthen their human firewall against both conventional cyberattacks and those driven by geopolitical motives. This human-centric approach to security helps staff identify and respond to threats effectively, whether they come through email, social media, collaboration tools or other vectors that exploit human psychology.

MANDATE MORE SECURITY FROM THIRD PARTIES

Attacks against businesses in the Manufacturing, Transportation, Storage & Delivery, and Retail & Wholesale sectors represent significant third-party risk of supply chain compromise. Companies should review their service-level agreements to set minimum levels of data security and cybersecurity and find ways to monitor their suppliers more closely, such as using external rating services and subjecting acquisitions to extra scrutiny.

BLOCK IMAGES IN EMAIL MESSAGES

Attackers are increasing their use of image-based file types to sneak in phishing lures and malicious code while evading detection. Mimecast's analysis has identified threat actors also using encryption and foreign language text within images to escape notice. Companies should configure email clients to prevent the loading of images in messages and isolate any images that users explicitly flag.

Note: CyberGraph users should leverage trusted sites to ensure banners load correctly.

SCAN ENVIRONMENT FOR MISCONFIGURATIONS OR EXTERNALLY OPEN PORTS

Organizations should regularly scan their infrastructure for known exploitable routes, such as insecure open external network ports or public cloud environments. Using tools like Cloud Security Posture Management, companies can quickly identify misconfigurations in their public cloud. This will ensure that any publicly accessible server ports are closed or adequately secured and protected.

As an example, Mimecast has noted continuing increases in attacks against remote desktop protocol (RDP) ports, which account for 80% of effective ransomware compromises. Attackers will continue to look for open RDP ports to target organizations.

SEGMENT THE NETWORK AND LOG INTERNAL TRAFFIC

Attackers, especially during a ransomware attack, can quickly move laterally throughout a network. Segmenting the internal network and putting critical assets in their own enclaves can reduce the damage caused by ransomware and other attacks. Monitoring internal traffic, especially communications into specific segments, can result in earlier detection of threats.

HARDEN USER CREDENTIALS, DEPLOY MFA

Many malware threats exploit common passwords to infiltrate networks. Recent attacks highlight how weak passwords contribute to breaches. Strengthen any network by enforcing robust passwords, especially for privileged users. IT security must eliminate default admin passwords. Requiring multifactor authentication can drastically reduce compromise of stolen accounts or credentials.

05.2

BEST PRACTICES AND ADVISORIES.

APT40 ADVISORY: PRC MSS TRADECRAFT IN ACTION

8 July 2024 READ MORE >

Organizations: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK, BND and others

The government agencies responsible for cybersecurity and law enforcement in Australia, Canada, New Zealand, Germany, South Korea, the United Kingdom, and the United States outlined the tactics used by Chinese state-sponsored threat actor APT40 (also known as Gingham Typhoon), which "has repeatedly targeted Australian networks, as well as government and private sector networks in the region." The group can quickly utilize adapt and exploit proof-of-concept code for new vulnerabilities into attacks and deploy those tools in campaigns.

DETECTING AND MITIGATING ACTIVE DIRECTORY COMPROMISES

Sept. 2024 READ MORE >

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

The cybersecurity agencies of the Five Eyes nations describe 17 different techniques for attacking Microsoft Active Directory, the most common identity and access solutions used in businesses. Because of its pivotal role in authentication and authorization, and its susceptibility to compromise due to default settings and complexity of installation, malicious actors often target Active Directory.

RUSSIAN MILITARY CYBER ACTORS TARGET U.S. AND GLOBAL CRITICAL INFRASTRUCTURE

5 Sept. 2024 READ MORE >

Organizations: CISA, FBI, NSA

Multiple Russian threat groups associated with military agencies targeted Ukrainian government agencies and other NATO allied targets with the destructive WhisperGate malware. The attackers have typically used vulnerabilities in network devices to gain initial access.

2023 TOP ROUTINELY EXPLOITED VULNERABILITIES

12 Nov. 2024 READ MORE >

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

Perhaps belatedly, the top agencies in the Five Eyes nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) released information on the top 15 routinely exploited vulnerabilities from 2023. Eleven of the 15 vulnerabilities were exploited in zero-day attacks, compared to only two zero-day issues of the dozen vulnerabilities listed in 2022.

CYBER RESILIENCE ENHANCEMENT: CISA RED TEAM'S U.S. INFRASTRUCTURE ASSESSMENT INSIGHTS

21 Nov. 2024 READ MORE >

Organizations: CISA

The Cybersecurity and Infrastructure Security Agency (CISA) identified significant cybersecurity weaknesses in a critical infrastructure organization during a red team assessment. The team breached the organization using a web shell left from a previous assessment, compromising its domain and sensitive systems due to poor network protections and slow responses.

IRGC-AFFILIATED CYBER ACTORS EXPLOIT PLCS IN MULTIPLE SECTORS, INCLUDING US WATER AND WASTEWATER SYSTEMS FACILITIES

18 Dec. 2024 READ MORE >

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

The cybersecurity agencies of the US, Israel, Canada, and the UK have issued an updated advisory. It describes malicious cyber activities by actors linked to Iran's Islamic Revolutionary Guard Corps (IRGC), including attacks on programmable logic controllers and critical infrastructure in the UK and Israel.

STEPS FOR MIMECAST CLIENTS.

Mimecast users can follow specific steps with medium technicality to guard against reported threats.

EMAIL SECURITY CLOUD GATEWAY

1. It is recommended to use single sign-on from your identity provider or leverage Mimecast's built in multi-factor authentication to reduce an attacker's ability to leverage email as their attack vector.
2. Ensure DNS authentication policies honor DMARC records. A second policy scoped to a policy group with the DMARC Fail action set to Ignore/Managed and Permitted Senders will provide an effective bypass for any legitimate mail being rejected/quarantined for DMARC failures.
3. Optimize Impersonation Protection as per the best practice guidelines of two hits set to tag Subject/Body and include a separate C-Level/VIP policy based on name match with a hold for admin review. In addition, create another policy for any detections of three hits or more with the admin hold action.
4. Implement Advanced BEC Protection with three policies: Moderate Enforcement for threat detection, Sender Bypass for trusted sources, and Recipient Bypass for internal exclusions.
5. Setting an aggressive re-writing of URLs will ensure all URLs are scanned upon click but be aware that anything that looks like a URL will be re-written e.g., IP addresses and internal links.
6. Utilize pre-built integrations with the majority of SIEM and XDR vendors to provide log capture and analysis for security policy enforcement.
7. Leverage bring-your-own threat intelligence to take advantage of any third-party threat feeds for automatic rejection of matching indicators.
8. End users should report potentially malicious messages received through Mimecast user tools to the Mimecast SOC for additional analysis.

EMAIL SECURITY CLOUD INTEGRATED

1. Enable Browser Isolation to minimize the risk of users accessing potentially suspicious sites.
2. Customize your Allow and Block rules to specifically who is allowed in your environment.
3. Review weekly reports to gain insight into the threats detected in your environment.
4. End users should report potentially malicious messages received through Mimecast user tools to the Mimecast SOC for additional analysis.

If you are unsure of the effect of any of the proposed settings, please reach out to your Mimecast account manager, customer success manager or log a call with Mimecast support.

CONCLUSION.

In the latter half of 2024, threat analysis revealed an intensification of sophisticated disinformation campaigns and coordinated hacktivist operations, coinciding with escalating geopolitical tensions that enabled threat actors to weaponize global events for targeted attacks; these evolved tactics now encompass systematic data exfiltration, targeted ransomware deployment, and orchestrated DDoS attacks, while exploiting human vulnerabilities through sophisticated social engineering campaigns centered around major geopolitical developments, collectively posing significant risks to business continuity and system availability.

The identification of malicious activity has become technically complex due to adversaries blending malicious actions with legitimate operations, including the exploitation of trusted services and common system binaries. Threat actors increasingly leverage legitimate red team tools, creating significant challenges for security controls to differentiate between authorized and unauthorized activities. This necessitates enhanced monitoring capabilities, including advanced behavioral analysis and anomaly detection systems.

In other areas of the threat landscape, social engineering attacks maintain high success rates, evolving through the integration of automated AI technologies. Advanced persistent threats now leverage sophisticated deepfake technologies and AI-generated content for targeted attacks, significantly complicating traditional detection and prevention mechanisms. The technical sophistication of these attacks highlights intricate social engineering research and analysis of supply chain communication patterns.

Perimeter security remains a critical concern, with threat actors consistently exploiting vulnerabilities in edge infrastructure, including VPN appliances, firewalls, and internet-facing services. Zero-day exploitation combined with delayed patch implementation creates extended vulnerability windows, particularly in high-availability environments requiring extensive patch testing. This challenge is amplified by complex network architectures and expanding attack surface driven by cloud infrastructure migration and evolving operational technologies. Organizations require dedicated incident response capabilities, including advanced forensic tooling, network analysis systems, and automated detection mechanisms.

Vulnerabilities likely to be exploited this year:

VPN

As seen in the recent addition of CVE 2025 0282 Ivanti Connect Secure VPN to the CISA Known Exploitable Vulnerabilities catalog.

AUTHENTICATION

Most recently seen in vulnerabilities exploiting Bypass via an alternative path or channel, and missing authentication code.

DENIAL OF SERVICE (DOS)

An increasingly popular malicious activity designed to disrupt business operations e.g CVE 2024 3393 PAN OS Firewall Denial of Service (DoS).

Resources.

webinar
Translating Threat Intelligence into Practical Security Strategies

research report
State of Email and Collaboration Security

TI HUB.

Mimecast TI Hub

Community.

Mimecast central

mimecast