Secureworks®

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

Many observed malware infections were linked to drive-by downloads and SEO poisoning. Preventing employees from visiting unauthorized websites can greatly reduce the risk of these infections.

Phishing remains a popular initial access vector for cybercrime and state-sponsored attacks.

Phishing kits can help threat actors conduct adversary-in-the-middle (AiTM) attacks to steal tokens and bypass multi-factor authentication (MFA).

OBSERVED TRENDS

CTU researchers examined the threat actors, engagement types, and initial access vectors (IAVs) observed in Q2 2024 IR engagements.

Engagement types

The most prevalent engagement type during Q2 2024 was malware infection (19%), followed by ransomware (16%). These results reflect a change from Q1 2024, when malware infections were included in the 'other' category because they represented less than 5% of engagements. The percentage of ransomware incidents dropped from 23% in Q1 to better align with the proportion recorded in Q2 2023. Business email compromise more than tripled to 11%, reflecting that this type of attack remains a threat to most businesses. As in previous quarters, many incidents were detected at an early stage before the threat actor's intention was clear.

The 'other' category comprises types that individually 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.

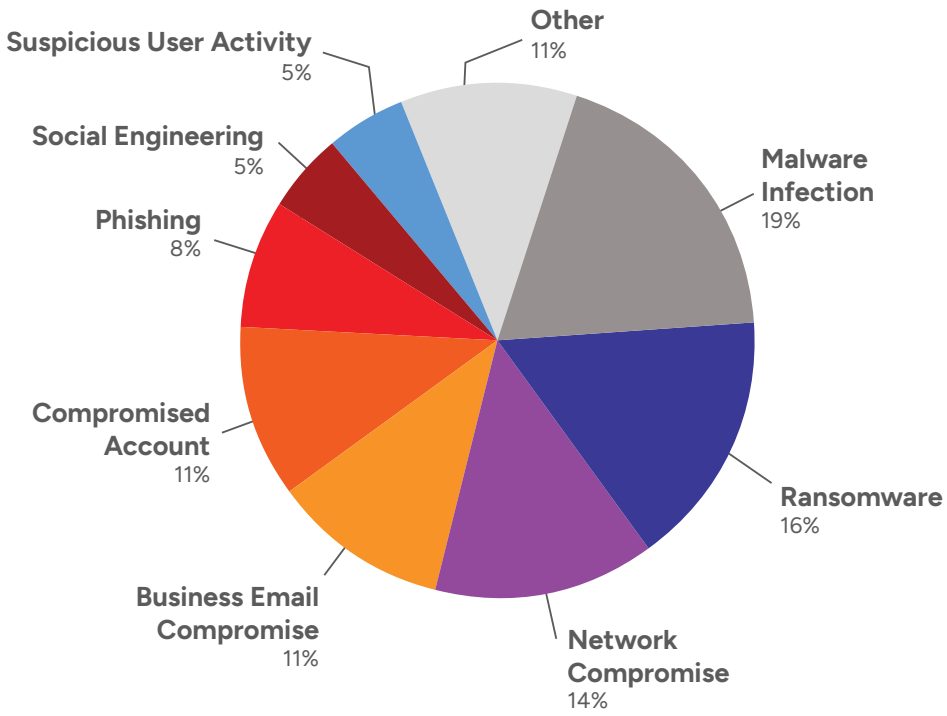


FIGURE 1. *IR engagement types in Q2 2024. (Source: Secureworks)*

Initial access vectors (IAVs)

Phishing provided initial access in 33% of Q2 2024 engagements, compared to 13% in Q1. It remains a useful technique for both state-sponsored threat actors and cybercriminals. The proportion of incidents using stolen credentials as an IAV also increased, from 13% in Q1 to 22% in Q2. By contrast, exploitation of vulnerabilities in internet-facing devices dropped from 64% to 19%. Drive-by downloads came fourth at 15%, but this IAV was most closely associated with the rise in malware infection incidents.

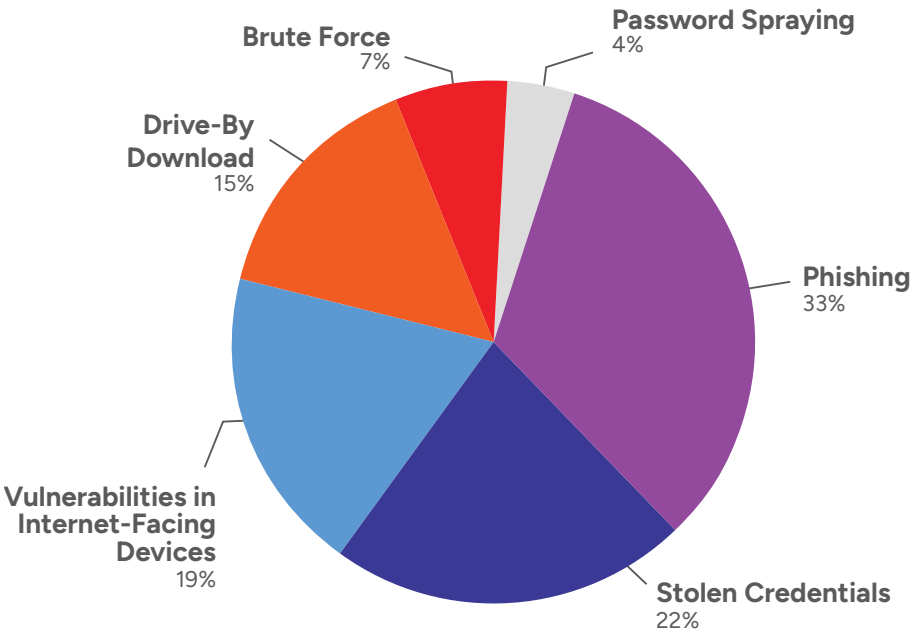


FIGURE 2. *IAVs observed in Q2 2024. (Source: Secureworks)*

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
Phishing	Phishing Spearphishing Attachment
Stolen credentials	Valid Accounts
Vulnerabilities in internet-facing devices	Exploitation of Remote Services Exploit Public-Facing Application
Drive-by download	Drive-by Compromise
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 Q2 2024 IR engagements

SEO poisoning leads to malware infections

Secureworks incident responders often discover Gootloader on victims' systems when investigating malware infections. This widely used first-stage downloader operated by the GOLD ZODIAC threat group is frequently delivered via drive-by downloads when search engine optimization (SEO) poisoning or malvertising directs victims to compromised WordPress websites. Since January 1, 2024, Secureworks tracking systems have directly observed over 4,500 Gootloader-infected websites on the internet, and the total number is likely significantly higher.

GOLD ZODIAC typically targets victims who search for legal phrases or resources (e.g., legal contract templates). However, the legal aspect was more tangential in one Gootloader incident investigated during the quarter. When casually browsing for information about nutritional supplements, an employee visited a link related to a controversial anti-aging supplement. They downloaded a ZIP archive file that ostensibly contained information about the supplement's legality in their country, but it actually contained malicious JavaScript that caused the infected endpoint to contact multiple malicious URLs before dropping a second malicious JavaScript file. Fortunately, the organization had installed an endpoint agent on the system, and the early detection allowed the incident to be contained before it spread to other hosts.

Another incident involving SEO poisoning occurred when an employee was temporarily granted local administrator access to enroll their device in the organization's endpoint management platform. During that period, a Google search for a high-profile legitimate website directed the employee to a spoofed website where they unwittingly downloaded a malicious file. Executing the file ran a PowerShell script to download and install the NetSupport remote access tool. The employee then returned to the malicious website, downloaded the same malicious file, and executed it again. This behavior suggests that the file masquerading as a legitimate download did not behave as anticipated. Microsoft Defender alerted on the execution of the script, but NetSupport had already been installed. A few minutes later, two PowerShell scripts were executed on the host, each via a command that allowed the script to bypass restrictions when run. These scripts created a loader as well as a scheduled task that enabled persistence.

Mitigation

User education is an important mitigation against SEO poisoning, but it is not enough. Security controls are essential, either to prevent unauthorized files from being downloaded or to stop them from harming the system. Organizations could completely restrict access to websites that are not on their allow list, block all downloads from unauthorized sources, or block specific types of downloads associated with common attacks. For example, Gootloader is frequently delivered via ZIP files. In addition, permissions could be adjusted to prohibit JavaScript downloads as most employees do not have a business need to download those types of files. Alternatively, the default application for opening JavaScript files could be changed to a text editor, preventing them from accidentally being executed. Implementing application allowlisting can prevent the execution of unauthorized executables, DLLs, scripts, and installation packages, greatly reducing threat actors' ability to execute malicious code on workstations and servers. However, testing and deploying application allowlisting may incur significant implementation and management costs.

Network segmentation limited scale of ransomware attack

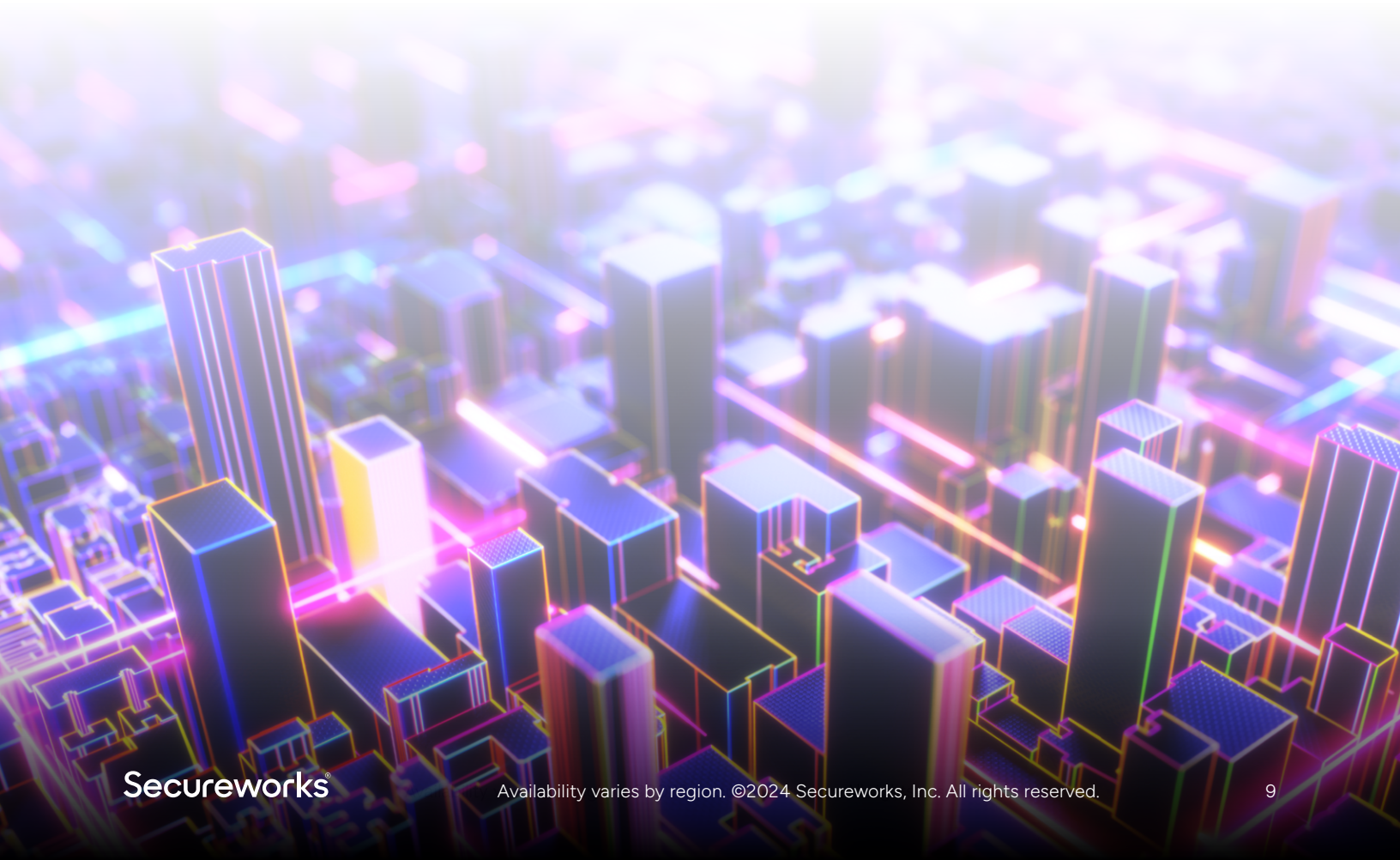
Network-attached storage (NAS) devices are often targeted by ransomware groups for encryption. During the quarter, Secureworks incident responders discovered that files hosted on a victim's NAS device were encrypted with Faust ransomware. Faust is likely a Phobos ransomware variant.

The threat actor gained initial access by conducting a brute-force attack against a Remote Desktop Protocol (RDP)-enabled host that was exposed to the internet, ultimately succeeding via the admin account. The attacker then deployed tools used by Phobos affiliates to harvest credentials, escalate privileges, scan the network, and disable antivirus software. The threat actor mapped multiple directories of the NAS disks as network shares and then executed the ransomware on the original host and the mapped NAS drives.

There was no evidence of data exfiltration, and the ransomware group is not known to operate a leak site. The scale of the attack was limited because the host was not on the main corporate network, making lateral movement extremely difficult.

Mitigation

Threat actors regularly use tools such as Shodan to scan for devices that are inadvertently exposed to the internet. To limit future risk, Secureworks incident responders advised the victim to regularly conduct scans to identify misconfigured devices on their networks before threat actors discover them. Devices that need to be externally accessible should be protected with multi-factor authentication (MFA). Replacing default manufacturer passwords with strong credentials for administrator accounts is another essential measure.



AiTM phishing kits facilitate MFA bypass

The increased use of adversary-in-the-middle (AiTM) techniques to bypass MFA is cause for concern. Threat actors conduct AiTM attacks by deploying a reverse proxy server that hosts a spoofed Microsoft 365 sign-in page and then sending phishing emails that contain a link to the page. This process allows them to steal both credentials and MFA tokens Threat actors can obtain phishing kits from underground forums to make these attacks easier to execute.

One Secureworks IR engagement revealed that the threat actor conducted an AiTM attack, authenticated to the victim's account using the stolen session token, and enrolled their own mobile device in the MFA implementation for persistent access. The attacker then sent phishing emails to external users and created an inbox rule to automatically delete emails that contained a specific header. Threat actors typically utilize inbox rules to hide their activities from the victim. The phishing emails prompted recipients to click a malicious link and enter their credentials to view a document.

Secureworks incident responders observed a similar attack chain in a separate incident. The threat actor created an inbox rule to delete emails from a specific domain and then synced invoice-related emails to their own device. The attacker then used the compromised account to send phishing emails. The similar layout and wording of the phishing emails in both incidents suggest that the threat actors used a phishing kit.

Mitigation

In addition to implementing phishing-resistant MFA to protect against AiTM attacks, organizations can conduct email scanning that detects and blocks phishing emails. Security training should also educate employees about how to recognize and report phishing emails. Additionally, organizations should establish alerts for activity that suggests that a threat actor has gained access to an MFA-protected account. For example, impossible travel alerts could detect login activity from different geolocations that could not be traversed within the elapsed timeframe.

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 Q2 2024, Secureworks incident responders most frequently issued the following recommendations:

- Enforce MFA on corporate systems and services, including web and cloud applications, VPN access, perimeter devices, and social media accounts. MFA implementations should be comprehensive and not leave gaps for legacy systems or administrator accounts.
- Rebuild or restore affected systems from known-good media to ensure that clean hosts and systems are reintegrated into the environment.
- Configure or enhance event logging. Comprehensive logging makes it easier to trace the cause of a compromise.
- Reset potentially compromised or exposed credentials. If appropriate, perform a global password reset.
- Implement an extended detection and response (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.

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 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