Secureworks®

Learning from Incident Response: January – March 2022

Secureworks® Counter Threat Unit™ Research Team

Table of Contents

Summary

Secureworks® Counter Threat Unit™ (CTU) researchers analyzed data from over 100 Secureworks incident response (IR) engagements completed between January and March 2022. 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.

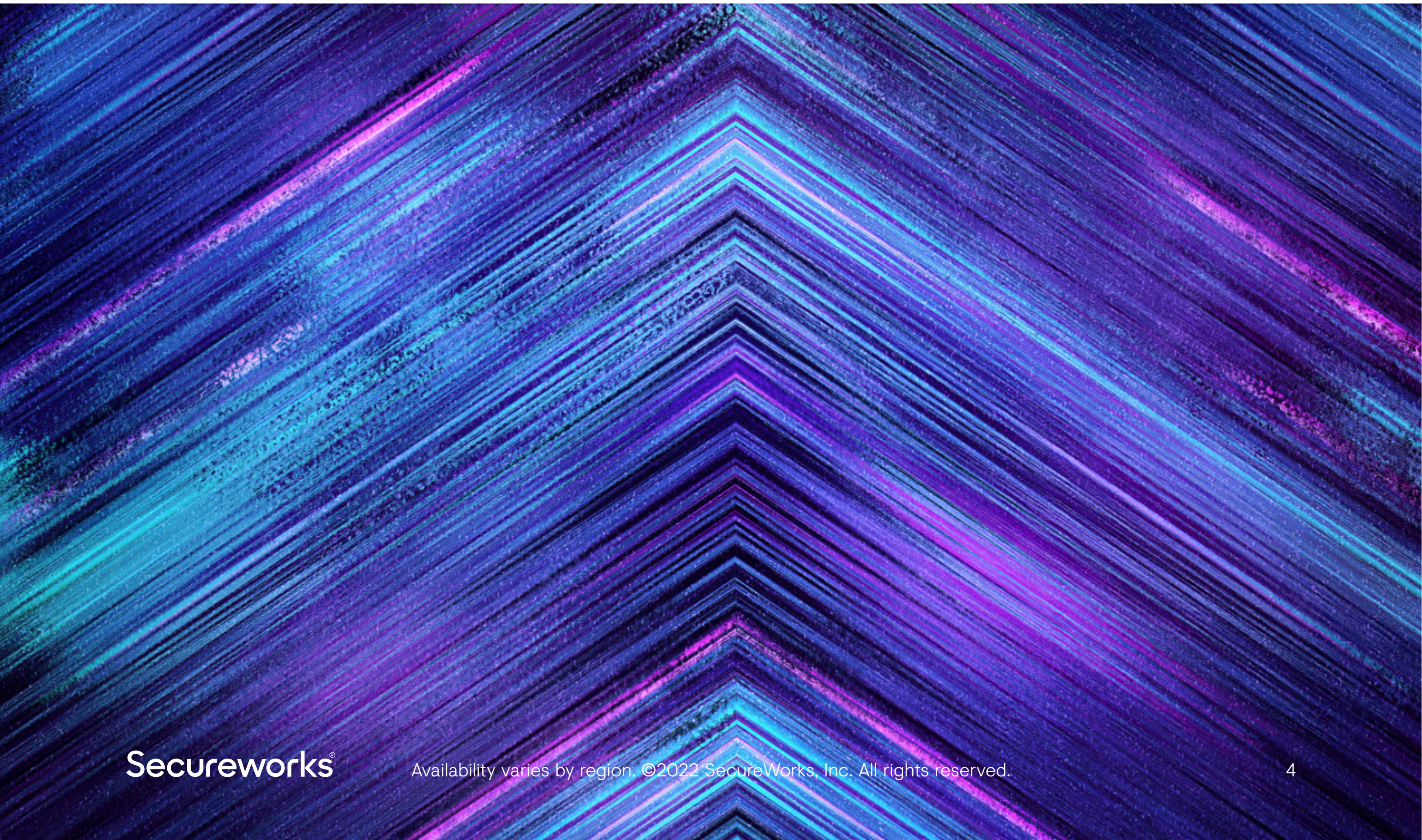
The motivation and context for IR engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or if the organization is entering a sensitive operational period. As a result, observed threat types may not reflect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

Multiple ransomware groups abused single-factor authentication solutions to gain access into victims' networks.

Internet-facing vulnerabilities are a favorite target of threat actors seeking a foothold in an organization.

Insider threat engagements more than doubled from the previous quarter, with incident responders helping victims mitigate the loss of large amounts of sensitive organizational data.



Observed Trends

CTU researchers examined the threat actors, threat types, and initial access vectors (IAVs) observed in Q1 2022 IR engagements.

Threat types

Financially motivated threats consistently represent most of the activity observed during IR engagements. These threats include ransomware, business email compromise (BEC), and cryptojacking (see Figure 1). Cybercriminal activity impacts organizations of all sizes and levels of revenue.

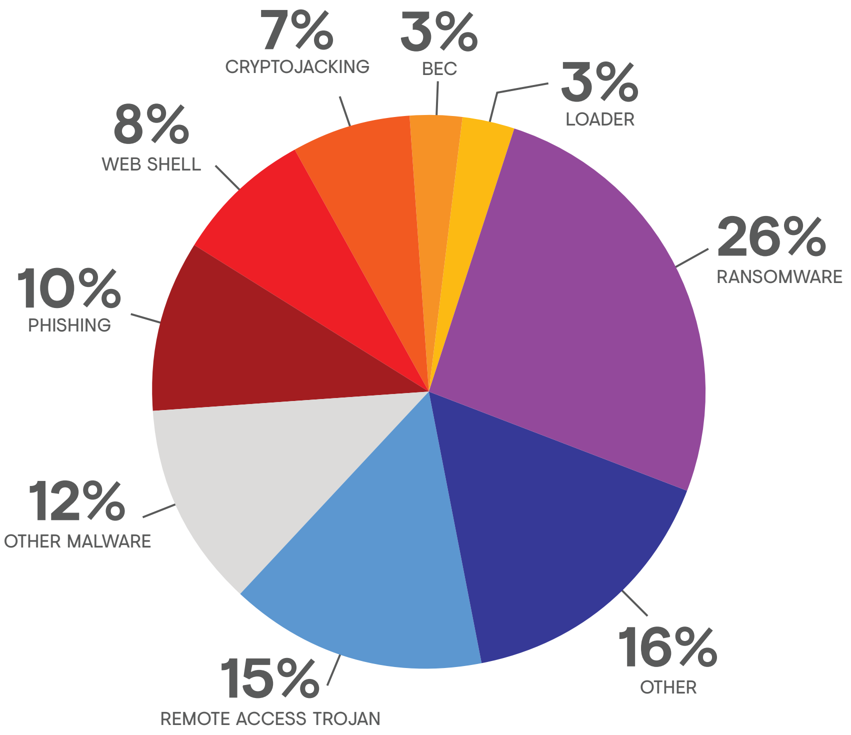


FIGURE 1. *Threats observed in Q1 2022 IR engagements. (Source: Secureworks)*

Initial access vectors

Continuing the trend from previous quarters, the most frequently observed IAV was the exploitation of vulnerabilities in internet-facing devices (see Figure 2). Threat actors took advantage of newly disclosed vulnerabilities, such as an authentication bypass flaw in the ManageEngine service management solution. Threat actors also leveraged unpatched older vulnerabilities, including the ProxyShell vulnerabilities that impact Microsoft Exchange servers.

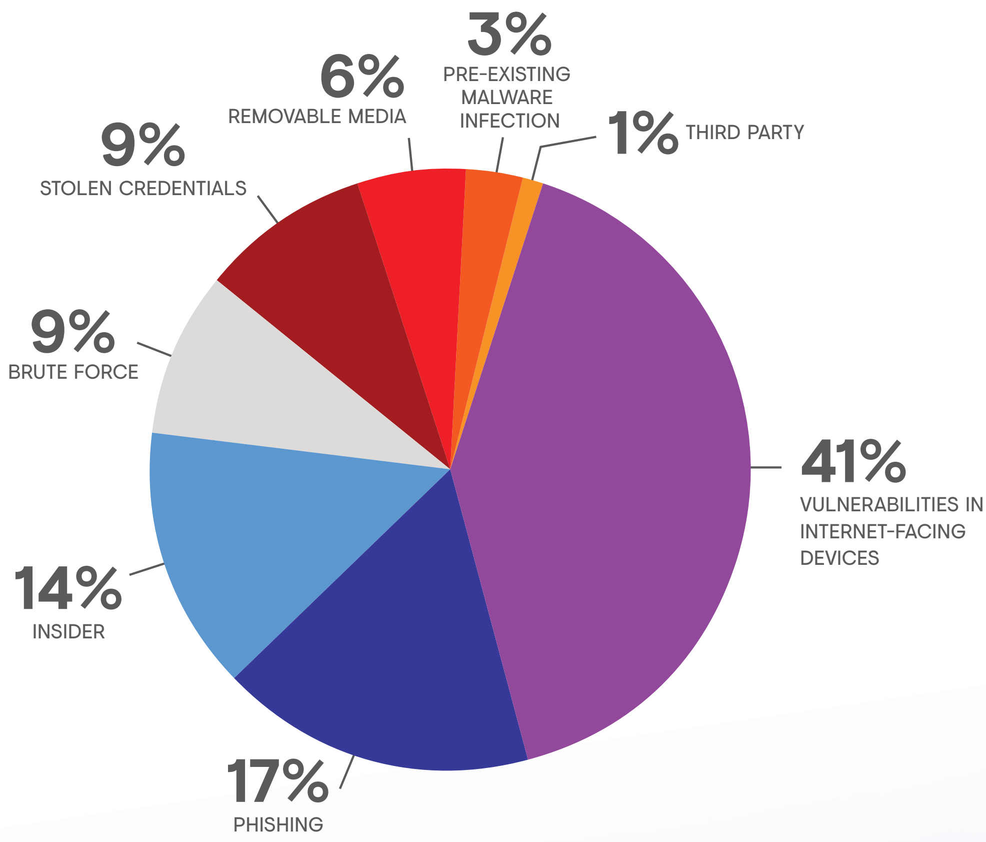
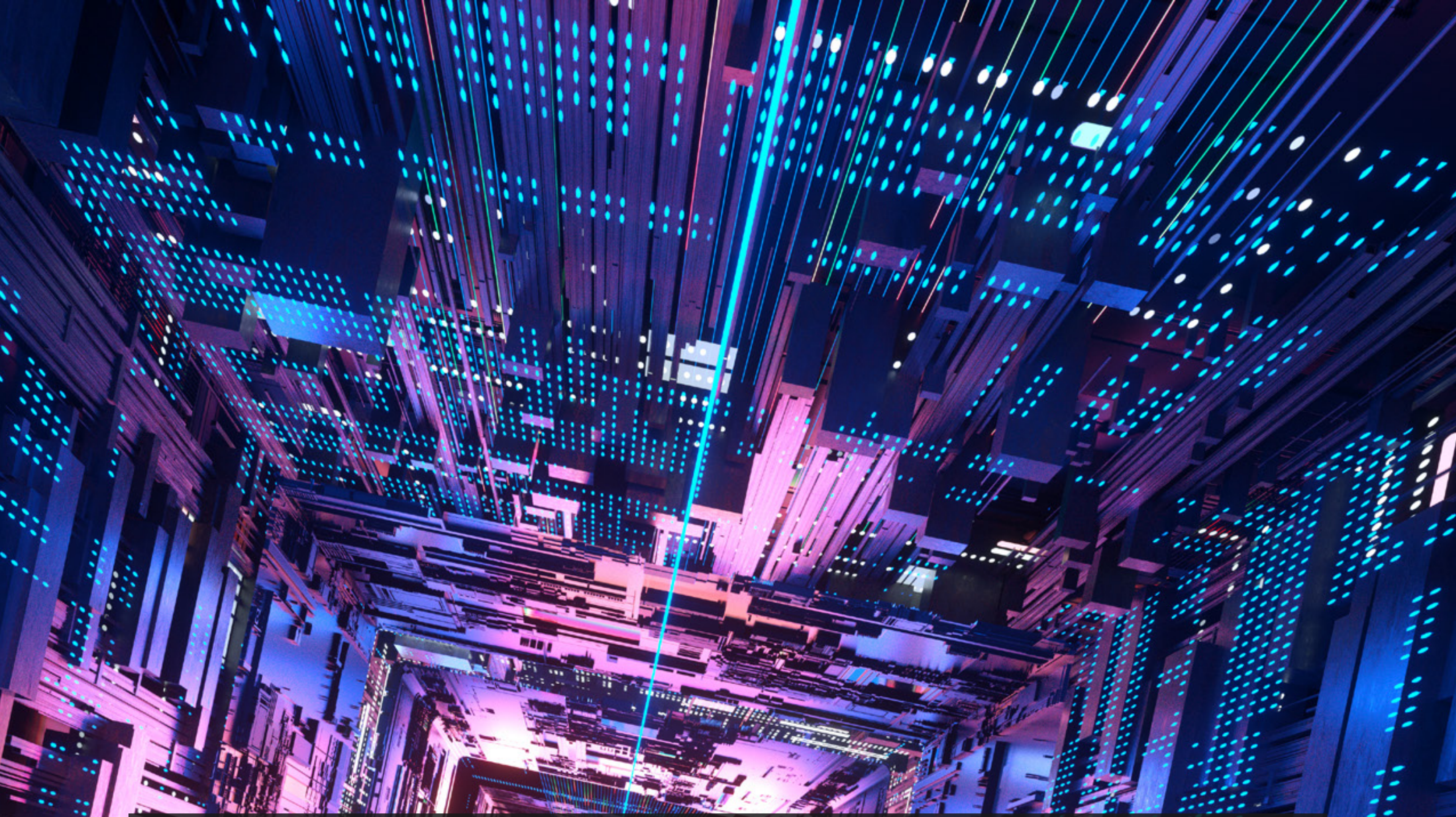


FIGURE 2. *IAVs observed in Q1 2022. (Source: Secureworks)*



Mapping IAVs to MITRE ATT&CK

This table 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
Credentials (brute force, password spraying, stolen credentials)	Valid Accounts Brute Force
Malicious emails	Phishing Spearphishing Attachment Spearphishing Link Spearphishing via Service
Third-party access	Supply Chain Compromise Trusted Relationship
Pre-existing malware infection	Develop Capabilities

Case Studies

The following sections highlight notable observations from Q1 2022 IR engagements.

Single-factor authentication can provide a foothold for ransomware attacks

In one Secureworks incident response engagement this quarter, a threat actor compromised several virtual private network (VPN) accounts that were not protected by MFA. The victim was running a SonicWall SMA-500V VPN appliance that contained an SQL injection vulnerability (CVE-2021-20016). The attacker exploited this flaw to acquire VPN account details, including the username, password, and other session-related information.

The threat actor then executed the Mimikatz credential theft tool and the Sysinternals ProcDump tool. ProcDump is commonly used to dump the Windows Local Security Authority Server Service (LSASS) process, whose output can be used to steal credentials. The attacker established an additional access vector by placing the SystemBC proxy malware on one of the compromised accounts before executing Cobalt Strike.

During the attack, the threat actor employed other commonly used tools: PowerShell to exploit the PrintNightmare vulnerability (CVE-2021-34527), the PowerSploit post-exploitation framework, the SoftPerfect Network Scanner, FileZilla for FTP, and the MegaSync cloud storage data sync tool. Stolen data was likely exfiltrated using MegaSync. After exfiltration, the threat actor deployed LV ransomware.

Delayed patching and software misconfiguration introduce risks

Secureworks incident responders remediated multiple intrusions caused by the exploitation of unpatched vulnerabilities or misconfigurations in software packages. When proof-of-concept exploits are published, threat actors often immediately scan the internet for potentially vulnerable systems. Organizations must patch their vulnerable systems as promptly as possible to minimize risk.

ProxyShell compromises in the first quarter of 2022 led to web shell, cryptocurrency miner, and ransomware deployments. This collection of vulnerabilities impacting Microsoft Exchange Servers (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) was publicly disclosed in August 2021. Although Microsoft had released security updates addressing these issues in April and May, some organizations were slow to implement the patches or chose not to apply them for operational reasons. Threat actors continue to scan for and exploit vulnerable systems.

Similarly, CTU researchers observed widespread scanning for systems vulnerable to ManageEngine critical security bypass vulnerability CVE-2021-40539. Threat actors could exploit this flaw to gain access to user environments. Following the September 2021 disclosure, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published an alert warning of exploit activity and encouraging organizations running affected software to patch immediately. In the first quarter of 2022, Secureworks incident responders assisted organizations that were slow to patch and were impacted by vulnerability scanning. Other customers had not properly configured their ManageEngine environments and continued to use the targeted default ManageEngine default administrator account.

Attackers who exploit unpatched vulnerabilities or access environments via default accounts often deploy web shells, backdoors, and other remote access trojans to maintain access. They then attempt to escalate privileges and move laterally across the compromised environment.

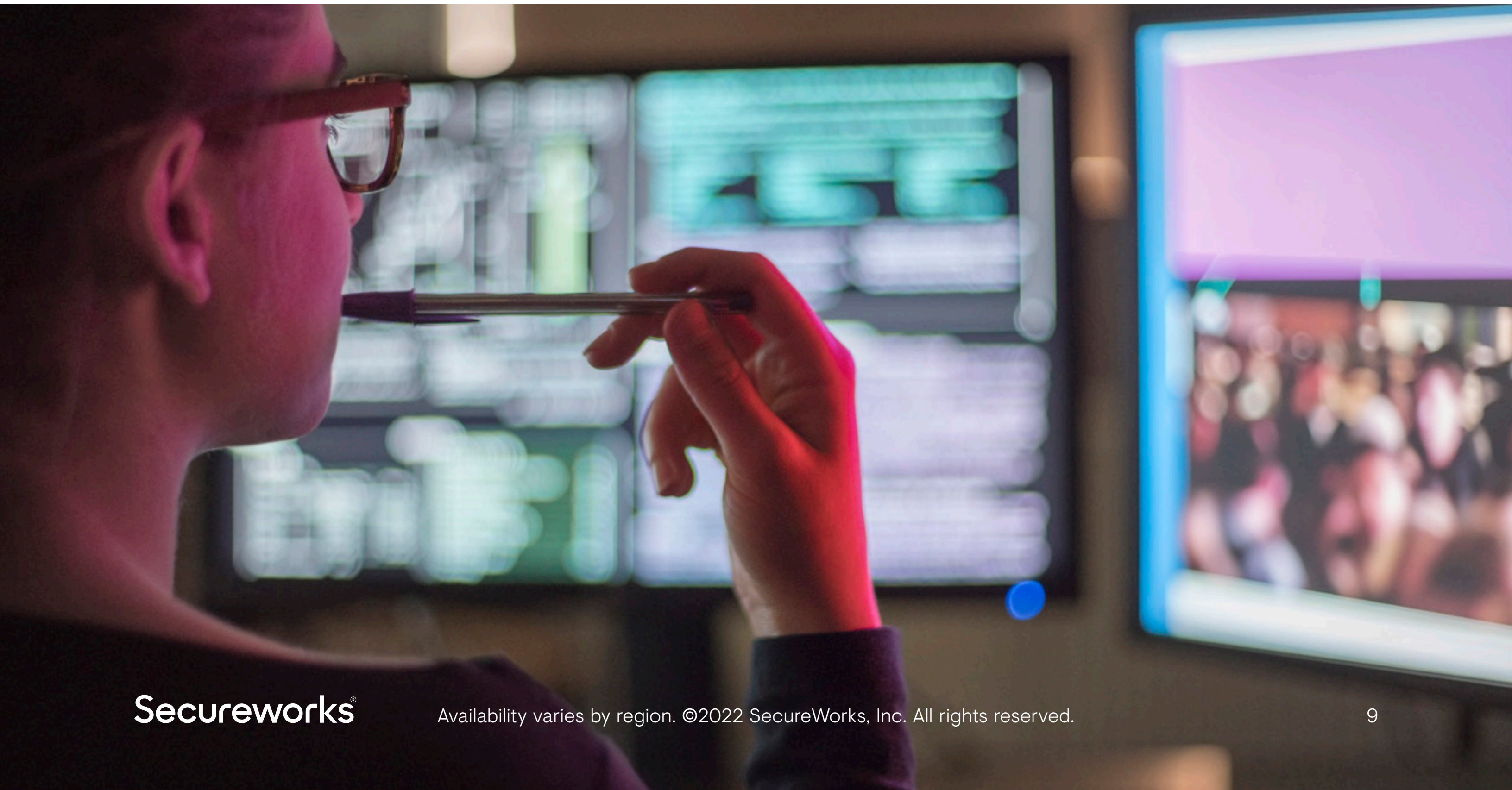
Insider threats are on the rise

This quarter, Secureworks incident responders investigated more than double the number of insider threat incidents than in the previous quarter. Approximately half of the incidents were due to negligence, while the other half were malicious.

In one incident, a terminated employee sent a significant number of sensitive company documents to themselves. The organization's data loss prevention (DLP) system alerted the organization and triggered an investigation. Secureworks incident responders determined that the insider used personal email on the organization's workstation to circumnavigate security controls. The investigation revealed the amount of information the insider exfiltrated before the activity was detected.

In another insider incident, a terminated remote employee retained local access to their workstation for more than a month after their network access was revoked. During that month, they removed a large amount of locally stored data and attempted to hide their activity. Forensic analysis revealed attempts to remove data using USB devices and network storage services. The insider also unsuccessfully attempted to circumvent operating system file locks.

These incidents illustrate why an organization needs established termination processes to protect its assets. The incidents also demonstrate the importance of DLP solutions to identify potential losses.



Recommendations

Figure 3 shows the top recommendations that Secureworks incident responders provided to affected organizations during Q1 2022 engagements. In many incidents, lack of MFA allowed threat actors who possessed valid credentials to further advance their attacks. Unpatched systems facilitated initial access to systems and environments. Limited availability of logs presented challenges for incident responders. Implementing these recommendations can help organizations avoid, detect, respond to, and recover from breaches.

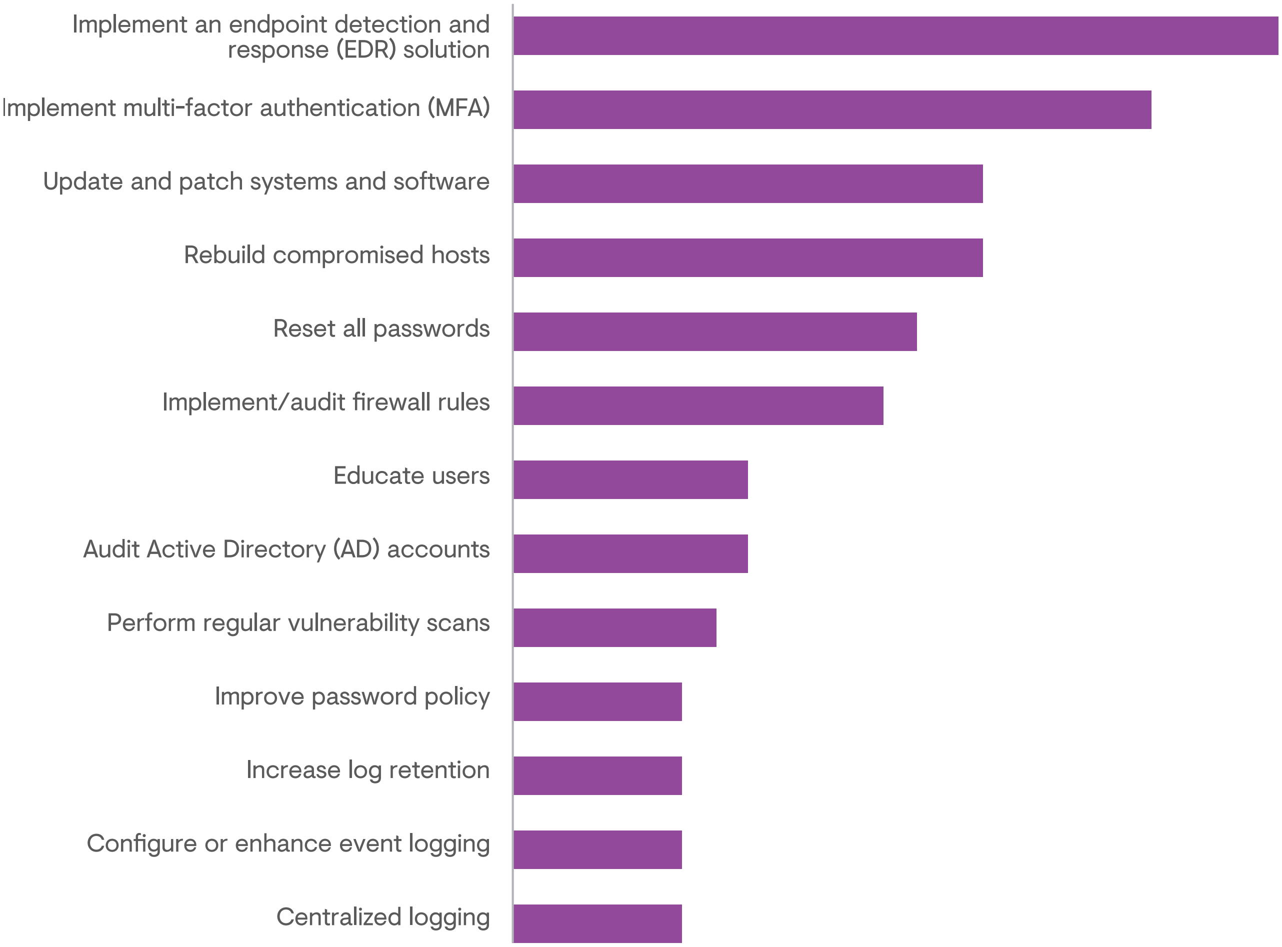


FIGURE 3. *Top recommendations provided to affected organizations in Q1 2022. (Source: Secureworks)*

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.

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

Sources

ManageEngine. "Security advisory - ADSelfService Plus authentication bypass vulnerability." September 7, 2021.

Secureworks. "LV Ransomware." June 22, 2021.

Tsai, Orange. "From Pwn2Own 2021: A New Attack Surface on Microsoft Exchange - ProxyShell!" Zero Day Initiative. August 18, 2021.

U.S. Cybersecurity & Infrastructure Security Agency. "APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus." November 22, 2021.