Cyberint
A Check Point Company

Retail Threat Landscape Report

Q1-Q3 2024 Summary

November 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The United States, is a prime target for cyber attacks. The U.S. retail sector, which holds nearly one-third of the global market share, has seen a significant rise in ransomware incidents, accounting for 45% of global retail ransomware cases in the past three quarters—a 9% increase from 2023.

New groups like Ransomhub and Hunters have emerged and supply chain threats have increased. Social engineering tactics are on the rise, with attackers impersonating IT personnel.

Threat actors continually seek ways to bypass security measures, using trusted platforms like GitHub to distribute malware. Stolen credentials remain a common compromise vector, often sold on darknet forums and used as a first stage in attacks.
AI integration brings both benefits and risks, such as 'shadow AI,' where employees share sensitive information with AI models. AI also aids in generating malicious code, impersonation and phishing emails.

Phishing remains a prevalent tactic, with campaigns using malicious QR codes and HR impersonation. State actors, especially those under sanctions, exploit remote work to steal information and fund regimes.

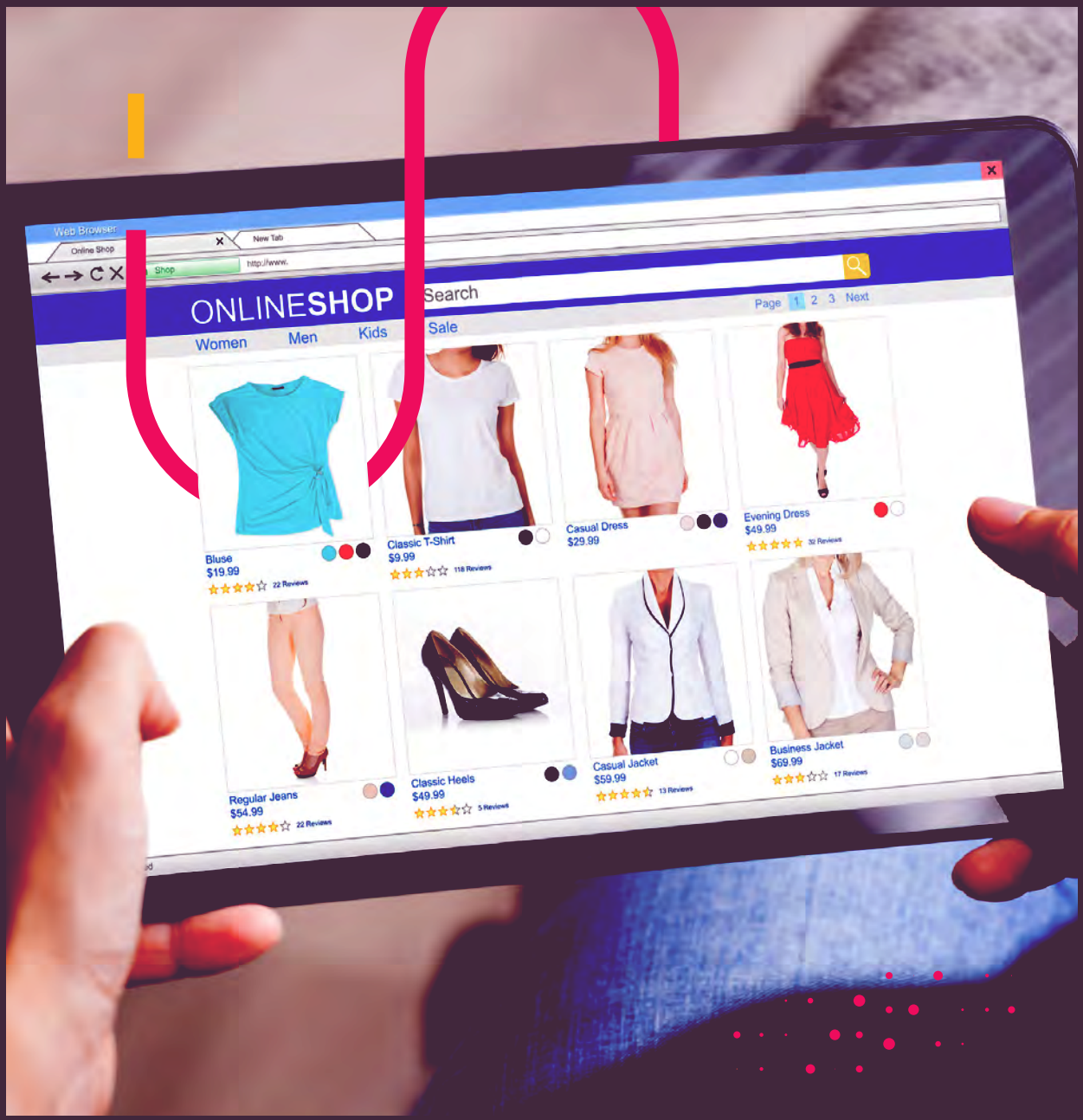
Cyber-activism has risen due to global tensions, targeting government entities and companies with controversial ties.

The rise in ransomware, new threat actors, and sophisticated tactics highlight the need for comprehensive risk assessments and robust security protocols.

INTRODUCTION

As one of the world's largest and most advanced economies, the United States remains a prime target for cyber adversaries and state actors. The retail industry faces a constantly evolving array of threats among its major sectors. The rise of e-commerce and the increasing volume of digitally collected and stored customer data have made retailers particularly vulnerable to cyber attacks.

This report examines the current threat landscape in the retail sector, identifying the most pressing threats, such as data breaches, ransomware, and supply chain attacks. We will also aim to provide strategies to mitigate these risks.



RANSOMWARE & RETAILERS IN THE U.S

Based on data collected from Q1 to Q3 of 2024, the United States remains the most targeted region for ransomware incidents. Over 1,700 incidents have been reported, affecting entities from small businesses to Fortune 500 companies. Notably, 48% of all global ransomware incidents occurred in the U.S for said quarters.

The retail industry in the U.S. reported 206 ransomware incidents in Q1-Q3 2023, and in 2024 alone, the U.S reported 256 ransomware incidents, an overall 24% increase in the same time period.

Top 5 Affected Countries In Retail Ransomware Cases

In the United States, retailers account for approximately 28% of the global retail market share[1] however, they account for nearly 45 % of all retail ransomware incidents collectively in the past 3 quarters. This increased likelihood is attributed to the expansion of many popular U.S. retailers outside the region and their overall dominance in the market. Additionally, U.S. culture and its brands are well-known thanks to Hollywood and other U.S. cultural exports, increasing the chances of being perceived by foreign hacker groups as noteworthy targets. Furthermore, hacking a U.S. entity has more prestige for a ransomware group looking to increase its reputation for both economic, and political reasons.

Ransomware attacks have the potential to inflict significant losses attributable to operational disruptions, data theft, and ransom payments. The retail sector, which stores confidential data encompassing customers' personal and fiscal details, makes retailers a lucrative target for ransomware groups.

[1] https://capitaloneshopping.com/research/retail-statistics/

The theft of customer data provides these groups with greater leverage, as it could potentially lead to widespread lawsuits and customer churn, which in some cases be more expensive than a ransomware payment (such as GDPR violations). Furthermore, the industry's dependence on technological systems for routine operations and its larger workforce renders it susceptible to ransomware infections via unsecured networks and devices.

An analysis of ransomware incidents across various sectors reveals that the retail industry remained a significant target. In Q1-Q3 2023, the retail sector accounted for 10% of the total 1634 ransomware incidents in the United States, making it the third most targeted sector. This trend continued into 2024, with the retail sector comprising 14% of the 1,782 ransomware cases placing it second place. Overall, data shows a 9% increase in ransomware incidents in these quarters of 2024 compared to 2023.

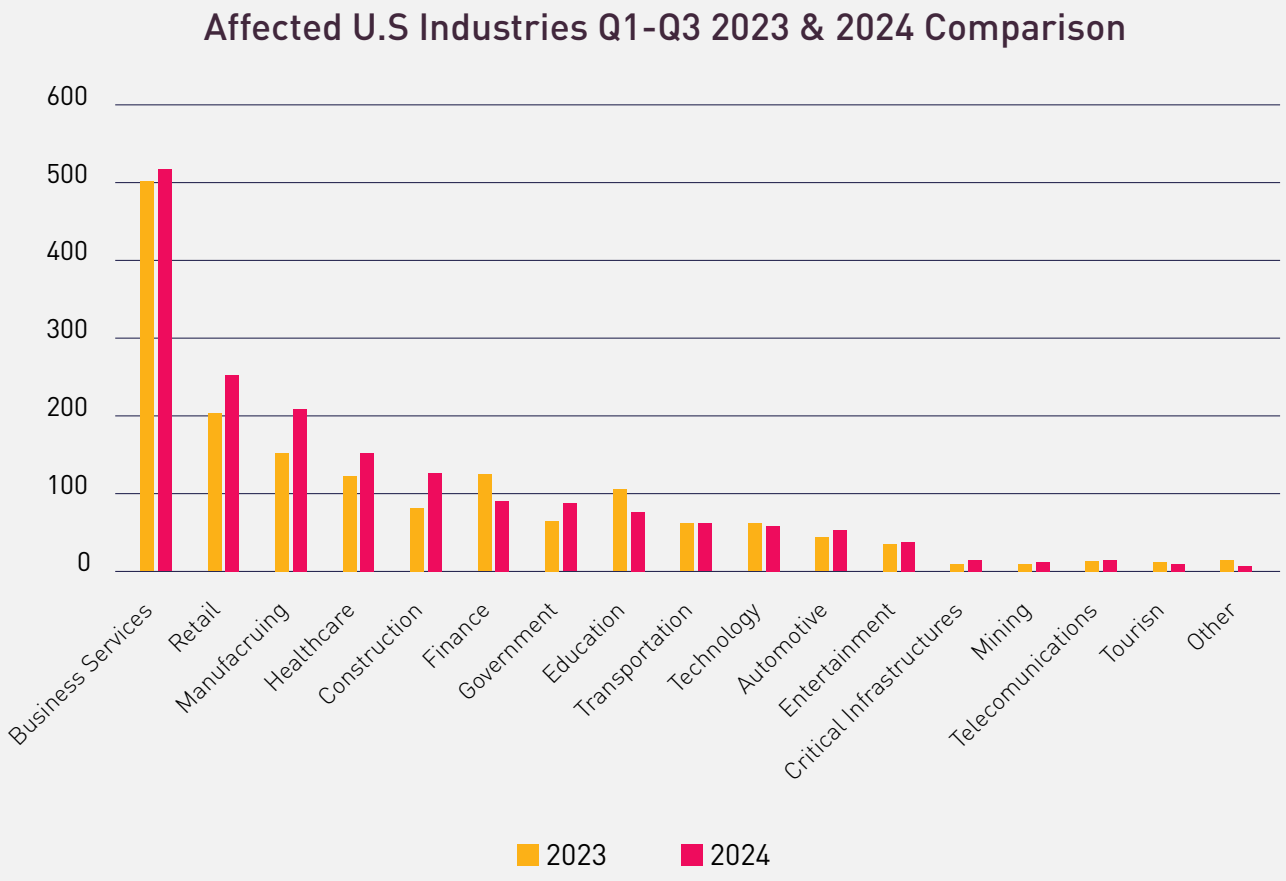


Figure 1: Q1-Q3 2023-2024 Comparison Overview of Ransomware Attacks in the U.S

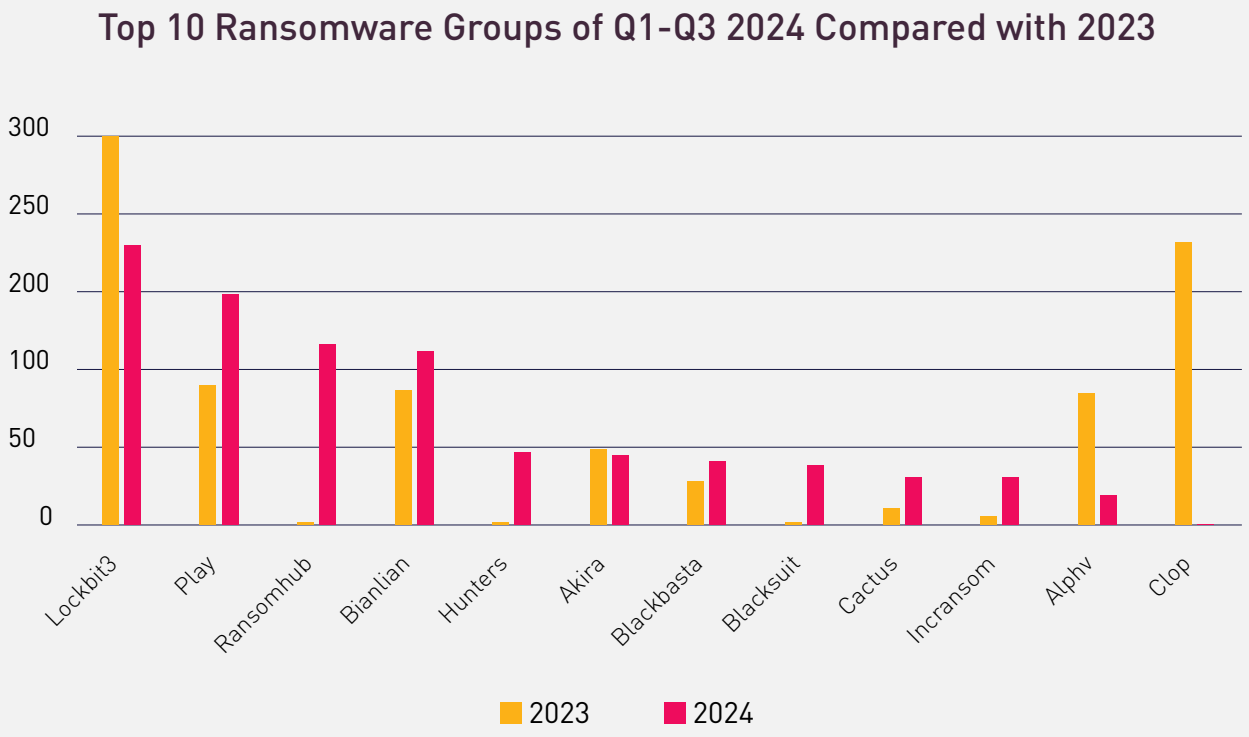
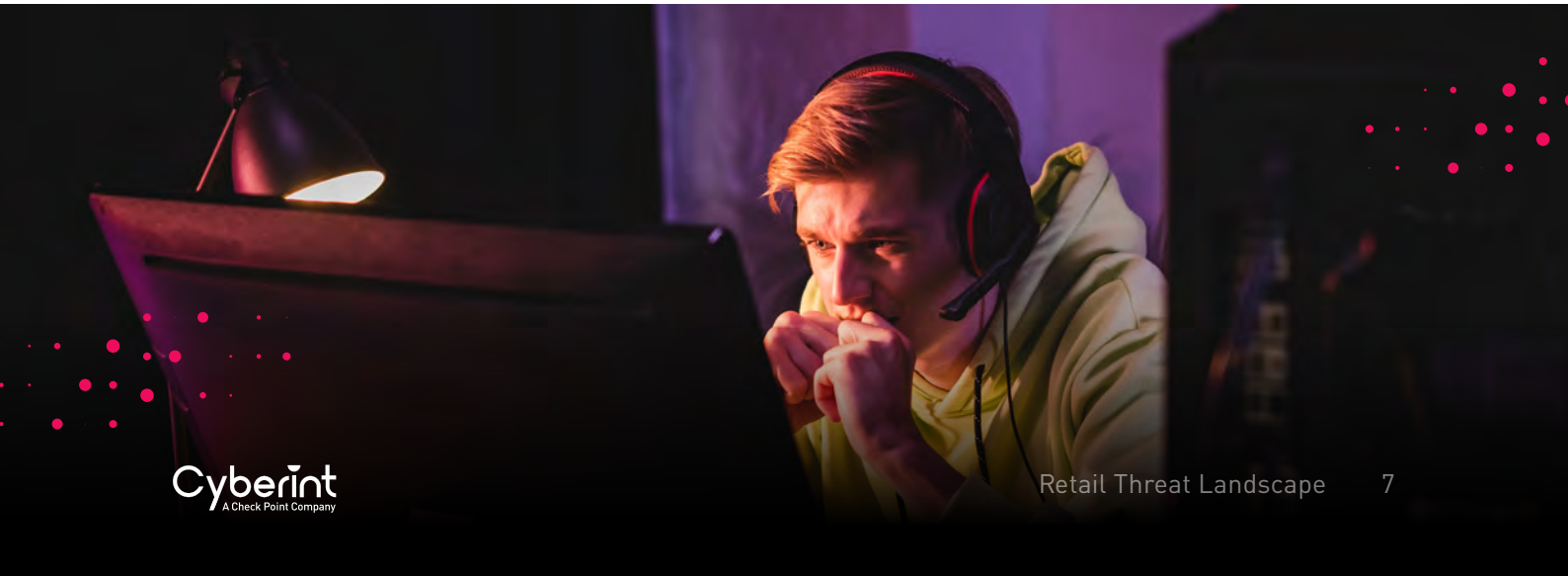


Figure 2: Q1-Q3 2023-2024 Top 10 Ransomware Group Activity – Alphv & Cl0p Notable Mentions

This increase is attributed to the rise of newer ransomware groups such as 'Ransomhub', 'Bianlian', 'Hunters', and 'Blacksuit', which are attempting to enhance their reputation and stand out among other ransomware groups.

It's worth noting that prominent ransomware groups' activities from 2023 have significantly dropped. This is attributed to law enforcement activity against major players such as Lockbit and AlphV/Black Cat during 2023-2024. Additionally, a potential hiatus of Cl0p, which collectively accounted for 40% of ransomware attacks in 2023 in the U.S.

For a more in-depth report on figures surrounding current trends and details surrounding the threat of ransomware please see our 'Ransomware Q3 Report' report.



SUPPLY-CHAIN THREATS

In 2023 and 2024, the topic surrounding supply chain threats almost became synonymous with discussions surrounding ransomware, as many high-profile data leaks in the past two years were due to supply chain vulnerabilities that ultimately led to ransomware. This trend is also shown in OpenText's 2024 Cybersecurity survey[2] which found that 62% of respondents experienced a ransomware attack originating from a supply chain partner.

In addition to the usual threats via privileged access through unsecured supply chain vectors, social engineering attacks that abuse the relationship between the third-party vendor and the client are also noteworthy. One such example is the infamous Crowdstrike-Microsoft outage, which led to many threat actors impersonating IT personnel and Crowdstrike support staff in hopes of installing trojans, stealing credentials, or getting backdoor access to systems.

Therefore, remaining vigilant against social engineering attacks following a data leak or significant outage is important. Additionally, supply chain breaches provide threat actors with opportunities to gather intelligence on the company, including knowledge of specific contracts and agreements and potential email correspondence history, which could be leveraged in their social engineering campaigns as it would make them seem more trustworthy.

Threat actors will persist in exploiting any vector that gives them an advantage in social engineering tactics to breach an organization.

KEY POLICY RECOMMENDATION AND CONSIDERATIONS:

It is imperative to conduct risk analyses of supply chain vendors and stay vigilant for social engineering attacks following a third-party breach, especially those that have business relations with the organization. Consider the following:

- Temporarily blocking communications to a third-party vendor after a breach (depending on its severity and access).
- Attach an automated warning temporarily to any emails received from an affected vendor to warn employees of the breach, and its implications.

[2] https://www.opentext.com/about/press-releases/opentext-cybersecurity-2024-ransomware-survey-supply-chain-attacks-surge-ransom-payments-persist

MALWARE INFECTION VECTORS

In 2024, Cyberint observed various methods employed by threat actors to compromise potential victims. These strategies were identified through darknet communications, instructional guides, tutorials, and use cases shared by clients and cyber security practitioners.

UTILIZATION OF TRUSTED PLATFORMS

In 2024 Cyberint observed the abuse of trusted platforms for malware distribution. For instance, malware payloads were distributed via GitHub comments, where the download links or payloads evaded endpoint system detection. Additionally, encrypted emails and platforms such as Dropbox were utilized to distribute malware, successfully bypassing firewalls in some cases.

These observations indicate that threat actors have identified that exploiting platforms trusted by endpoint systems and firewalls increases their chances of evading initial detection, thereby providing more opportunities to infect victims.

```
https://github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
https://github[.]com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip
```

Figure 3: GitHub Comments Distributing Malware Hosted on Microsoft's Official GitHub Repository

INFO STEALER MALWARE

Information stealers or stealer malware are a type of malware designed to steal sensitive data such as financial information, credentials, and sensitive personal data. Moreover, Info stealers do not only steal credentials, but also cookies that may enable them to bypass multi-factor authentication.

Information stealers can spread through phishing emails, malicious software downloads, and other means, making it important for retailers to have robust security measures in place to protect their customers' and employees' sensitive information.
Stealer malware will continue to be a prominent risk among all industries due to its successful implementation of the Malware-As-A-Service nefarious strategy.

TOP AFFECTED REGIONS IN INFO STEALER MALWARE

The most targeted regions are Brazil, Turkey, and Egypt. Compared to 2023, the United States dropped from 5th place to 7th place among the countries most affected by info stealers. One of the most common vectors for info stealer infections is the downloading of pirated software, which is more prevalent in the top targeted regions.

Figure 4: Top 10 Affected Regions In Info Stealers

INFO STEALER MALWARE FAMILIES DISTRIBUTION

Currently, the information stealers industry is distributed among various malware families. While Redline remains the leading player, accounting for 55% of stealer cases in the U.S (42% worldwide), it is no longer the sole dominant force. Aurora is linked to 32% of cases, followed by other significant players such as Raccoon and Lumma. The remaining stealer malware families collectively hold less than 1% of the share in the U.S.

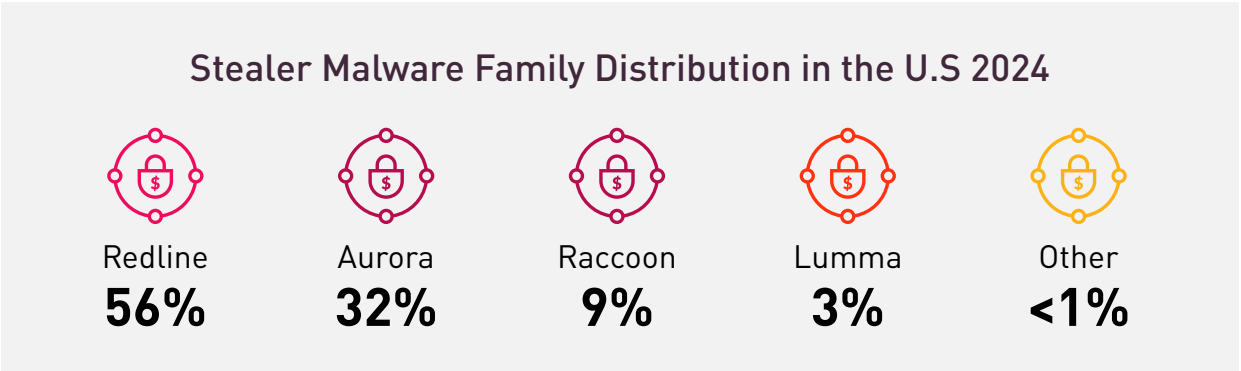


Figure 5: Info Stealer Malware Distribution

TOP AFFECTED EMAIL HOSTNAMES

Cyberint has collected the top affected email hostnames exfiltrated by info stealers.

Gmail has been present in over 1.3 billion instances. A notable mention is the 'other category' that includes all other email hostnames, including, but not limited to corporate hostnames totalling 314 million instances. Based on Cyberint's experience, most of the corporate credentials are exposed on a private machine, which shows the importance of managing browser syncs on private devices used for work purposes.

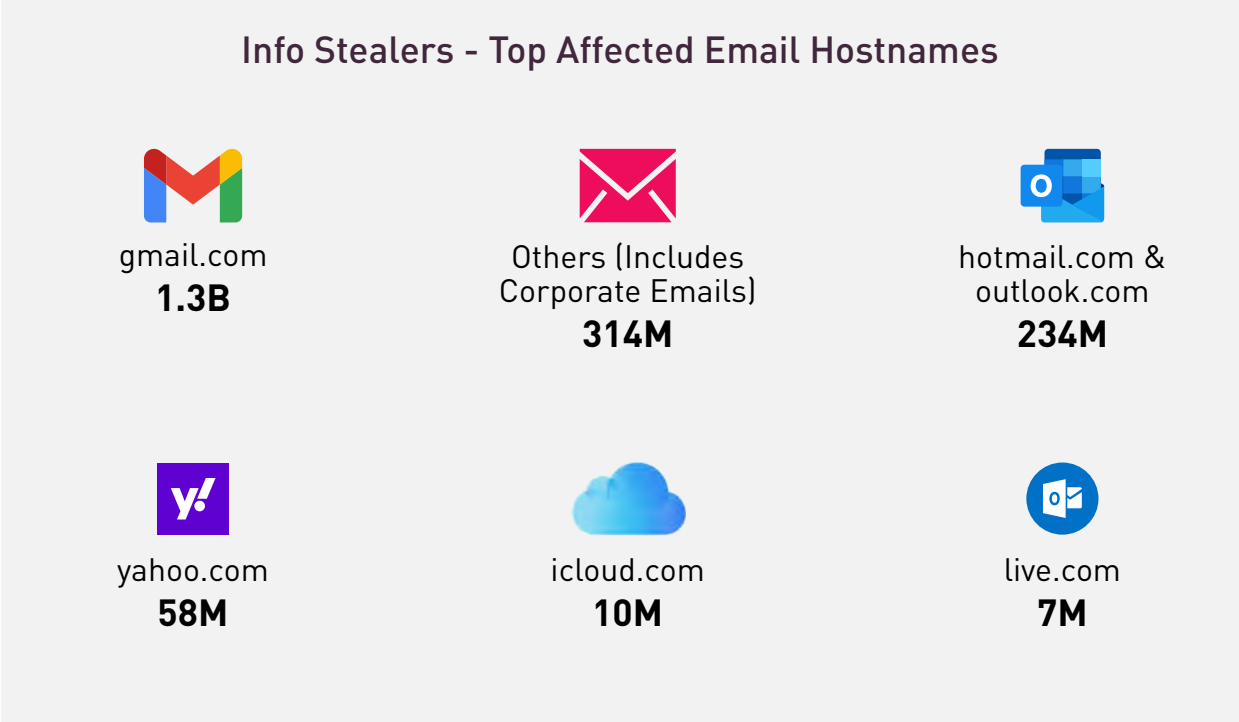
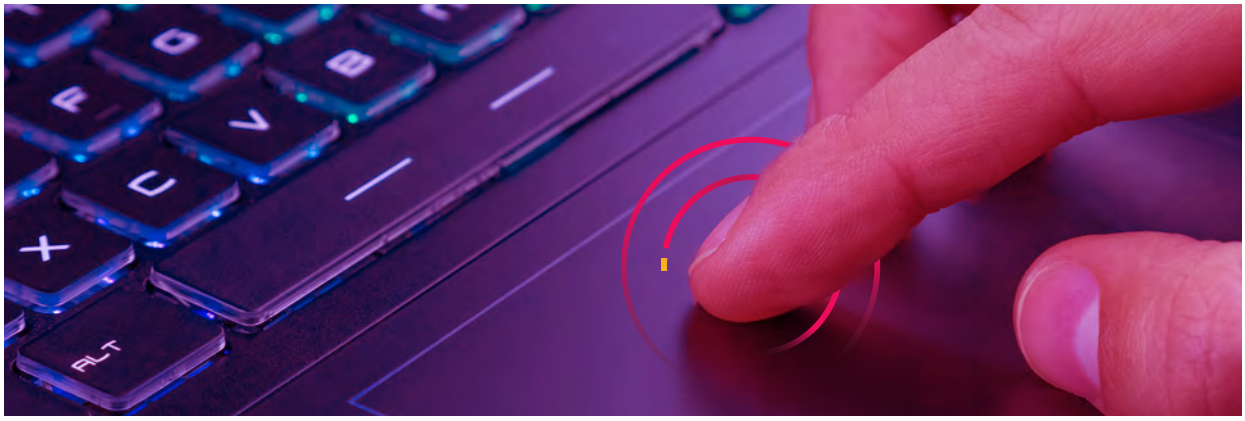


Figure 6: Top 5 & Notable Mention - Total Count of Emails Exfiltrated by Info Stealers

It is imperative to note that each collected malware log has the same email propagated many times, in some cases with the email counted hundreds of times on a single malware log which will skew the overall amount. This shows that each hostname is linked to hundreds of URLs, possibly affecting hundreds of different accounts.



TOP COMPROMISED PLATFORMS

The top 3 services most frequently targeted for theft are rather unchanging, Google, Facebook, and Roblox have been the top 3 affected platforms since 2021. Notably 21 million login.microsoftlonline.com were at risk of compromise, these include many Microsoft SSO credentials; placing it at 9th place compared to the rest.

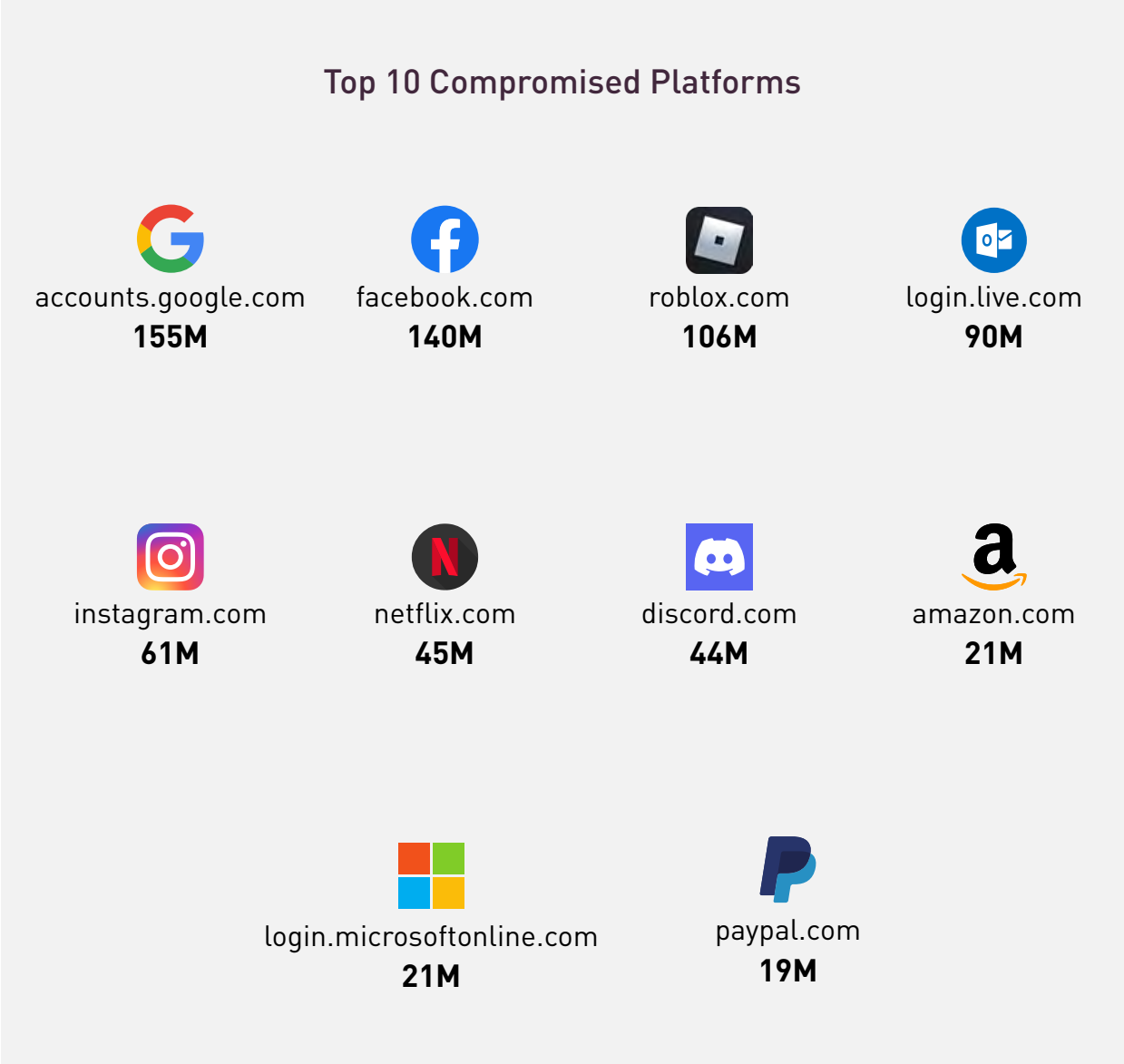


Figure 7: Top 10 Compromised Platforms at Risk

Info Stealer malware is one of the most common account compromise vectors, they are distributed among initial access brokers, state actors, ransomware groups, and many others. In most cases the machines infected by info stealers are private machines. A compromised private device could be used for spear phishing purposes, or directly affect an employee's private life, ultimately putting the organization at risk. One such example is Threat Actors employing extortion campaigns demanding corporate access to an account after taking over their Gmail, Facebook accounts or other private accounts.

KEY POLICY RECOMMENDATION AND CONSIDERATIONS:

- **Employee Awareness:** Employees should be reminded to practice good credential hygiene, such as not reusing credentials, and to give due consideration to the security of any stored credentials, such as within applications.

- **Behavioural Analysis:** Monitoring for behaviour that deviates from a baseline, such as unusual login times and unauthorized access of resources could assist in preventing access to a Threat Actor in cases of a compromise.

- **Practice Least Privilege – Conditional Access:** In cases where employees or vendors that have internal access are compromised, implementing conditional access best practices can help mitigate the risk. By allowing only compliant devices from specific locations to access company resources, the potential vectors through which threat actors could infiltrate company systems are significantly limited.

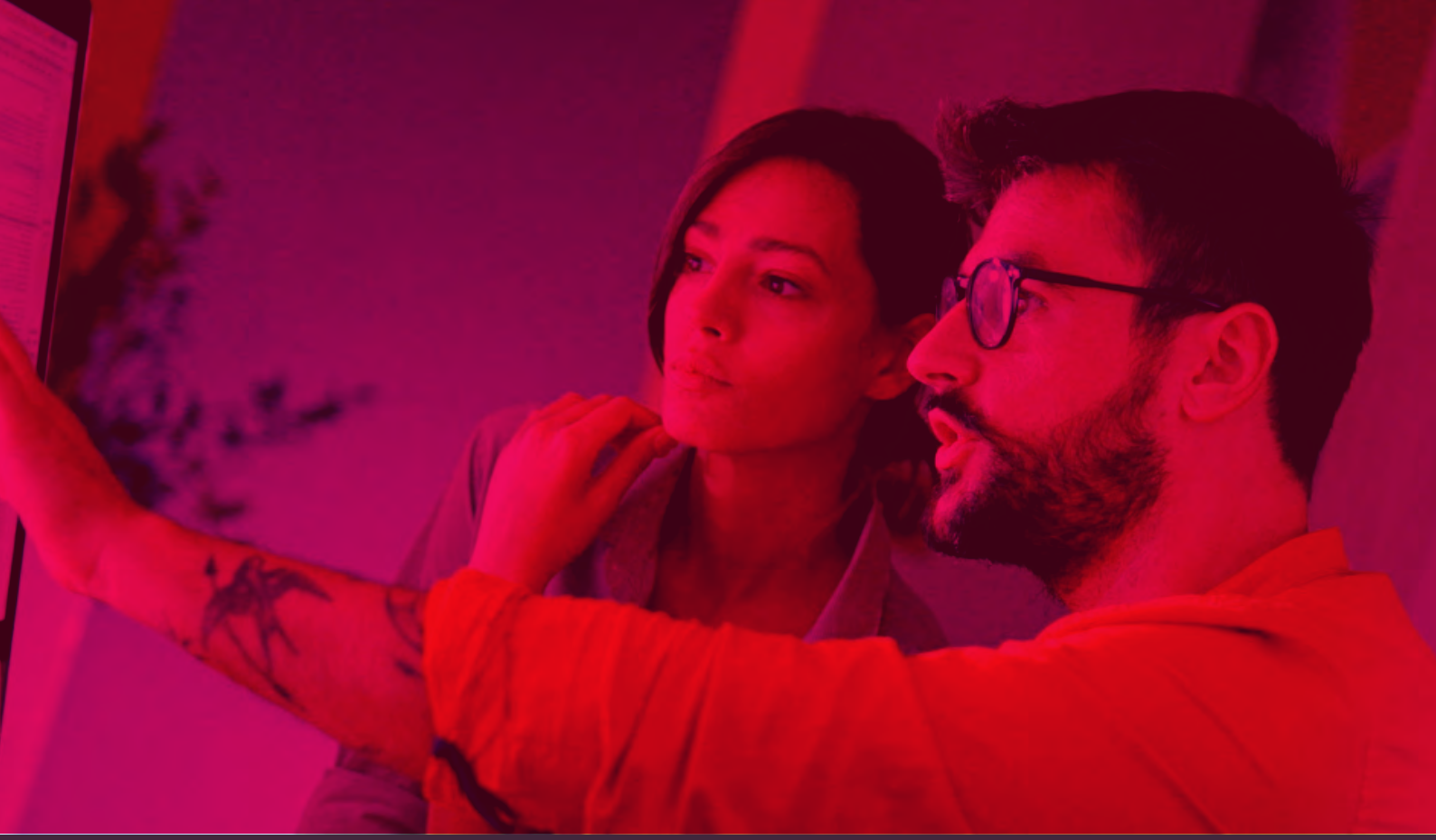
AI TOOL THREATS

THE EMERGENCE OF 'SHADOW AI'

Since ChatGPT's public debut in 2022, discussions surrounding artificial intelligence, and its implications have increased exponentially. Subsequently, numerous new competitors have entered the market for large language models (LLMs), integrating these technologies into our daily technological landscape. It is expected that the use of these tools will soon become as commonplace as using search engines, becoming an integral part of our everyday lives.

However, this integration is not without its risks, as it introduces new attack vectors. These could be exploited to steal input data from compromised accounts stored in public LLM platforms or to abuse hypothetical vulnerabilities in LLM databases that have been trained on sensitive proprietary data. This is demonstrated by OpenAI's ChatGPT, which publicly stated that it lacks the capability to delete data that has been submitted to it, even if it's propriety or sensitive data that would be used to train its future models. In theory, "jailbreaking" and certain manipulated queries might grant access to this sensitive data. One such use case involves 'Samsung' which experienced 3 different incidents due to 'shadow AI'.

Similar to the concept of 'shadow IT,' the emergence of 'shadow AI' introduces new attack vectors for companies. This phenomenon inherently exposes organizations as unauthorized AI tools and applications are adopted without proper oversight and security measures.



KEY POLICY RECOMMENDATION AND CONSIDERATIONS:

- **Define Acceptable Use:** Establish clear guidelines on the acceptable use of AI tools, specifying which applications and scenarios are permitted. This includes outlining the types of data that can be processed and the ethical considerations.

- **Implement Access Controls:** Restrict access to AI tools to authorized personnel only. This can be achieved through authentication mechanisms and role-based access controls to ensure that only qualified individuals can utilize these technologies.

- **Regular Audits and Monitoring:** Consider conducting regular audits and continuous monitoring of AI tool usage to detect any unauthorized activities. Implementing automated monitoring systems can help in identifying and addressing potential misuse.

- **Training and Awareness Programs:** Educate employees about the risks associated with 'Shadow AI' and the importance of adhering to established policies.

- **Incident Response Plan:** Develop a comprehensive incident response plan to address any breaches or misuse of AI tools. This plan should include steps for immediate containment, investigation, and remediation of any identified issues.

AI TOOLS IN SOCIAL ENGINEERING ATTACKS

Just as everyday AI tools enhance productivity and efficiency for employees, they also benefit threat actors by aiding in generating code snippets and modifying malicious code; scaling their operation. Although it's still far from generating fully functional malicious code, it already proved useful in generating convincing phishing emails with little to no experience.

Social engineering, image, and voice impersonation threats have recently made headlines in the past year. Cyberint expects more to come, as this type of threat is relatively new and has little exposure. While current best practices tend to train employees to detect suspicious emails, attachments, and SMS messages, most employees are less likely to suspect voice & video meetings from their fellow colleagues. Although it's still relatively rare, several victims have already fallen to these types of attacks, and it is imperative for companies to share with employees the new dangers of impersonating AI calls and even video impersonation in suspicious meetings, looking for tell-tale signs of social engineering attempts.

Those most at risk for this type of impersonation are employees who have extensive public exposure, including, but not limited to, public meetings, podcasts, conference calls, etc. This vulnerability arises because sufficient recordings of their voice and/or images can be used to train AI models specializing in speech and video generation. Consequently, such AI tools could be employed to impersonate an executive's voice or image during a call or online meeting, potentially deceiving employees.

KEY POLICY RECOMMENDATIONS AND CONSIDERATIONS:

It is imperative to keep employees informed and updated on current social engineering trends. Organizations should include these new threats in their social engineering threat awareness training courses.

EXAMPLES:

- **Scenario-Based Training:** Incorporate real-world scenarios involving voice and video impersonation to help employees effectively recognize and respond to these threats.

- **Verification Protocols:** Consider implementing additional verification protocols before sensitive actions are made to circumvent the possible threat, such as large contracts and transactions. Use pre-agreed verification questions or codes during meetings to confirm the identity of participants, especially for high-risk individuals.

NOTABLE PHISHING THREATS

In 2024, Cyberint discovered and analyzed many different phishing campaigns, with several more sophisticated and distributed than others. The most notable are the campaigns that attempted to bypass email firewalls with malicious QR codes, phishing websites that tried to circumvent and steal 2FA codes, and the continuing trend of malicious ads.

Additionally, certain events, such as benefit enrollment periods, Defcon and Blackhat, or other industry-specific conferences, are potential opportunities for Threat Actors to utilize in their phishing campaigns.

MALICIOUS QR CODES THAT REDIRECT TO PHISHING INTERFACES

Cyberint have observed an increasing trend of malicious QR codes being used to bypass email firewalls. Typically, these emails do not contain any other links or executable malicious content. Most security solutions do not actively scan QR codes to verify if they link to malicious content, making QR codes an additional vector that threat actors can exploit to circumvent email firewalls.

If the email content is convincing and not blocked due to the sender's IP address or a potentially spoofed domain, recipients who scan the QR code may be directed to a phishing link if they do not exercise due diligence. Furthermore, malicious QR codes can indirectly bypass corporate endpoint security and firewalls, as recipients are likely to use their private devices, which are usually not under organizational scrutiny. Consequently, uninformed victims are more likely to visit phishing sites or download malware.

Figure 8: Malicious QR Code Utilized for Phishing

AI TOOLS EMPOWERING PHISHING CAMPAIGNS

Generative AI tools have been observed aiding social engineering methods by impersonating human users in live chats. These tools often pose as support staff or interact with victims in real-time on social media platforms, SMS, and other communication channels. Essentially functioning as chatbots, these AI tools possess greater autonomy due to their generative capabilities, making them highly convincing and increasing the likelihood of victims falling for these attacks.

Compared to a pre-determined set of instructions in static phishing kit code, this enables threat actors to act during real time during their phishing campaigns.

HR IMPERSONATION – ABUSING KNOWN PROCEEDINGS

During the first half of 2024, several clients were targeted by email phishing campaigns impersonating HR personnel during the expected benefits enrollment period. These campaigns primarily targeted newly employed individuals, indicating that threat actors are actively monitoring new hires within various companies. New employees are perceived as particularly vulnerable and more susceptible to social engineering attacks due to their limited familiarity with the company's email correspondence, procedures, and protocols.

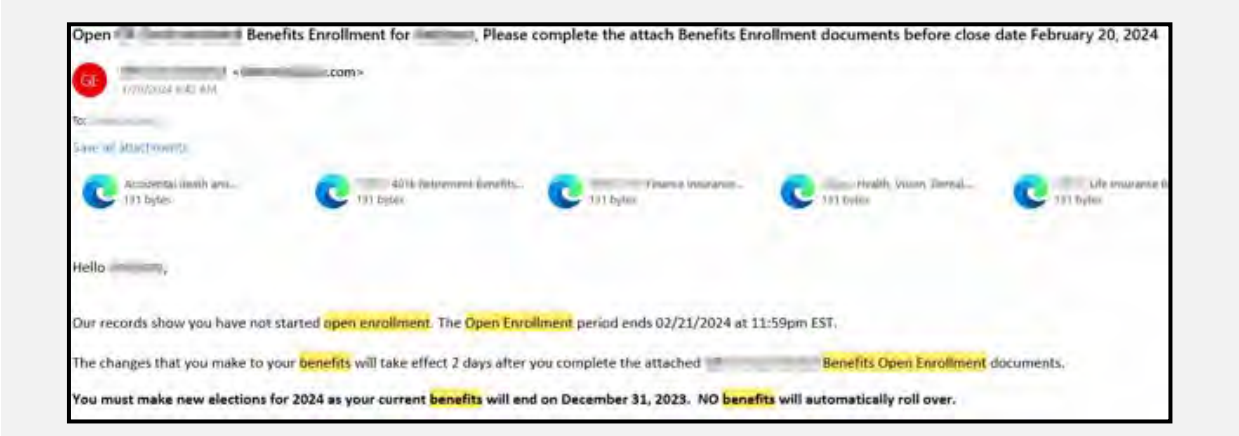


Figure 9: HR Impersonation – Fake Benefits Enrollment

KEY POLICY RECOMMENDATIONS AND CONSIDERATIONS:

Organizations should implement and add these additional tactics (malicious QR codes, HR impersonations around known events, chatbots powered by generative AI) to their repository of phishing exercises. Organizations should consider:

- Implementing additional security solutions that can detect and block any of the newer threats.

- Consider sharing regular updates and reminders during known periods when phishing campaigns are rampant. Such periods include, but are not limited to, tax filing season, elections, world events (such as the Olympics, World Cup, NFL season), etc.

STATE ACTOR THREATS

NEFARIOUS STATE ACTORS INFILTRATING ORGANIZATIONS

In 2024, the issue of insider threats has gained significant attention, particularly concerning nefarious state actors under sanctions who apply for legitimate positions within organizations. The entities at risk do not only include government organizations but also corporations that offer remote work positions or outsourcing opportunities in other regions. This threat is particularly noteworthy because these employees perform their job duties while funneling their salaries into shell accounts controlled by state actors, most nefarious being North Korea[3]. In more severe cases, these insider employees are waiting for an opportunity such as privileged access or other means to attack the organization's systems, install backdoors, steal proprietary information, or install ransomware.

Retailers are not expected to be ignored by such state actors, and it's imperative to conduct due diligence, as most remote tech positions, such as SWEs, developers, AI, Cloud, and Cybersecurity roles, are on their radar.

KEY POLICY RECOMMENDATION AND CONSIDERATIONS:

Organizations should conduct additional due diligences for remote positions and consider the following inspections:

- Monitor for suspicious IP inconsistencies (where the employee claims to be physical compared to where they are logging in from).
- Monitoring logs for any suspicious activity like malicious uploads, trying to access things they are not supposed to, and working outside of "normal" work hours that are not standard or approved beforehand.
- Threat Actors typically want to get hired for tech roles. Therefore, extra scrutiny checks for remote positions in SWEs, developers, AI, Cloud, and Cybersecurity roles should be a priority.
- Communicate with HR and check for any hires who exhibit concerning behaviors. These include repeatedly rescheduling interviews, unclear communication, constant failure to use a webcam during virtual meetings, unsuccessful background checks, and discrepancies between their claimed skillsets and actual work performance.

[3] https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

GLOBAL EVENTS INFLUENCING CYBER ACTIVISM

Global events significantly influence cyber activism, often serving as catalysts for increased online activity and coordinated efforts by hacktivist groups.

Political upheavals, social justice movements, and international conflicts can drive cyber activists to target entities they perceive as responsible for injustices or to support causes they believe in. For instance, geopolitical tensions may lead to cyber-attacks on government institutions, while social movements might inspire campaigns against corporations or organizations seen as opposing the activists' goals. Additionally, global events such as pandemics or economic crises can exacerbate vulnerabilities, providing opportunities for cyber activists to exploit these situations to further their agendas.

Due to United States' influence in the world stage and its image as the forefront of Western ideology, it is a major target for cyber activists, also affecting U.S corporations.

KEY POLICY RECOMMENDATIONS AND CONSIDERATIONS:

Organizations should monitor global events influenced by U.S. policies and conduct risk assessment analyses. This is particularly important if certain executives or individuals affiliated with the organization have outspoken controversial or political opinions, as they may become targets of interest for cyber activists.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-37-286-777
17 Ha-Mefalsim St Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House,
14-18 Great Titchfield Street,
London, W1W 8BD

USA - TX

Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm