Secureworks®

Learning from Incident Response: April - June 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 April and June 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.

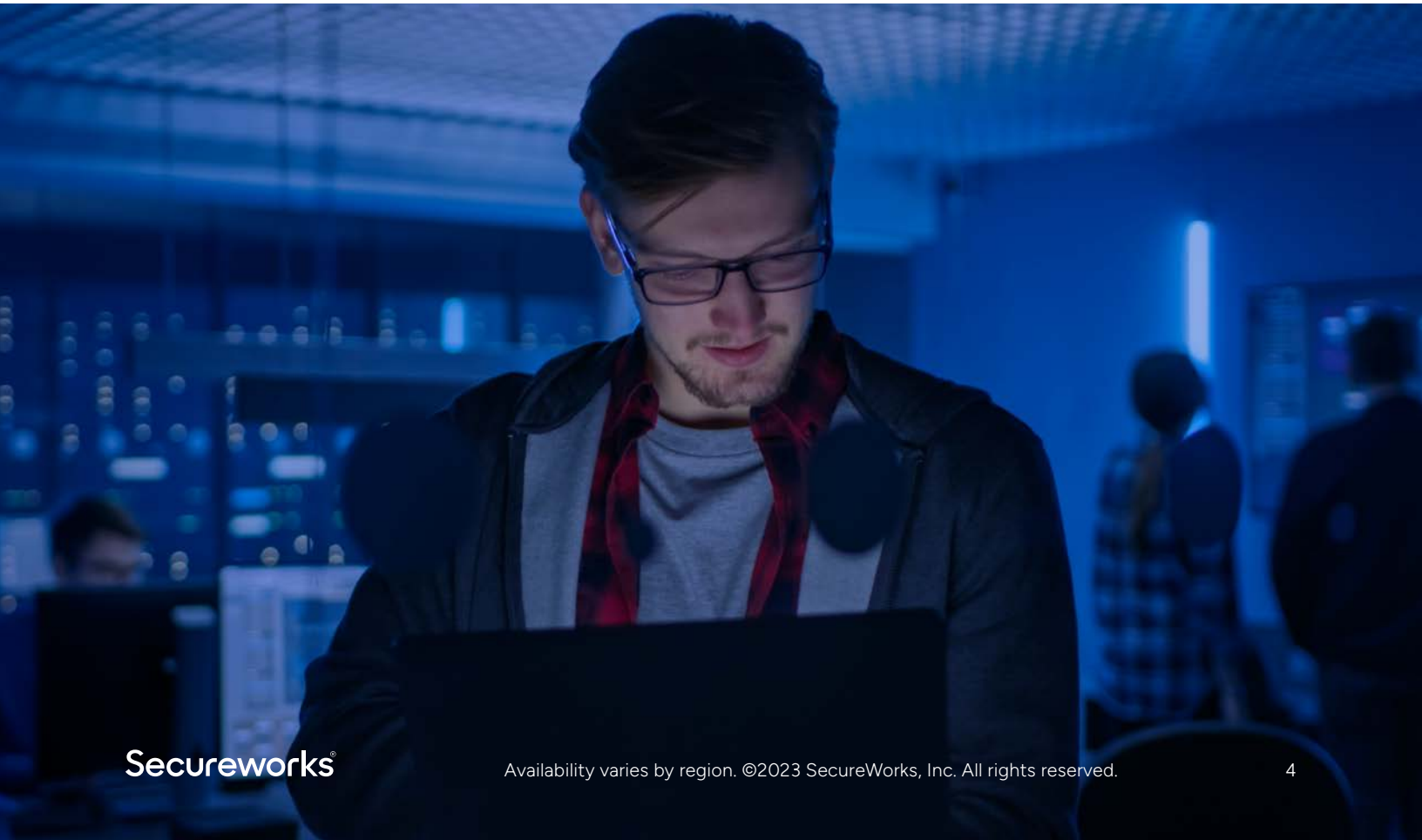
The motivation and context for IR engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or the organization entering a sensitive operational period. As a result, observed threat types may not reflect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

The proportion of Secureworks IR engagements involving ransomware more than doubled compared to the first quarter of 2023.

After establishing access to a network, threat actors may wait months or even years before returning and continuing their malicious activities.

Logs provide valuable insights into incidents. Increasing log retention periods can help incident responders during their investigations and can also contribute to preventing repeat attacks.



OBSERVED TRENDS

CTU researchers examined the threat actors, engagement types, and initial access vectors (IAVs) observed in Q2 2023 IR engagements.

Engagement types

The most prevalent engagement type in Q2 2023 was 'compromised account', which accounted for 26% of intrusions (see Figure 1). Typically, this category represents a compromise detected at an early stage via monitoring solutions such as Secureworks Taegis™. Undetected, these compromises could have led to ransomware deployment, business email compromise (BEC), or cyberespionage.

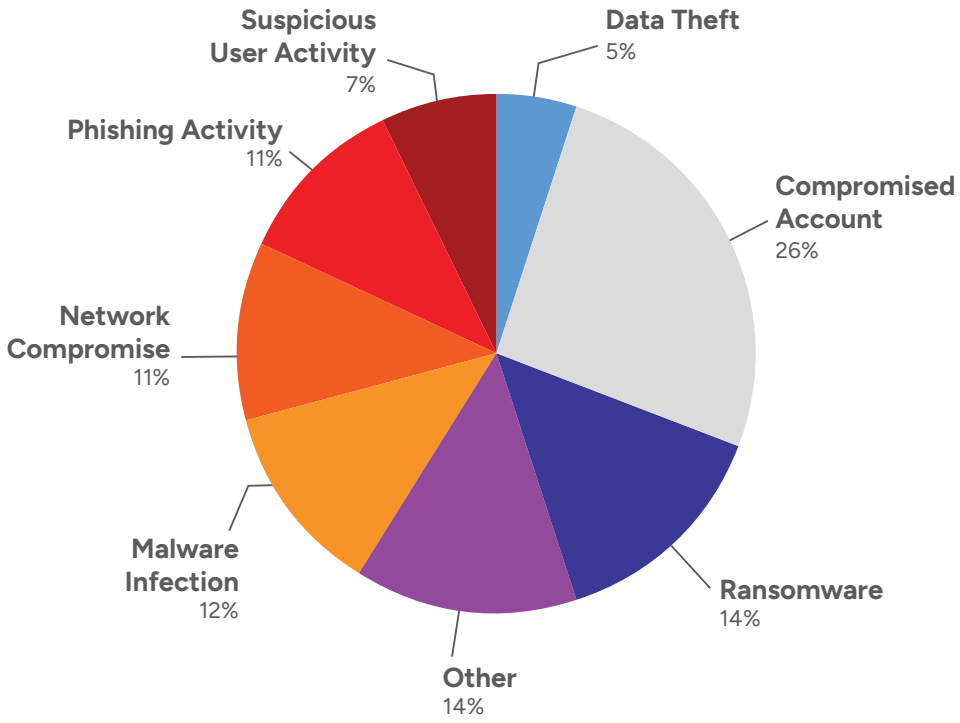


FIGURE 1. *IR engagement types in Q2 2023. (Source: Secureworks)*

Ransomware represented 14% of engagements, which is a significant increase over the 6% in Q1 2023. This increase aligns with a higher number of victims published to leak sites in Q2 2023 compared to the two previous quarters.

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. For example, BEC is included in the 'other' category for Q2 2023 but continues to pose a major threat to organizations.

Initial access vectors (IAVs)

Phishing and exploitation of vulnerabilities in internet-facing devices remained the most frequently observed IAVs. The proportion of both of these IAVs was higher than in Q1 2023. However, the percentage of engagements involving phishing only increased slightly while exploitation of vulnerabilities grew from 20% to 32%. Threat actors may use either of these IAVs in attacks involving credential theft, malware deployment, ransomware, or data exfiltration.

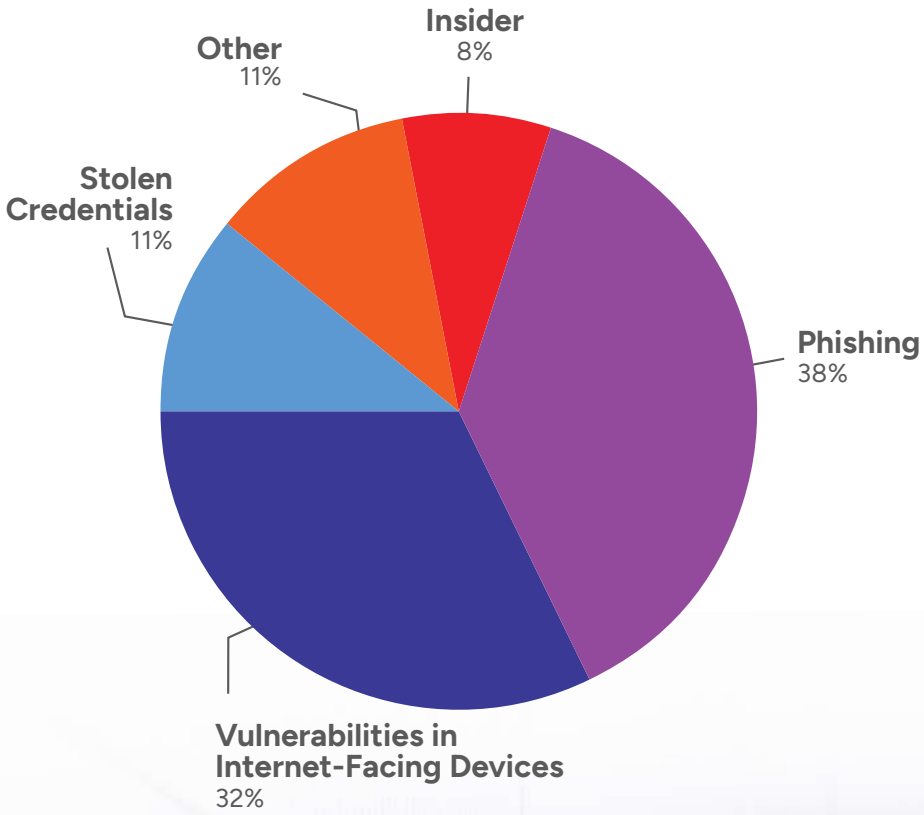


FIGURE 2. *IAVs observed in Q2 2023. (Source: Secureworks)*

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
Stolen credentials	Valid Accounts
Insider	Replication Through Removable Media

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

CASE STUDIES

The following sections highlight notable observations from Q2 2023 IR engagements.

Ransomware actor deleted logs to frustrate investigation

Secureworks incident responders investigated a ransomware incident after the victim discovered encrypted files within their server environment. The investigation revealed that an unauthorized user obtained access to the victim's environment, likely via a VPN, and established a remote desktop session to a domain controller. From there, they conducted network discovery activity. Two days later, the attacker installed and then immediately uninstalled a cloud hosting app from the domain controller, deleting the app's logs in the process. Threat actors typically use this application to exfiltrate data.

The next day, the threat actor established a remote desktop session from the same domain controller to an endpoint, installed the cloud hosting app on the endpoint, and used the app to upload multiple files to cloud-based servers. They then leveraged the domain controller to establish remote desktop sessions to other systems throughout the environment. The attacker executed a Zeppelin ransomware executable on the domain controller before pushing the ransomware to other systems. Zeppelin was one of the ransomware variants deployed by the financially motivated GOLD VICTOR threat group during its operation of the Vice Society name-and-shame scheme. The group rebranded its operations as Rhysida in June.

Analysis of this Zeppelin sample revealed capabilities for clearing host-based logs, likely to frustrate incident response. However, the process was not entirely successful. After the ransomware was deployed, some remaining host-based logs identified a remote desktop session that was terminated from an IP address likely associated with the victim's VPN pool. This evidence suggests that the threat actor may have used the VPN to access the environment.

Fraudulent login attempts generated "impossible travel" alerts

A combination of Microsoft 365 portal alerts for impossible travel and fraudulent text messages containing links to a credential-harvesting website alerted a multi-national organization to an incident. The Secureworks IR investigation revealed that the attack started with multiple failed authentication attempts originating from countries far from the legitimate user's location. The Microsoft 365 portal flagged the attempts for impossible travel and because the locations were previously linked to malicious activity.

A month later, a threat actor leveraged an IP address associated with yet another country and attempted to authenticate to a Microsoft 365 account associated with another employee of the compromised organization. This account was protected by multi-factor authentication (MFA), but the threat actor's MFA fatigue attack caused the user to eventually approve an MFA request. After gaining access to the account, the attacker registered several devices within the victim's environment and began to view corporate SharePoint documents. These documents contained information such as VPN instructions and employee phone numbers.

During a five-month period, the threat actor successfully logged into several Microsoft 365 accounts and conducted follow-on activity from some of them. The attacker also established a number of VPN sessions using their own device and the second account. These sessions originated from IP addresses registered on several different continents.

Toward the end of their time on the network, the threat actor again used the second account to upload a web page to the victim's SharePoint directory. The attacker then sent text messages to multiple other employees directing them to this fake corporate-branded login page. The submitted credentials were transmitted to the threat actor via Telegram.

A separate Secureworks IR engagement involved a threat actor compromising an account and then sending phishing emails to other employees in the victim's network inviting them to view a document. By the time the organization detected the campaign, multiple users had clicked on the link contained in the email and supplied their credentials. CTU analysis confirmed that the link embedded in the email had been used in previous phishing campaigns.

In addition, log analysis revealed multiple login attempts from foreign IP addresses to accounts that normally only received local logins. The logs also showed that the threat actor focused on legacy authentication protocols for initial access, bypassing MFA. It was not clear exactly when the fraudulent login attempts began, as the logs no longer existed due to the organization's log retention policy.

Attackers waited three years before making virtual storage inaccessible

Three years after first obtaining access to an organization's network via a standalone server, a threat actor altered the settings of a storage device on the network. This change prevented the victim from accessing their virtual machines (VMs).

Secureworks incident responders discovered that several years ago, a threat actor made several Remote Desktop Protocol (RDP) connections from a U.S. IP address to a host in the victim's network. The threat actor then installed a legitimate remote management tool as a service. Three years later, a threat actor used this service to connect to the host from an Italian IP address, and then made a successful RDP connection to an Administrator account. Several more connections to the same host from different IP addresses occurred over the next few days. Then after a ten-day gap, the threat actor connected again and conducted several activities using the Administrator account, including browsing the internet, accessing directories and documents, and executing programs. The browsing included research into how to interact with the organization's storage device.

Two months later, after making additional remote management and RDP connections to the Administrator account from Russia-based IP addresses, the threat actor uninstalled the remote management tool from the originally compromised host. They then logged into the storage device several times using the Administrator account. Two days later, the threat actor logged in from an Italian IP address and altered the storage device's IP address configuration settings, making the VMs inaccessible. Secureworks incident responders did not observe evidence of data exfiltration from the storage device or the host. It is unclear why the threat actor waited three years to sabotage access to the victim's VMs.

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. In Q2 2023, the most commonly issued standard recommendations were to enforce MFA across all accounts and platforms, to reset potentially compromised or exposed credentials to prevent attacker reuse, and to develop and implement security awareness training at all levels of the organization. Additional advice included deploying endpoint detection tools throughout the environment, conducting regular penetration tests and vulnerability scans, and maintaining a regular and timely patching program.

The case studies in this report prompted the following specific recommendations to remediate these incidents and avoid similar attacks in the future. This advice may be relevant to other organizations.

- Remove local administrator permissions to limit the level of access a threat actor can obtain during a compromise. If disabling local administrator rights is not feasible, require additional authentication checks and frequent reauthentication on these accounts.
- Following a compromise of Microsoft Entra ID (formerly Azure Active Directory), revoke refresh tokens for all impacted users in the tenant. Changing passwords will not automatically revoke these tokens, so a threat actor could continue to access authorized applications.
- Only allow software necessary for business purposes. Using software inventory tools, maintain an up-to-date inventory of authorized software that is required in the enterprise for any business purpose on any corporate system.
- Determine which logs are appropriate to collect based on the organization's network environment and risk assessment, and retain logs for a minimum of one year. The National Institute of Standards and Technology (NIST) published detailed guidance on log management.

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 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