Secureworks®

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

Ransomware activity continued to increase, with multiple threat groups operating both new and long-running ransomware families.

The number of engagements involving business email compromise (BEC) more than doubled compared to Q1 2022.

Use of phishing to gain initial access increased by more than 15% over the previous quarter.

Observed Trends

CTU researchers examined the threat actors, threat types, and initial access vectors (IAVs) observed in Q2 2022 IR engagements.

Threat types

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

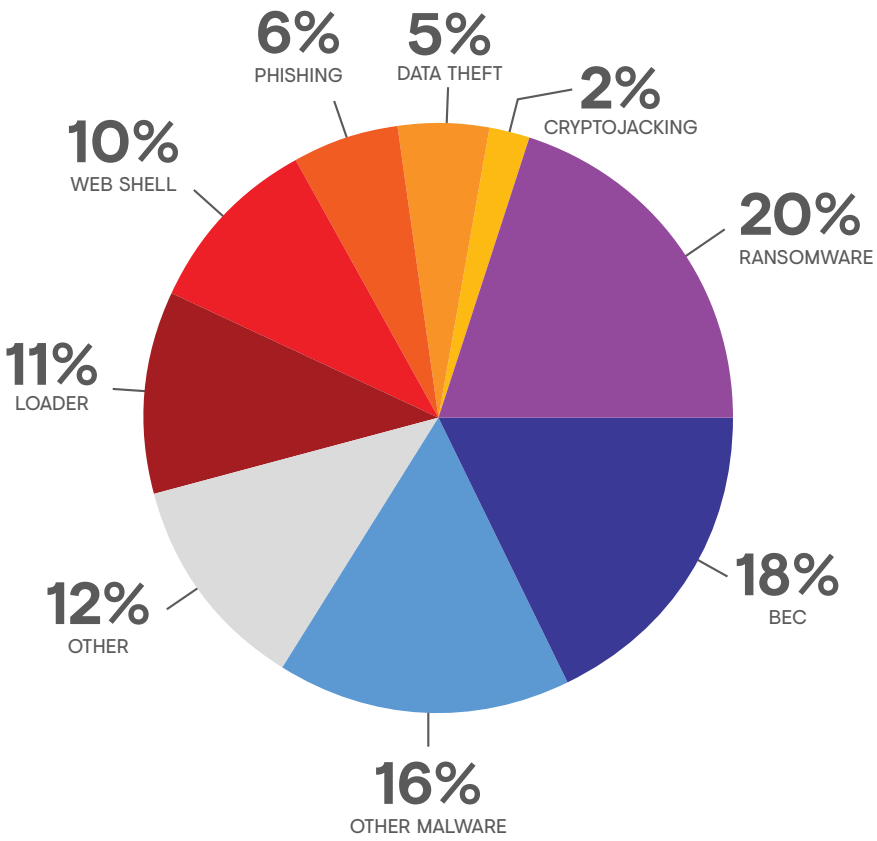


FIGURE 1. *Threats observed in Q2 2022 IR engagements. (Source: Secureworks)*

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). Multiple ransomware operators exploited the ManageEngine ADSelfService Plus authentication bypass vulnerability (CVE-2021-40539) to gain initial access to unpatched servers. Phishing emails containing malicious attachments and links to credential-harvesting websites remained a primary access method, ranking close behind vulnerability exploitation this quarter.

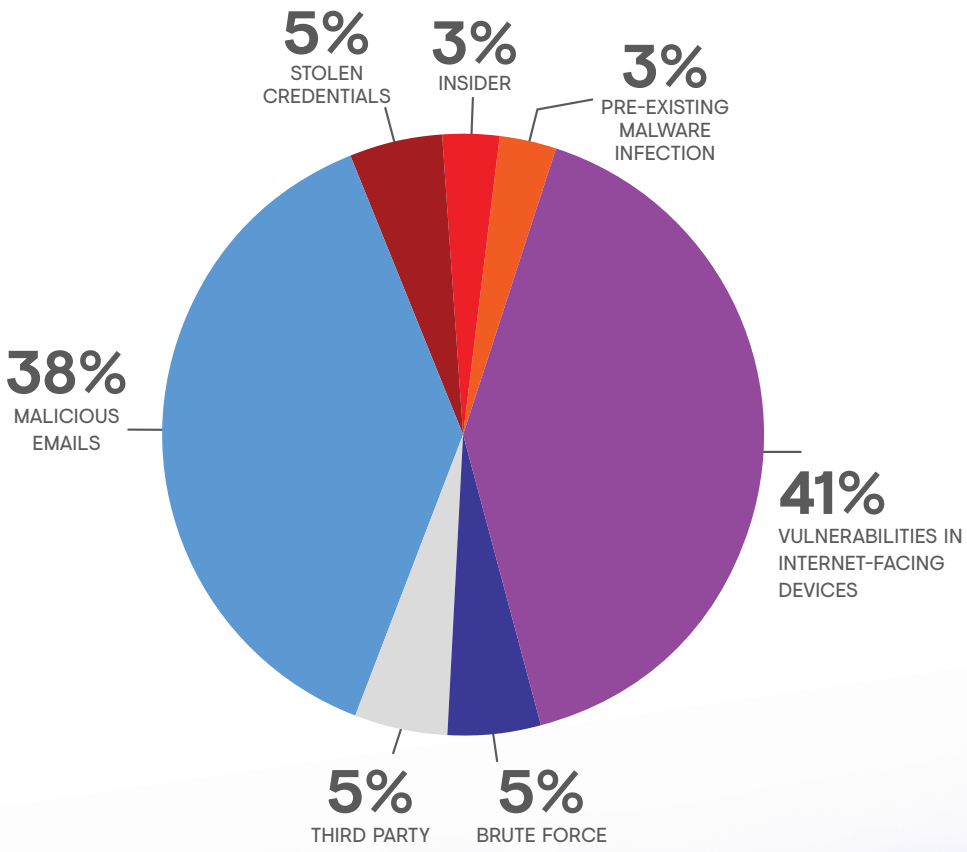
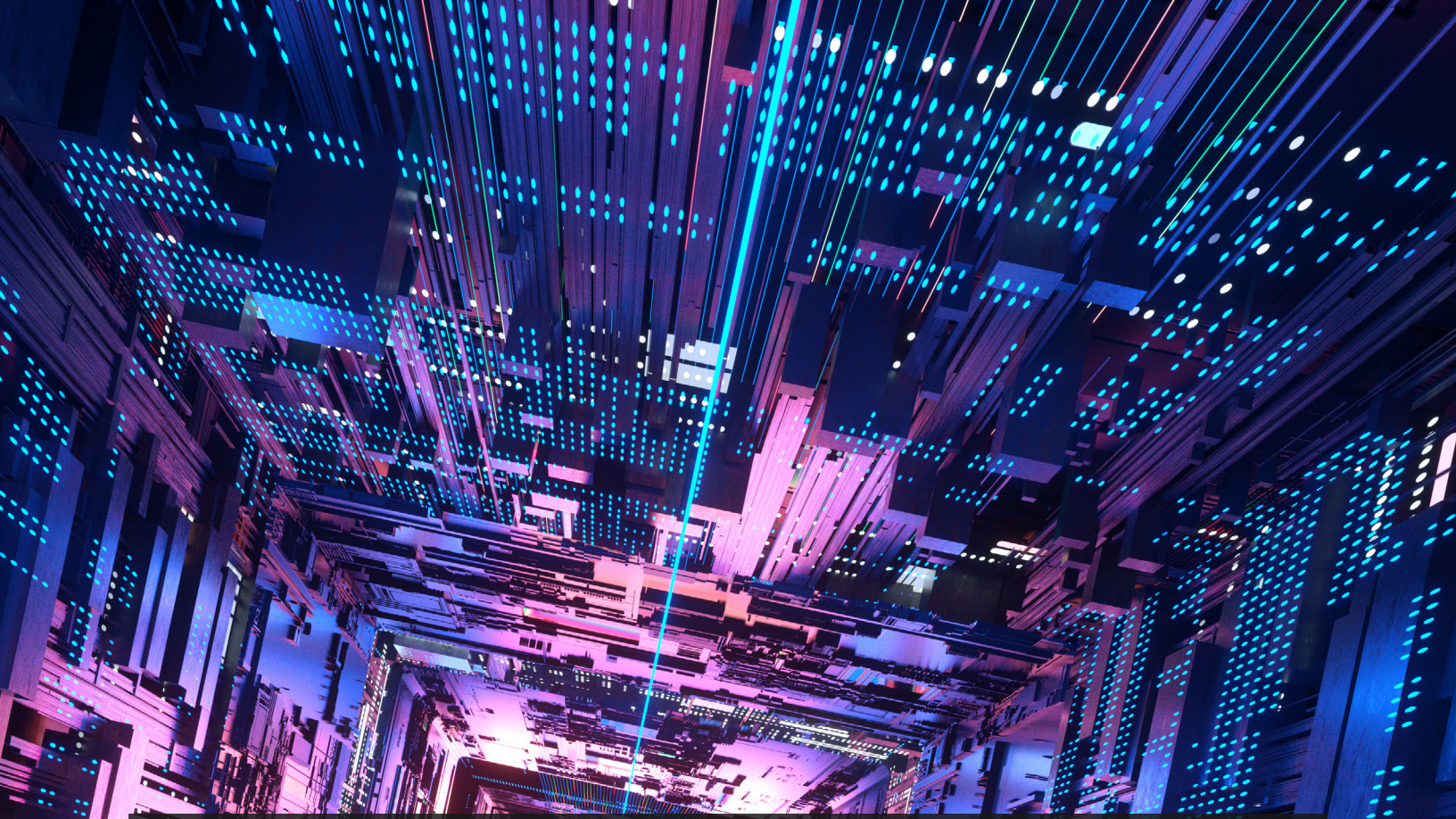


FIGURE 2. *IAVs observed in Q2 2022. (Source: Secureworks)*



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 Q2 2022 IR engagements.

MSP compromise leads to ALPHV ransomware

In one Secureworks IR engagement this quarter, a threat actor exploited a compromised managed services provider (MSP) account to access the victim's environment. The threat actor leveraged that foothold to escalate privileges, map the network, and deploy ransomware.

The threat actor first connected to the victim's network through a remote desktop connection using a legitimate user account at the victim's MSP. Immediately after accessing the network, the threat actor installed a ScreenConnect client used for remote connections, likely for persistence. They then dumped the Local Security Authority Subsystem Service (LSASS) to extract credentials, ran netscan.exe to map the network, and moved laterally to other accounts on the network. They viewed files on these other accounts and installed the MegaSync cloud storage tool to exfiltrate files to attacker-controlled infrastructure.

For the next two days, the threat actor repeated this process on hosts throughout the network, always uninstalling MegaSync after each session to avoid detection. After two days, the threat actor successfully deployed ALPHV (also known as BlackCat) ransomware on some systems via PowerShell scripts that downloaded and executed the binaries from the attacker's infrastructure. The impact of the attack was minimal because the victim's backups were not affected and antivirus partially disrupted the ransomware.

Activity related to the conflict in Ukraine

Since the beginning of the Russian invasion of Ukraine in February 2022, CTU researchers have closely tracked related threats that may impact customers. While there has not been major offensive activity outside of the conflict's geographic region, related activities have had effects on organizations worldwide.

In one incident, the Secureworks Taegis™ ManagedXDR solution detected and alerted an organization to suspicious scripts running on multiple virtual machines in the organization's network. An investigation revealed that the scripts were launching distributed denial of service (DDoS) attacks against multiple IP addresses geolocated in Russia. Employees knowingly visited websites, downloaded publicly available tools, and executed software that facilitated DDoS attacks. The tools contacted hard-coded URLs and retrieved a list of targets to attack.

While this activity did not significantly impact business operations, it exposed the organization to potentially serious risks. Unauthorized software and scripts could introduce malware or access vectors into the environment, and entities associated with the targeted IP addresses could conduct retaliatory attacks.

Single-factor authentication leads to Hive ransomware

Requiring multi-factor authentication (MFA) on every privileged account in an organization's network is a necessary control in modern cybersecurity. Threat actors often abuse single-factor accounts to gain an initial foothold in a network.

During this quarter, Secureworks incident responders discovered that a threat actor logged on to an organization's VPN host via single-factor authentication. Although the organization generally required MFA, the threat actor discovered and accessed specific utility accounts that only required single-factor authentication.

After accessing the VPN host, the threat actor installed Cobalt Strike, gathered credentials, and mapped the network. Within 24 hours, the threat actor escalated privileges, moved throughout the network, exfiltrated more than 30 GB of data and documents, targeted and stole the Active Directory database, and used Group Policy Objects to deploy and execute GOLD HAWTHORNE's Hive ransomware.

Recommendations

Figure 3 shows the top recommendations that Secureworks incident responders provided to affected organizations during Q2 2022 IR engagements. In many incidents, lack of an endpoint detection and response (EDR) solution such as Taegis XDR allowed threat actors to traverse networks, escalate privileges, and launch attacks undetected. Many of the proactive recommendations provided during IR engagements reflect good security practices that are relevant to all organizations. For example, applying a robust patch management policy is key to avoiding compromises from known vulnerabilities. Organizations should also consider implementing an allowlisting policy to limit exposure to unwanted and malicious programs.

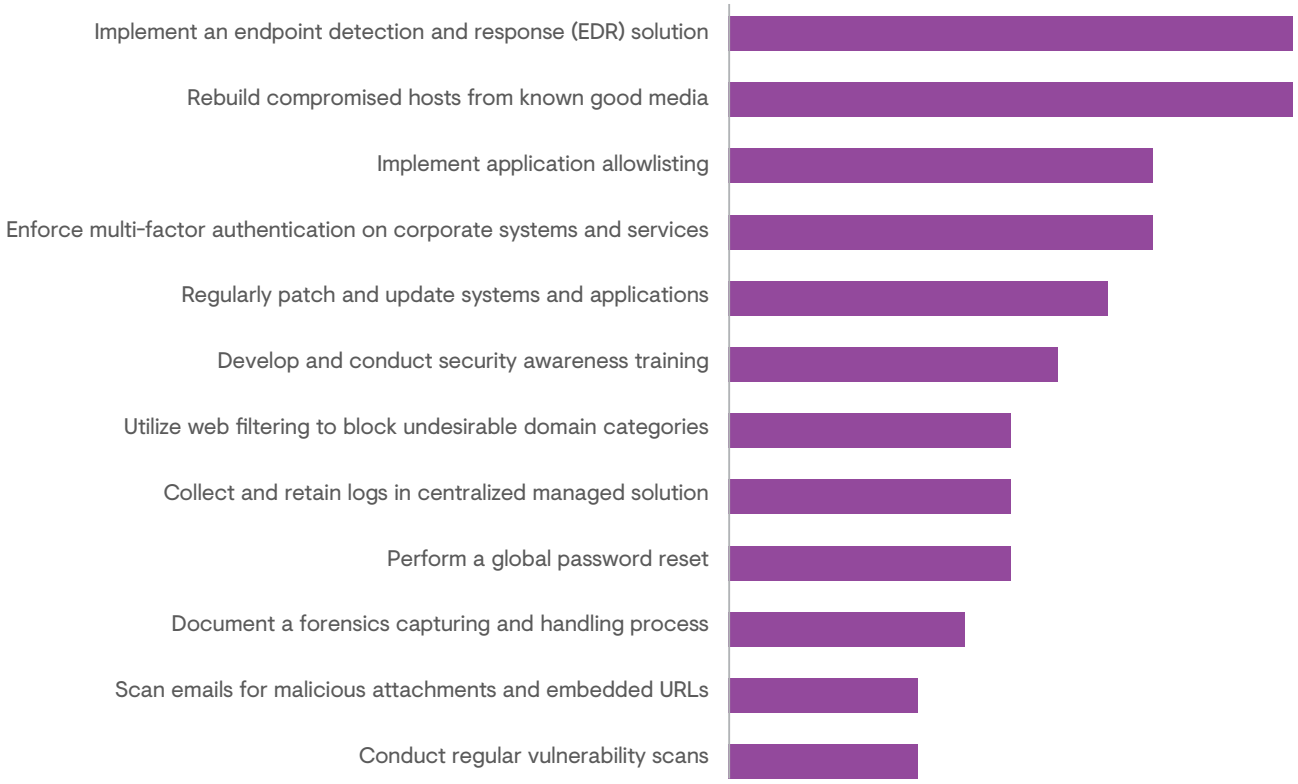


FIGURE 3. *Top recommendations provided to affected organizations during Q2 2022 IR engagements. (Source: Secureworks)*

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.

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