Secureworks®

Learning from Incident Response: July – September 2023

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 July and September 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.

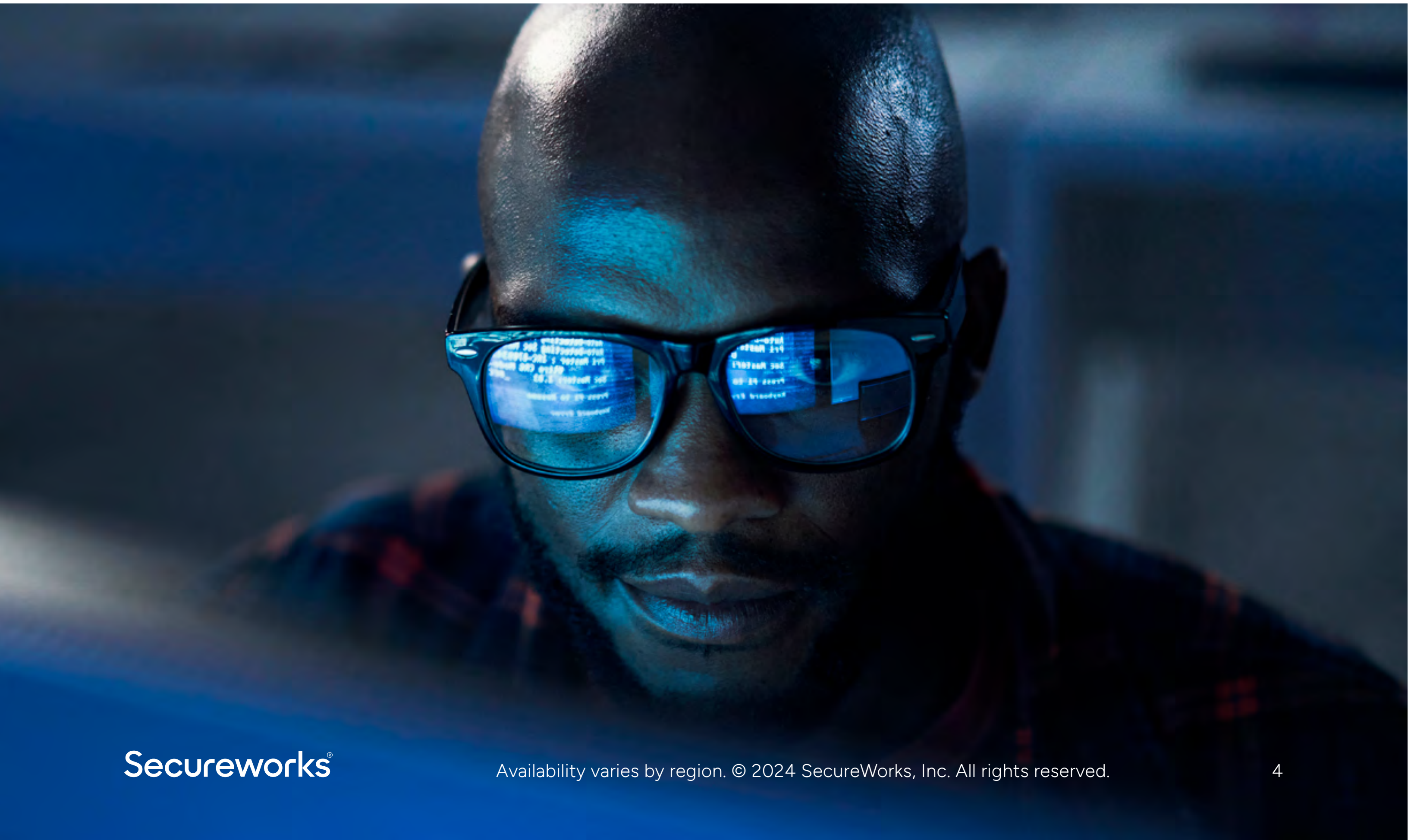
The motivation and context for IR engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or the organization entering a sensitive operational period. As a result, observed threat types may not reflect 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 prevalence of business email compromise (BEC) engagements increased during the quarter. Techniques used to dupe victims vary in complexity. Simpler techniques may be detectable via visual inspection of the email, including the sender's address.

Ransomware continued to account for multiple engagements. Early-stage detection and swift remediation can prevent ransomware attacks from progressing to encryption.

Organizations should consider implementing application control features such as AppLocker to limit the risk of employees downloading malicious documents from websites promoted via search engine optimization (SEO) poisoning.

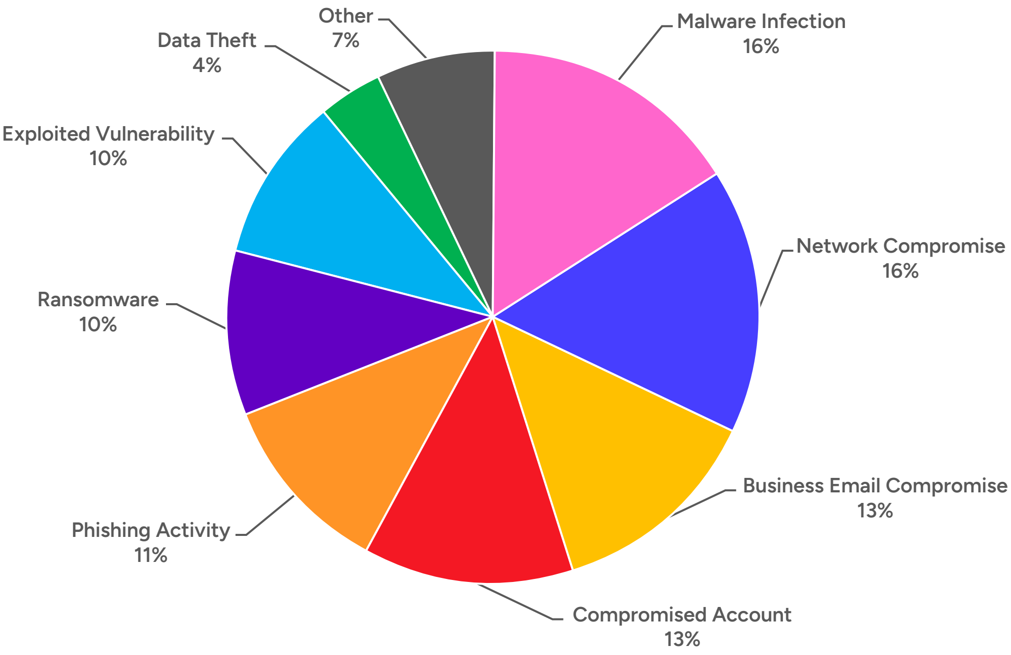


OBSERVED TRENDS

CTU researchers examined the threat actors, engagement types, and initial access vectors (IAVs) observed in Q3 2023 IR engagements.

Engagement types

'Malware infection' and 'network compromise' tied as the most prevalent engagement types in Q3 2023. Typically, these categories represent compromises that were detected at an early stage via monitoring solutions such as Secureworks Taegis™. Close behind were 'business email compromise' (BEC) and 'compromised account'. The proportion of BEC engagements was higher than during the previous quarter, reinforcing CTU researchers' perception that the number of BEC attacks is increasing.



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 Q3 2023. (Source: Secureworks)*

Initial access vectors (IAVs)

'Phishing' and 'vulnerabilities in internet-facing devices' remained the most frequently observed IAVs, although the proportion of engagements involving these IAVs was lower than the previous quarter. There was a significant increase in the percentage of engagements in which 'drive-by download' was the IAV. Drive-by downloads of first-stage malware such as loaders are often associated with SEO poisoning. The proportion of 'stolen credentials' as the IAV also increased compared to the previous quarter.

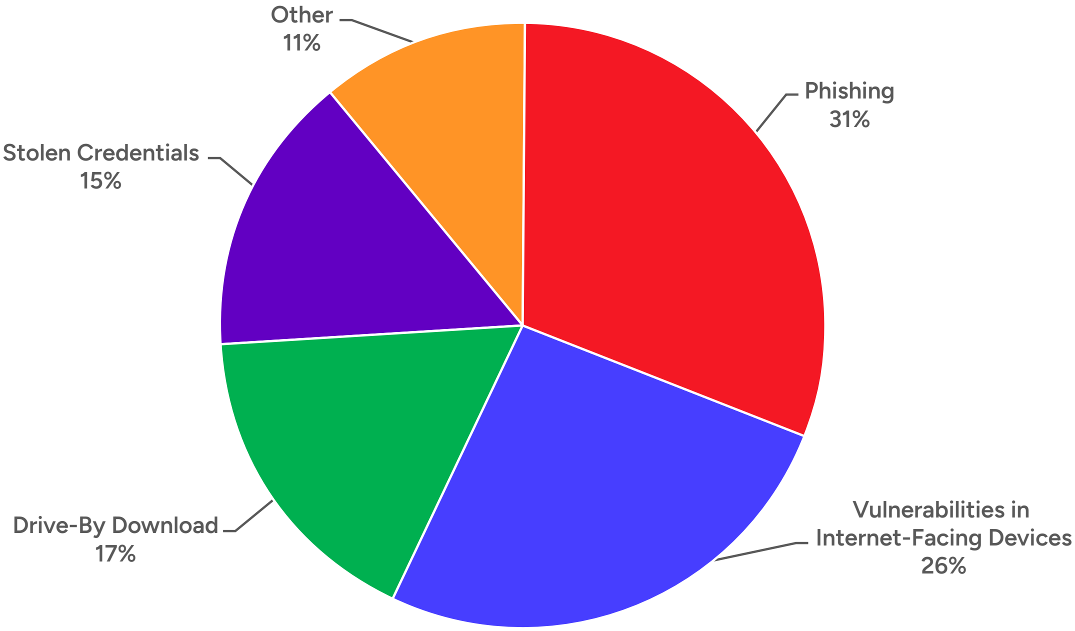


FIGURE 2. *IAVs observed in Q3 2023. (Source: Secureworks)*

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

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

CASE STUDIES

The following sections highlight notable observations from Q3 2023 IR engagements.

Searches for legal templates led to malware

Several incidents during the quarter involved users inadvertently downloading Gootloader malware after searching for legal templates on the internet. Gootloader is a first-stage downloader that often leads to additional malicious activity in the network. It is frequently delivered via drive-by downloads when SEO poisoning or malvertising directs victims searching for legal topics to visit compromised websites. In each analyzed incident, the victim's Google search presented several results, at least one of which was highly ranked because of SEO poisoning.

The victims navigated to a malicious site that appeared to be a forum containing comments and questions relating to the search phrase. Although the victims, the legal search terms, and the compromised websites varied, the same fake forum was displayed. In each instance, a post from a fake "Emma Hill" persona requested a document corresponding to the search term entered by the victim, and a fake forum administrator replied with a download link. CTU researchers observed the Emma Hill persona used in similar attacks in 2022.

Clicking the link downloaded a ZIP archive containing a malicious Gootloader JavaScript payload. Extracting the archive file and executing the JavaScript installed Gootloader. The malware then sent information about the infected system to attacker-controlled command and control (C2) servers for possible further exploitation. In some of the incidents, attackers executed encoded PowerShell scripts and used credentials obtained via Group Policy Preferences and Kerberoasting attacks to move laterally to Active Directory domain controllers.

The close parallels across these incidents does not mean that the same threat actor conducted each attack. Many threat actors seeking to distribute loaders and infostealers use kits that are available for sale or rent on underground forums. Gootloader's availability as a kit results in similarities such as the fake forum and personas, and incidents involving similar infection chains have been observed for several years.

Mitigation

Secureworks incident responders provided victims with recommendations focused on rebuilding compromised hosts and resetting passwords. They also recommended removing users' local administrator permissions, using different local administrator passwords for each system, and implementing controls to detect malware downloads at an early stage and prevent threat actors from moving laterally throughout the network.

Organizations can use application control features (e.g., AppLocker) to limit the locations from which files can be downloaded so users cannot inadvertently select infected search results. Prohibiting execution of JavaScript and PowerShell scripts on endpoints may prevent downloaded malware from installing. In addition, organizations can improve their Active Directory security by requesting a Secureworks Active Directory Security Assessment and by proactively identifying and patching privilege escalation vulnerabilities.

BEC attacks succeeded by using simple subterfuge

Two BEC attacks investigated by Secureworks incident responders during the quarter targeted very similar small organizations. Although the techniques were subtly different, both attacks were successful and relatively simple.

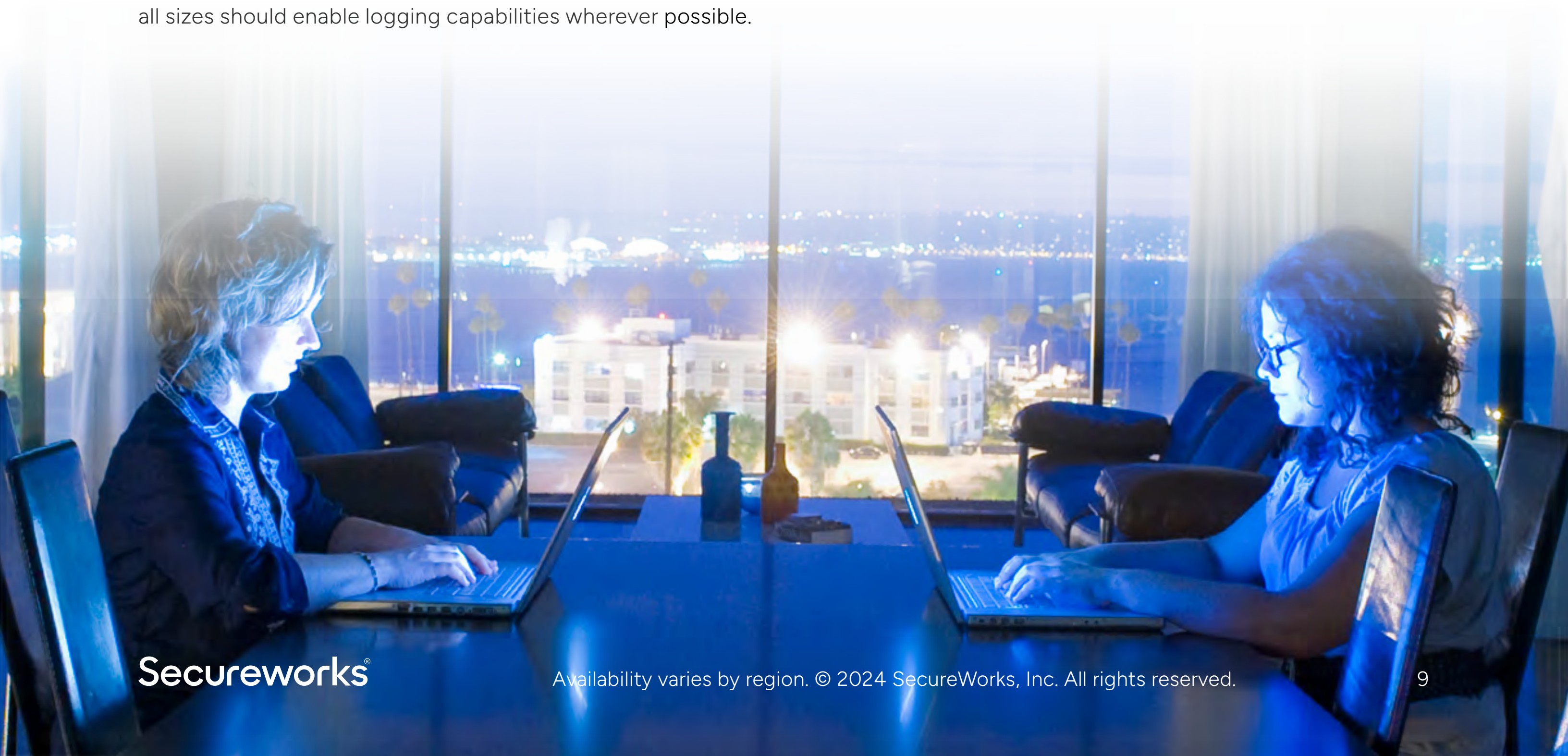
In one of the incidents, a legitimate email and invoice renewing an annual business service was closely followed by an email from the threat actor claiming that the original email contained outdated bank details. The original email was appended to the second email. The attacker's email originated from an email address that was similar enough to the legitimate sender that a cursory inspection might have missed the difference.

In the other incident, the victim received an invoice by email for services received. However, inspection revealed that the sender email address had been spoofed, and a homograph attack had been applied to the reply-to address. The replacement of one character with two others that together looked very similar to the single character made the address appear to be associated with a reputable domain. The fraudulent email and invoice purported to be amended copies of a previous legitimate invoice.

In both incidents, a lack of logging in the victims' email systems limited the availability of attack details. In particular, there was insufficient data to determine if the threat actors had previous access to the victims' systems. Small organizations may have fewer IT resources than larger corporations or may use services that lack robust logging features. These limitations can make it difficult to determine how attacks occurred.

Mitigation

Secureworks incident responders issued recommendations to help the victims avoid similar attacks in future. The advice included requiring stronger passwords and multi-factor authentication (MFA), as well as mandating staff awareness training describing fraudulent tactics and techniques. Implementing manual verification protocols for financial transactions, including verifying payment requests via channels other than email, is also important for mitigating BEC attacks. Organizations of all sizes should enable logging capabilities wherever possible.



Swift detection and action thwarted a ransomware attack

Secureworks Taegis alerted a customer to suspicious activity that indicated a potential ransomware attack. Secureworks incident responders' review of Taegis telemetry revealed that the threat actor gained initial access to a service account that had administrative privileges on the network. The threat actor then used Windows commands to conduct discovery on the network before installing and executing a malicious binary on multiple hosts. This binary communicated with external resources and enabled exfiltration of sensitive data. The threat actor also relied on an open-source Python toolkit and other Windows utilities for lateral movement and remote command execution. They attempted to turn off Windows event logging to hide their activity.

The victim's swift response to the alert stopped the attack before ransomware was deployed. These actions included isolating compromised hosts, resetting passwords and Kerberos, and rebuilding the part of the network that contained the device that the threat actor initially compromised.

Mitigation

The customer's actions covered many of the recommendations that Secureworks incident responders would typically give for this type of incident. In addition to these actions, Secureworks incident responders advised the customer to conduct red team exercises on the compromised segment of the network to identify remaining security gaps. They also recommended storing sensitive data on separate virtual local area networks (VLANs) to hinder lateral movement.

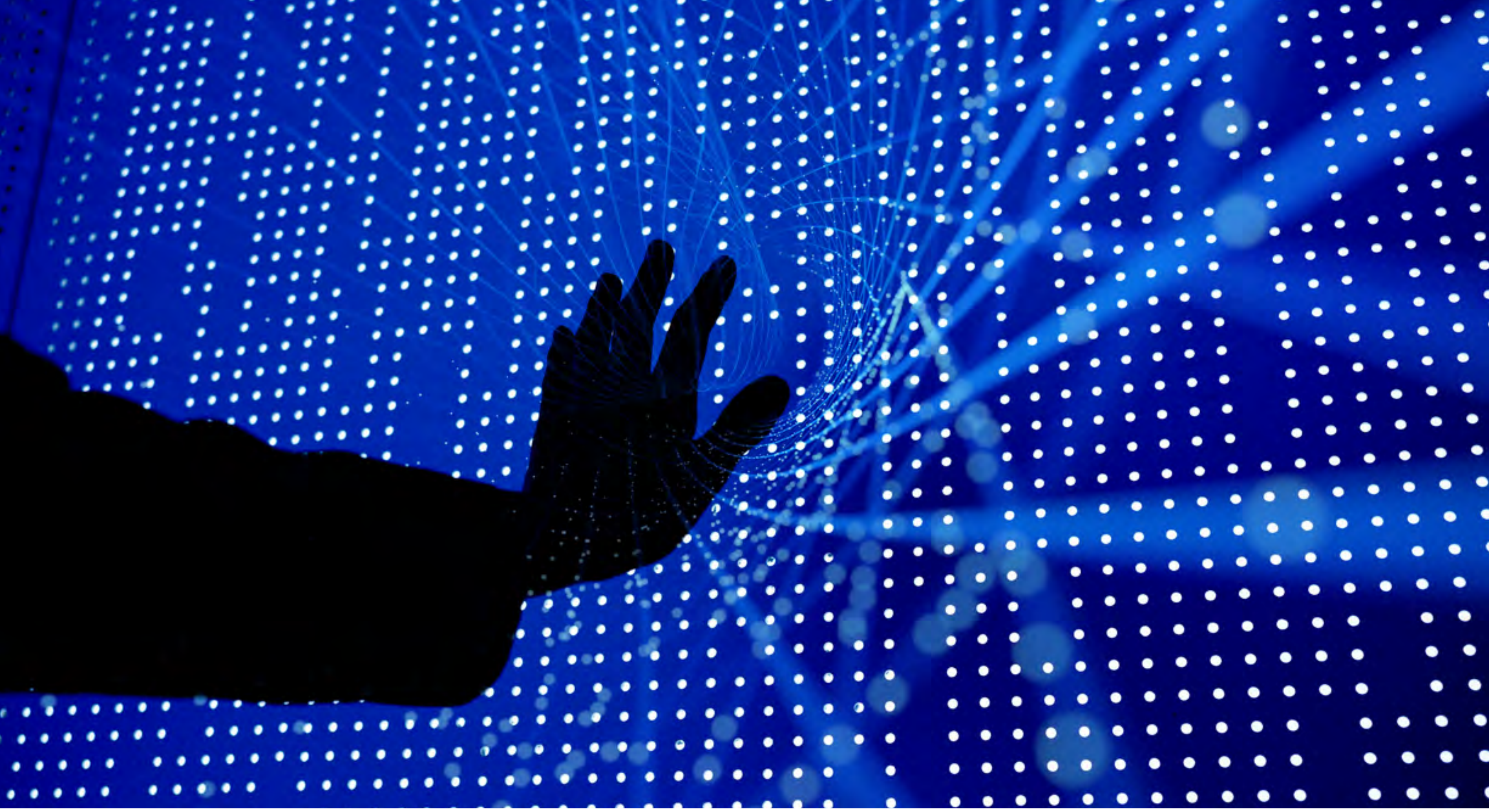
RECOMMENDATIONS

At the end of engagements, Secureworks incident responders provide remediation advice to prevent further damage from the current incident. These recommendations may be useful to other organizations that experienced similar events. In Q3 2023, Secureworks incident responders most frequently issued the following remediation recommendations:

- 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. Ensure that service accounts and group managed service accounts have strong, unique passwords.

To reduce the likelihood of similar incidents in the future, the following were the most common proactive recommendations given by Secureworks incident responders:

- Develop and implement security awareness training that includes instructions for users to report suspected suspicious activity.
- Enforce MFA to access company systems and services. MFA implementations should be comprehensive and not leave gaps for legacy systems or administrator accounts.
- Implement an extended detection and response solution such as Taegis XDR 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