Secureworks®

Learning from Incident Response: January - March 2024

Secureworks® Counter Threat Unit™ Research Team

TABLE OF CONTENTS

SUMMARY

Secureworks® Counter Threat Unit™ (CTU) researchers analyzed data from Secureworks incident response (IR) engagements completed between January and March 2024. This data provided CTU™ researchers with insight into emerging threats and developing trends that organizations can use to guide risk management decision-making and prioritization.

The motivation and context for IR engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or the organization entering a sensitive operational period. As a result, observed threat types may not reflect the broader threat landscape. Despite these limitations, data from IR engagements reveals how threat actors breach networks, how this activity impacts affected organizations, and how the incidents could have been prevented.

KEY POINTS:

Despite law enforcement action against individual groups, the number of ransomware engagements remained high. Ransomware remains a major threat to organizations in all sectors.

Exploitation of vulnerabilities in internet-facing devices was the most frequently observed initial access vector (IAV) in Q1 2024. Publication of exploit code makes exploitation more accessible to a wider range of threat actors.

Patching vulnerable systems in a timely manner is an essential defense, as older vulnerabilities can still pose a risk to organizations.

OBSERVED TRENDS

CTU researchers examined the threat actors, engagement types, and IAVs observed in Q1 2024 IR engagements.

Engagement types

The most prevalent engagement type during Q1 2024 was ransomware (23%), followed by exploited vulnerability (17%) (see Figure 1). Web compromise and network compromise tied at 13%. The proportion of ransomware incidents was significantly higher than the 6% of engagements in Q1 2023. As in previous quarters, many incidents were detected at an early stage before the threat actor's intention was clear. Some ransomware incidents were contained before ransomware was deployed.

The 'other' category comprises activity that accounted for less than 5% of the engagements during the quarter. The breakdown of Secureworks IR engagements may not always correspond with the overall threat landscape or reflect the prevalence of the threat.

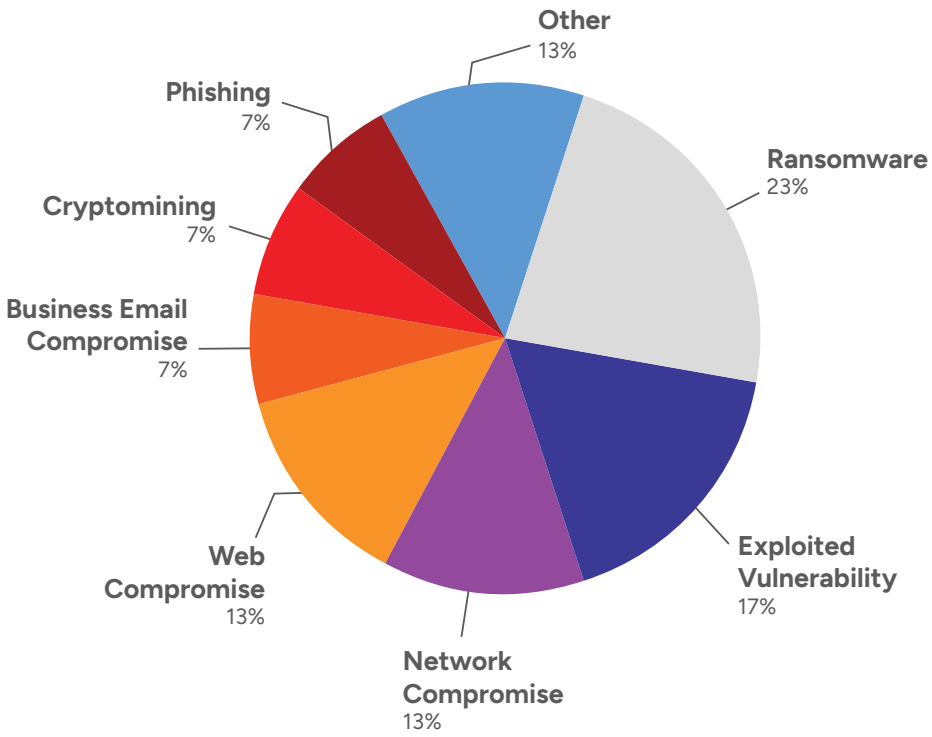

FIGURE 1. *IR engagement types in Q1 2024. (Source: Secureworks)*

Initial access vectors (IAVs)

The most frequently observed IAV by far in Q1 2024 was vulnerabilities in internet-facing devices, which accounted for almost two thirds (64%) of incidents (see Figure 2). Phishing and stolen credentials each accounted for 13%. These percentages represent a significant shift from Q1 2023, when phishing was the most prevalent IAV at 34%, followed by vulnerabilities in internet-facing devices at 17%. Threat actors regularly scan for vulnerable devices that are exposed to the internet, focusing on both newly disclosed and long-established flaws, reinforcing the importance of patching in a timely manner.

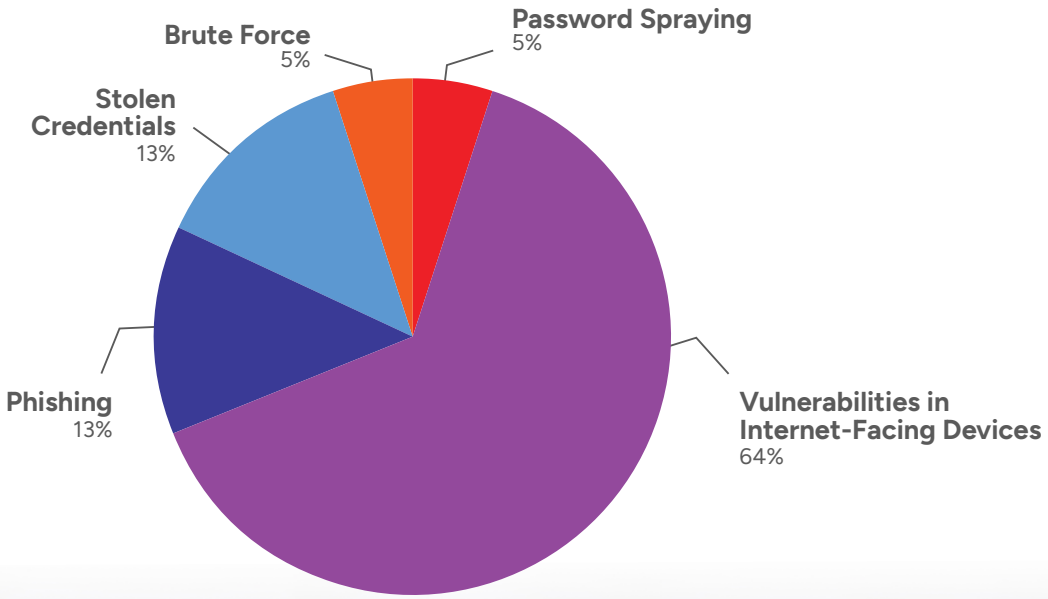

FIGURE 2. *IAVs observed in Q1 2024. (Source: Secureworks)*

Mapping IAVs to MITRE ATT&CK

Table 1 maps these IAVs to MITRE ATT&CK® categories. Organizations can use information from this knowledgebase to organize and operationalize threat intelligence data.

INITIAL ACCESS VECTOR (IAV)	MITRE ATT&CK MAPPING
Vulnerabilities in internet-facing devices	Exploitation of Remote Services Exploit Public-Facing Application
Phishing	Phishing Spearphishing Attachment
Stolen credentials	Valid Accounts
Brute force	Brute Force I/O
Password spraying	Password Spraying

TABLE 1. *Mapping IAVs to MITRE ATT&CK.*

CASE STUDIES

The following sections highlight notable observations from Q1 2024 IR engagements.

Ransomware continues to flourish

Despite disruptive law enforcement action against LockBit operator GOLD MYSTIC and an exit scam conducted by ALPHV (also known as BlackCat) operator GOLD BLAZER during the quarter, ransomware attacks continued to pose a significant threat to organizations. The number of victims listed on leak sites rose each month of the quarter, suggesting that disruption to one operation may simply lead to affiliates moving to other groups. Cyber insurers also noted the elevated Q1 2024 ransomware activity.

During Q1 2024 engagements, Secureworks incident responders discovered that attackers deployed or attempted to deploy ransomware variants such as LockBit, ALPHV, BlackByte (operated by GOLD LOTUS), Akira (GOLD SAHARA), Black Basta (GOLD REBELLION), INC (GOLD IONIC), and Black Suit (GOLD SOUVENIR). The use of highly prolific ransomware such as LockBit and ALPHV, longstanding lower-profile operations like BlackByte, and a relative newcomer like Black Suit that emerged in 2023 illustrates the breadth of the ransomware landscape.

The investigations revealed a range of IAVs. Exploitation of vulnerabilities in internet-facing devices and stolen credentials were the most common IAVs in the analyzed ransomware attacks. The combination of stolen credentials and single-factor authentication on internet-facing devices likely facilitated attackers' initial access in several incidents.

In one ALPHV deployment, the IAV was a Remote Desktop Protocol (RDP) server protected with only a username and password. RDP can be highly susceptible to compromises due to its weak authentication requirement. The threat actor also used RDP for lateral movement, as well as Advanced Port Scanner and SoftPerfect Network Scanner for discovery, PowerShell to download Cobalt Strike, PsExec to execute commands, and Mimikatz for credential harvesting. In addition, they attempted to exfiltrate data and disable Microsoft Defender. The attacker also created scheduled tasks for clearing activity logs to hide their actions and then deployed ransomware more than a month after gaining initial access to the environment.

RDP was also used for lateral movement in a separate incident that resulted in deployment of Akira ransomware on ESXi hosts. In this attack, the dwell time was only two days. The threat actor used Advanced IP Scanner for enumeration and both AnyDesk and MobaXterm for remote access. The attacker encrypted logs on the ESXi hosts as well as the most recent backups, which reduced the number of forensic artifacts available for analysis.

Mitigation

One essential mitigation in any ransomware engagement is to block the attacker's re-entry to the network; for example, by removing external access to appliances or hosts. In the ALPHV incident, the threat actor attempted to re-enter the environment the day after deploying the ransomware. The intent may have been to destroy logs and other forensic artifacts to complicate analysis and recovery. Attackers may also try to establish persistent access, leaving the victim susceptible to a future attack.

Other typical mitigations following ransomware attacks are performing global password resets to prevent reuse of stolen credentials and replacing single-factor authentication with multi-factor authentication (MFA). Organizations should also deploy extended detection and response (XDR) solutions to detect threat actor activity earlier in the attack chain.

Vulnerability disclosures attract all levels of threat actors

Exploitation of vulnerabilities in internet-facing devices was the IAV for several types of incidents during the quarter. Vulnerabilities in Ivanti Secure products (CVE-2023-46805, CVE-2024-21887) and Citrix NetScaler ADC and NetScaler Gateway appliances (CVE-2023-4966, dubbed 'Citrix Bleed') gained considerable media coverage, which likely prompted threat actors of all skill levels to attempt exploitation.

Threat actors can exploit Citrix Bleed to take control of legitimate sessions on NetScaler ADC and Gateway appliances, bypassing password entry and MFA. In one engagement, Secureworks incident responders discovered that the threat actor followed successful exploitation with multiple failed attempts to establish communication with a command and control (C2) server to download a Cobalt Strike payload. The threat actor did download a script to extract artifacts from an Active Directory (AD) environment but then failed to execute the script, map the AD environment, or obtain accounts that would be vulnerable to a Kerberoasting attack.

Secureworks incident responders also investigated multiple attacks in which successful exploitation of the Ivanti vulnerabilities was followed by additional malicious activity. One instance resulted in limited exfiltration of archived, non-sensitive data. In another incident that was likely part of a global campaign by suspected Chinese state-sponsored threat actor UTA0178, the attacker exploited CVE-2023-46805 and CVE-2024-21887 in tandem to modify a legitimate system file and create a backdoor on the system.

Older vulnerabilities were also represented in engagements completed in Q1 2024. For example, analysis of a cryptominer discovered in one customer network revealed that the web server was compromised via a Laravel debugging tool flaw disclosed in 2021 (CVE-2021-3129). Code and instructions for exploiting this vulnerability are widely available online.

Mitigation

Organizations should audit their environments and scan for known vulnerabilities. Timely patching also remains an essential defense. While the mean time to exploit "high-risk vulnerabilities" in 2023 was reportedly 44 days, this time is far shorter for high-profile issues. Once a vulnerability is disclosed, exploit code is often published within a few days and attackers of all skill levels attempt to compromise systems.

Prioritizing systems according to business risk can make patching more manageable. Perimeter devices appear to be increasingly targeted, so patching them is especially important. Even flaws that have been known for several years can still be exploited. The U.S. Cybersecurity Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities catalog lists vulnerabilities under active exploitation, which may help with prioritization. Implementing XDR solutions that monitor endpoints, networks, and cloud environments ensures that exploitation attempts are swiftly detected so they can be contained.

Email rules help hide phishing attacks

A customer discovered a suspicious email forwarding rule and a large volume of emails being sent from an internal account. Secureworks incident responders determined that the attack originated from phishing emails sent to several employee accounts. The emails contained a link to view documents on a file-sharing platform, and all the recipients clicked on the link and supplied their credentials. The threat actor circumvented the accounts' MFA by using an adversary-in-the-middle (AiTM) attack to steal session cookies for access.

The attacker then accessed SharePoint documents, created inbox rules, and granted consent to an application to enable full syncing of the victims' mailboxes to external devices. The threat actor also used one of the compromised accounts to send a high volume of phishing emails. Secureworks incident responders did not find evidence of explicit data exfiltration, but the email rules were designed to obscure activity.

Another IR engagement involving the abuse of email rules revealed that the attacker stole user credentials via a phishing attack. They then accessed the victim's account and created inbox rules to move certain incoming emails to the deleted folder. The threat actor used the stolen credentials to create an Adobe account and sent fake Adobe Sign documents to other employees to capture additional credentials. The email rule enabled the threat actor to reply to emails from recipients who questioned the validity of the Adobe Sign request. The attacker also deleted their original email to evade detection.

Mitigation

Both organizations disabled and reset compromised accounts after discovering the incidents. They also deleted phishing emails that remained in employees' inboxes. Secureworks incident responders advised the victims to enable and tune email rules for filtering potential phishing messages and to enable MailItemsAccessed auditing for users with sensitive data in their mailboxes. Reviewing logs to detect the addition of suspicious email forwarding or deletion rules can reveal malicious activity. Organizations should also consider implementing phishing-resistant MFA or a solution that uses number matching.

RECOMMENDATIONS

At the end of engagements, Secureworks incident responders provide advice to prevent further damage from the current incident and to defend against similar attacks. These recommendations may be useful to other organizations that experienced similar events. In Q1 2024, Secureworks incident responders most frequently issued the following recommendations:

- Enforce MFA on corporate systems and services. MFA implementations should be comprehensive and not leave gaps for legacy systems or administrator accounts.
- Regularly patch and update systems and applications.
- Rebuild or restore affected systems from known-good media to ensure that clean hosts and systems are reintegrated into the environment.
- Reset potentially compromised or exposed credentials. If appropriate, perform a global password reset.
- Implement an XDR solution across all endpoints, networks, and cloud resources.

CONCLUSION

CTU researchers track behaviors identified during IR engagements to develop an understanding of the nature and evolution of various threats. Through countermeasure development, periodic trend analysis, and ad-hoc tactical reporting on activity observed during IR engagements, CTU researchers and Secureworks incident responders continuously provide protection, insight, and guidance derived from real-world incidents to Secureworks customers.

About Secureworks Incident Response

The Secureworks incident response team provides a wide range of expertise, cyber threat intelligence, and purpose-built technologies to help organizations prepare for and respond to cyber incidents successfully. Secureworks can assist organizations with onsite or remote Incident Commanders in support of an incident response. Secureworks experts work closely with in-house teams via emergency incident response services, threat hunting assessments, tabletop exercises, and a range of other incident readiness services – all designed to help you build an incident response program and resolve incidents efficiently and effectively at scale.

About Secureworks

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

www.secureworks.com