Secureworks®

Learning from Incident Response: January - March 2023

Secureworks® Counter Threat Unit™ Research Team

TABLE OF CONTENTS

SUMMARY

Secureworks® Counter Threat Unit™ (CTU) researchers analyzed data from reactive Secureworks incident response (IR) engagements completed between January and March 2023. This data provided CTU™ researchers with insight into emerging threats and developing trends that customers can use to guide risk management decision-making and prioritization.

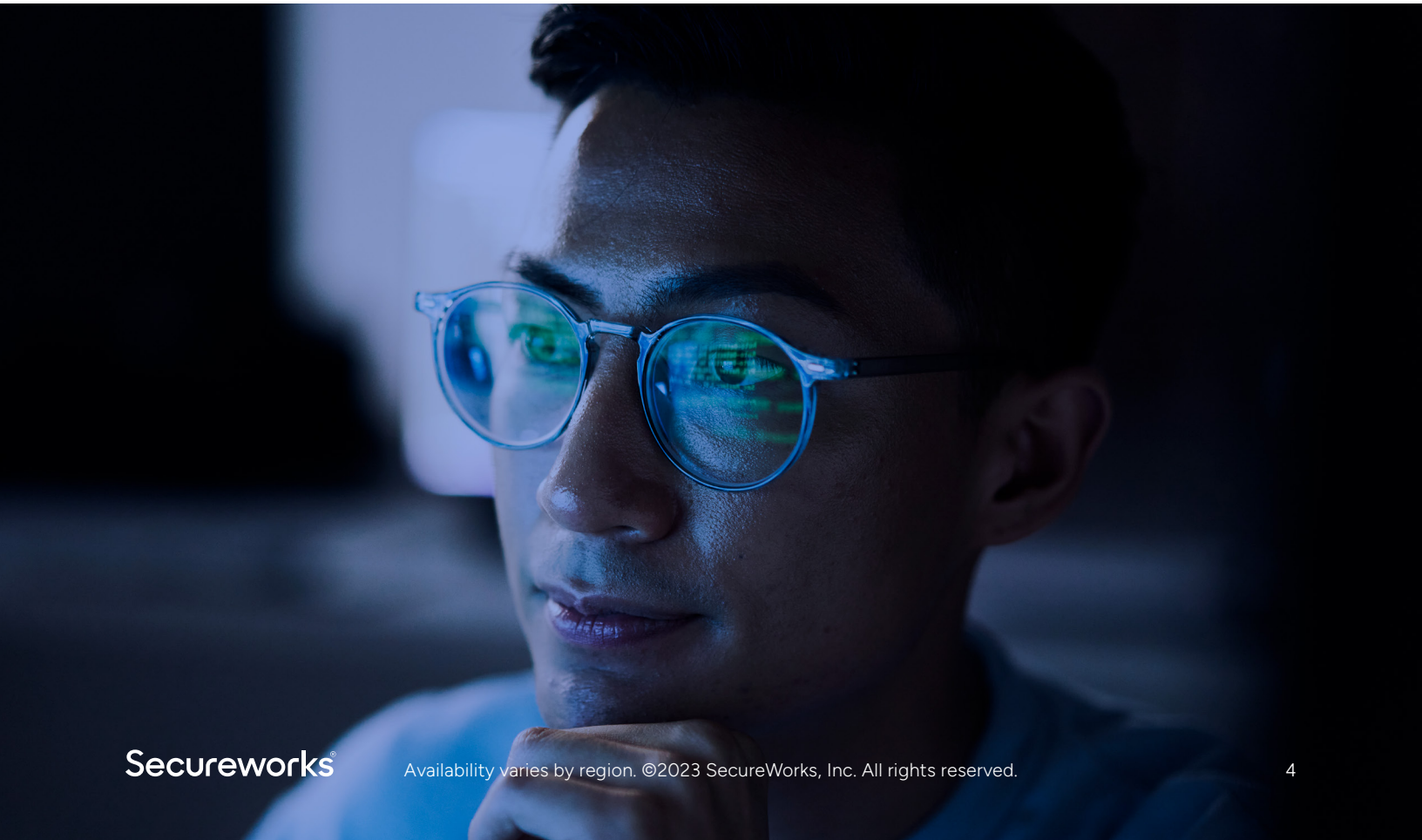
The motivation and context for IR engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or the organization entering a sensitive operational period. As a result, observed threat types may not reflect 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:

Early detection of malicious activity can stop malware infections from progressing to ransomware deployment.

The vast majority of cyberattacks observed by Secureworks incident responders are likely financially motivated. Both ransomware and business email compromise (BEC) remain major threats.

Phishing continues to represent the most significant initial attack vector (IAV).



OBSERVED TRENDS

CTU researchers examined the threat actors, engagement types, and IAVs observed in Q1 2023 IR engagements.

Engagement types

Malware infections comprised almost one-third of IR engagements during the quarter (see Figure 1). Network compromise was the second-largest type of engagement at 15%. The engagement type classifications can reflect the point at which the incident is detected. Some of the incidents in these categories might have progressed to ransomware attacks if they had not been detected and stopped at an early stage by the victim's extended detection and response (XDR) solution.

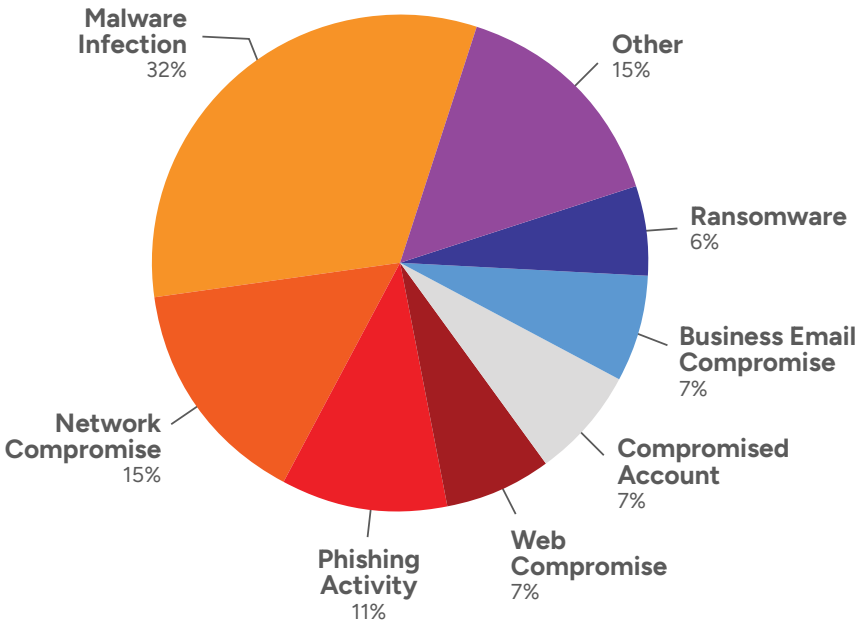


FIGURE 1. *IR engagement types in Q1 2023. (Source: Secureworks)*

The breakdown of Secureworks IR engagements during the quarter may not always correspond with the overall threat landscape or reflect the prevalence of the threat. For example, BEC accounted for a small percentage of Q1 2023 IR engagements, but it continues to pose a major threat to organizations. Similarly, ransomware remains a significant threat despite representing only 6% of the incidents investigated during the quarter. According to the U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), ransomware reports decreased in 2022. However, early-stage detection of precursor activity may have prevented ransomware deployment. In addition, some victims do not report incidents or retain IR services, meaning that actual number may be higher. CTU tracking of leak sites indicates that name-and-shame ransomware remains active. Organizations must continue to implement security controls and training to address these threats.

Initial access vectors

Phishing was the most frequently observed IAV (see Figure 2), accounting for 34% of Secureworks engagements this quarter. The second most prevalent IAV was exploitation of vulnerabilities in internet-facing devices at 20%. The proportion of drive-by downloads (17%) was a significant increase over 2022, when it comprised only 2% of IR engagements across the entire year. This increase may reflect financially motivated threat actors' growing interest in the use of SEO poisoning. During Q1 2023, drive-by downloads led to malware infections and network compromises.

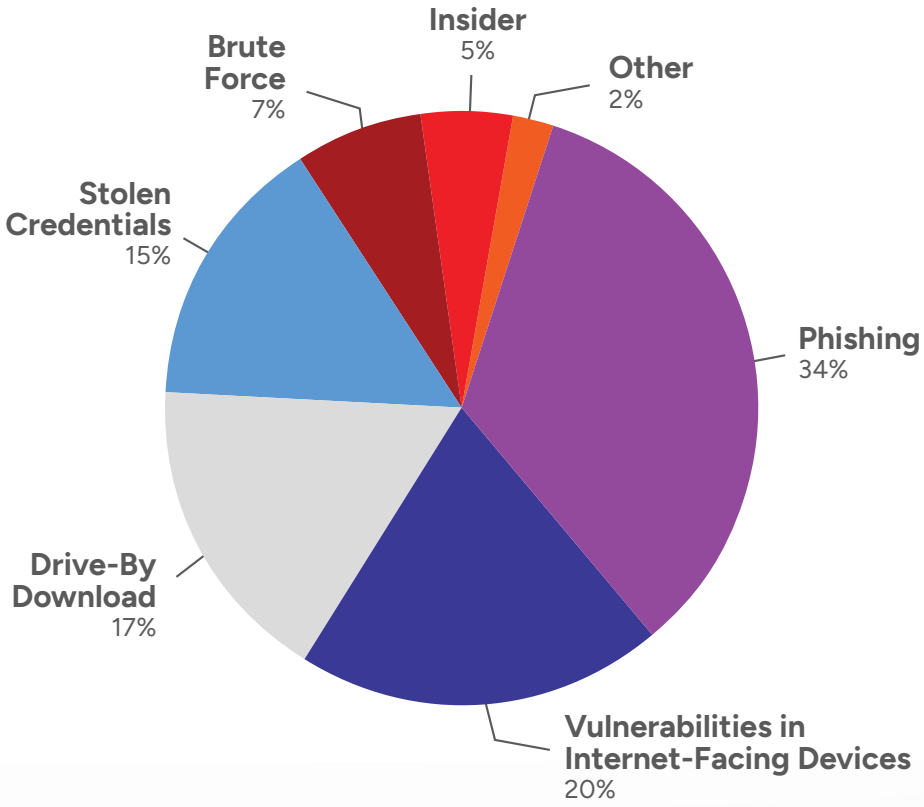
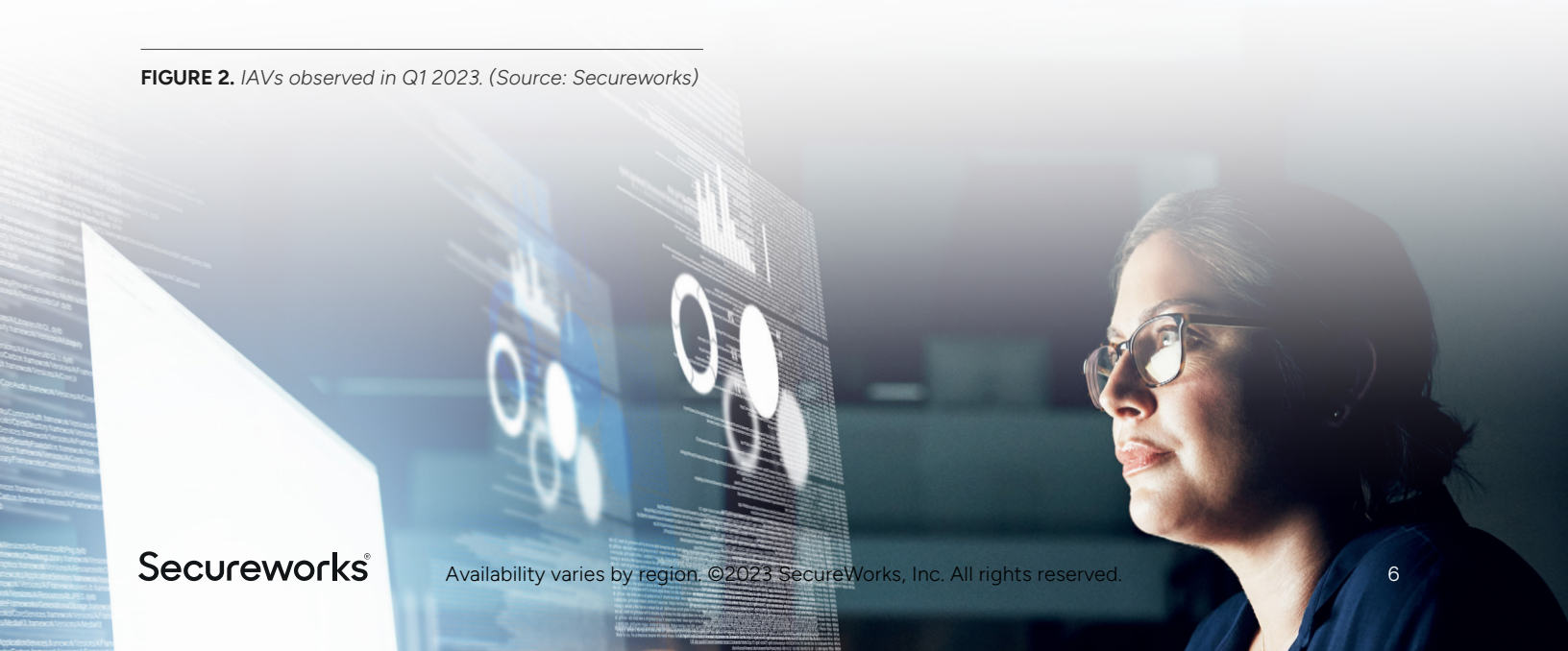


FIGURE 2. *IAVs observed in Q1 2023. (Source: Secureworks)*



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
Phishing	Phishing Spearphishing Attachment
Vulnerabilities in internet-facing devices	Exploitation of Remote Services Exploit Public-Facing Application
Drive-by download	Drive-by Compromise
Stolen credentials	Valid Accounts
Brute force	Brute Force
Insider	Replication Through Removable Media

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

CASE STUDIES

The following sections highlight notable observations from Q1 2023 IR engagements.

BEC actor abused MFA implementation gap

Secureworks incident responders investigated an incident where a BEC actor distributed a malicious document via internal email. The threat actor then posed as a senior executive to send text messages to employees' personal cell phones and request gift cards. The investigation highlighted issues that organizations should consider when implementing multi-factor authentication (MFA).

The attacker initially authenticated to an employee's Microsoft 365 (M365) account using credentials they had previously obtained from an unknown source. The authentication originated from a network address associated with a public virtual private network (VPN) service. Although the account was protected with MFA, the employee's acceptance of the attacker-generated MFA request gave the threat actor access to the account.

The threat actor made several attempts to distribute a malicious file to gain access to other employees' accounts by uploading a file to the compromised user's SharePoint, renaming it, and sharing it. Microsoft Defender Advanced Threat Protection (ATP) flagged the file and classified it as a Phish_PDF_MacLer_A malware sample. This detection made the link inaccessible to the recipients.

After sharing the linked file, the attacker followed up with an email asking if the recipients received the link and were able to access the shared file. On discovering that the link was inaccessible, the threat actor created a malicious inbox rule to delete messages mentioning 'Sharepoint' or 'file.' They then uploaded a new file and successfully re-shared it.

Two employees opened the file. One employee's account was protected with MFA, but the other account was not. The threat actor authenticated to the unprotected account and then posed as this employee to send texts requesting gift cards.

Organizations could mitigate BEC attacks by comprehensively implementing MFA across all user accounts, including senior executives' accounts, and training employees not to accept MFA requests they did not generate.

Use of corporate devices to access personal resources led to malware

Secureworks incident responders investigated several incidents during the quarter where an employee accessing personal or non-work resources from a corporate device resulted in a malware infection or compromise. One compromise began with an individual using a corporate laptop to read personal email and clicking a link that downloaded and executed a Qakbot malware variant. The email message was manipulated to appear that it was part of an existing business-themed email thread, although it was sent to the recipient's personal email account and was not relevant to their employment. Clicking a link in the email led to a download that culminated in obfuscated Qakbot code loading and running on the victim's system.

Qakbot then downloaded additional malware that allowed the threat actor to execute network reconnaissance commands. Approximately 20 minutes later, the attacker used a privileged user account to remotely execute Cobalt Strike on at least three domain controllers. Then they leveraged the impacted systems to deploy Cobalt Strike throughout the environment, ultimately compromising numerous systems across multiple countries. In addition, Cobalt Strike enabled the threat actor to obtain user account information and password hashes for all accounts within the domain, putting all user account passwords at risk. The attack took just over one day from the initial download.

In another incident, two malicious files detected on a compromised host ('123.txt' and '123.bat') contained the same contents: '%0 |%0.' Known as a fork bomb, this technique

continuously spawns processes and repeatedly executes the file. Fork bombs consume system resources and slow down the system, sometimes leading to a system crash. Analysis suggests that the fork bomb was created when the victim visited a puzzle site and downloaded what they believed to be puzzle code.

In a third incident, a user downloaded and opened a ZIP archive file containing adult content on a corporate device. Although the user deleted the files, an additional malicious file containing Raspberry Robin malware had been created seconds after opening the downloaded content. This malware executed twice, generating traffic from the host to the Tor anonymity network.

While it may not be practical or desirable to prevent employees from accessing non-work resources on corporate devices, monitoring downloads and using application allowlisting solutions could have prevented these incidents from creating malicious files on the system.

Malicious OneNote file led to Black Basta ransomware incident

One Secureworks IR engagement revealed that a threat actor inserted a malicious email into an existing legitimate email thread to deliver Qakbot. The sender posed as a third party known to the recipient, although there was no attempt to disguise the actual sender's email address and it visibly belonged to a different individual and domain. The email contained a malicious OneNote file attachment. When the recipient downloaded and executed the attachment, batch scripts and PowerShell downloaded and executed a Qakbot payload. This infection chain allowed the attacker to remotely access the compromised system.

The presence of Qakbot triggered Microsoft Defender alerts, which caused the payload file to be quarantined. Nonetheless, the threat actor was able to continue the compromise, downloading tools for reconnaissance, privilege escalation, and lateral movement. The AdFind.exe command-line query tool queried Active Directory, and Base64-encoded PowerShell launched a reconnaissance-related function to discover accounts with local administrator access.

The attacker logged on to one of the two servers in the environment via an Administrator account and installed the ScreenConnect remote desktop tool. This tool provided an additional foothold and allowed persistent and direct access to the compromised host after rebooting. After 15 hours of inactivity, the threat actor then installed additional tools and services on the originally compromised host and the server. These tools included the PSEXESVC service, which is created when the PsExec remote access tool executes a command on the system. Finally, the attacker connected to the second server. Both servers were encrypted with the Black Basta ransomware operated by the GOLD REBELLION threat group, and the ransom note was created. This incident continues a trend Secureworks incident responders observed in late 2022 of multiple engagements involving Qakbot leading to Black Basta deployment.

RECOMMENDATIONS

At the end of engagements, Secureworks incident responders provide customers with proactive recommendations to reduce the chance of similar incidents in the future, as well as remediation advice to prevent further damage from the current incident. General proactive recommendations reflect good security practices relevant to most organizations:

- Enforce MFA for access to corporate systems and services. Comprehensive enforcement of MFA across all accounts and platforms helps prevent threat actors from successfully using stolen credentials. Implementing phishing-resistant MFA that incorporates number matching, geolocation validation, or PKI adds extra protection.
- Develop and implement security awareness training. A relevant and accessible training program helps users understand the role they play in limiting the impact of cybersecurity breaches.
- Conduct regular internal and external penetration tests and vulnerability scans. Penetration testing lets organizations understand possible attack vectors and security weaknesses from the perspective of a potential attacker.
- Regularly patch and update systems and applications.
- Implement full endpoint, cloud, and network traffic monitoring.

Secureworks incident responders also issue specific proactive advice relevant to each engagement. The case studies in this report prompted the following recommendations:

- Implement an allowlisting policy and solution for software and website access to limit exposure to unwanted and malicious programs and content. Perform comprehensive testing before deploying any solution.
- Conduct phishing simulation exercises to help users avoid falling victim to malicious emails.
- Implement web filters to restrict users from accessing personal email accounts or other non-work content.
- Ensure that local administrators have separate credentials for their standard and administrative activities to make it difficult for threat actors to elevate privileges.

The following were the most common remediation recommendations Secureworks incident responders gave in Q1 2023:

- Reset any potentially compromised or exposed passwords and credentials. This action prevents the attacker from reusing the credentials to regain entry or from sharing them with other threat actors.
- Rebuild or restore affected systems and hosts from known-good media.
- Reset the KRBTGT (Kerberos Ticket Granting Ticket) service account if the attacker could have accessed it.

CONCLUSION

CTU researchers track threats and 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.

Secureworks®

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 (subject to applicable pandemic travel restrictions) 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 protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

www.secureworks.com