Secureworks®

Learning from Incident Response: 2022 Year in Review

Secureworks® Counter Threat Unit™ Research Team

Table of Contents

Summary

Between January and December 2022, Secureworks® assisted in the containment and remediation of over 500 security incidents. Visibility of these real-world incidents provided Secureworks Counter Threat Unit™ (CTU) researchers with insight into emerging threats and developing trends that organizations can use to guide risk management decision-making, inform best practice, and prioritize resource allocation.

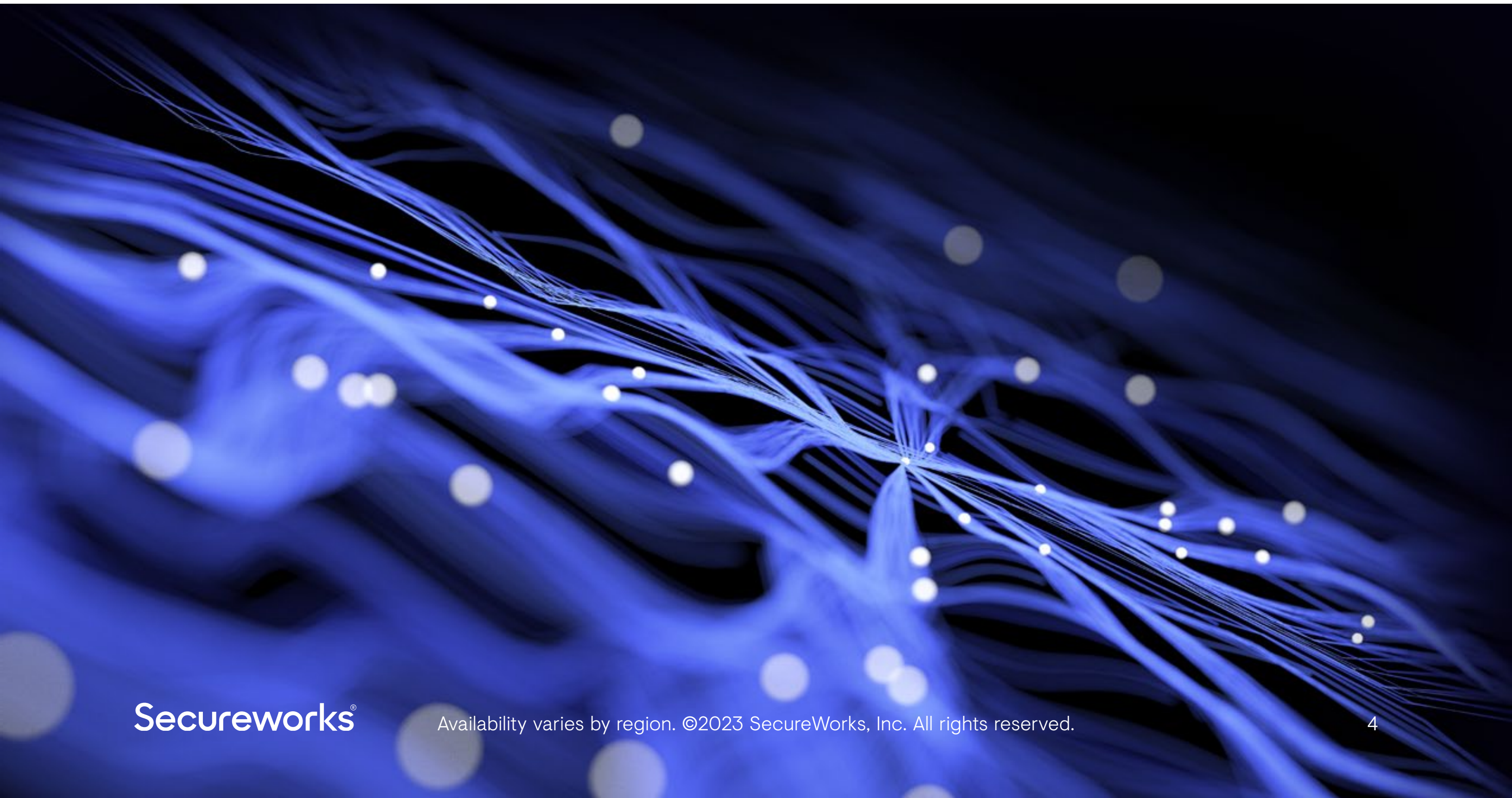
The motivation and context for incident response (IR) engagements vary. For example, an organization's decision to use IR services could be influenced by the organization's internal resources, media reporting, or the organization entering a sensitive operational period.
As a result, observed threat types 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:

Post-intrusion ransomware continued to represent a significant threat to organizations due to the high impact these attacks can cause. However, business email compromise (BEC) attacks overtook post-intrusion ransomware to become the most common type of financially motivated activity observed during Secureworks IR engagements in 2022.

Vulnerabilities in internet-facing systems remained a common initial access vector (IAV). However, the percentage of engagements where phishing was the IAV increased from 13% in 2021 to 33% in 2022, likely due to an increase in BEC attacks.

Multi-factor authentication (MFA) and cloud-based hosting have changed the attack surface, prompting threat actors to find creative ways to circumvent the security controls to achieve their objectives.



Observed Trends

Cybercrime continued to represent the greatest threat to Secureworks customers, with 79% of incidents attributed to financially motivated cybercriminals. By comparison, hostile government-sponsored activity was observed in approximately 9% of Secureworks IR engagements. The remaining incidents were due to deliberate or accidental actions by organizations' employees. The proportion of financially motivated intrusions was lower than previous years, down from 85% in 2021 and 92% in 2020 (see Figure 1). This shift may be due in part to Russia's invasion of Ukraine; it is possible that Ukrainian and Russian cybercriminals diverted their attention to hacktivist operations targeting organizations that supported the opposing country.

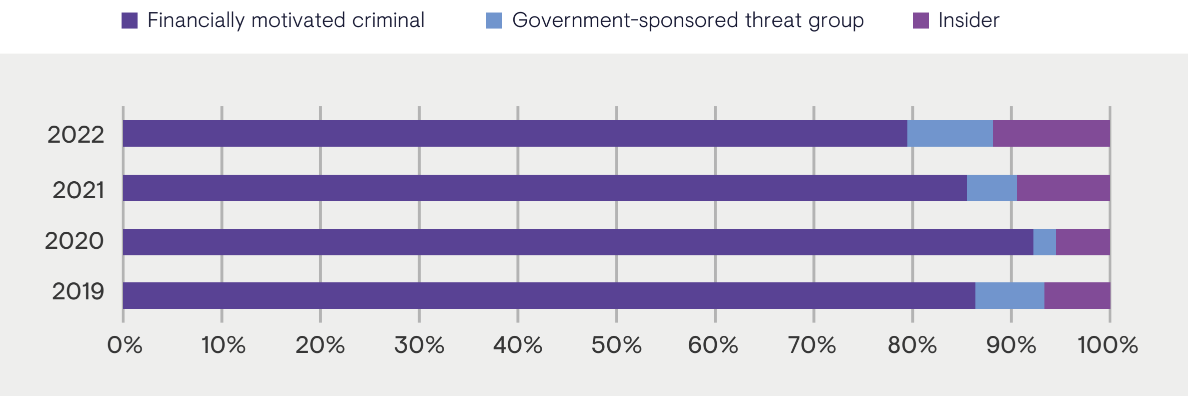


FIGURE 1. *Breakdown of threat actor types observed in Secureworks IR engagements from 2019 through 2022. (Source: Secureworks)*

The financially motivated incidents in 2022 involved threats such as ransomware, BEC, and cryptojacking. Cybercriminal activity is opportunistic and is driven by threat actors' ability to maximize the profits that can be generated by unauthorized access to compromised networks. For that reason, extortion-based attacks such as ransomware continued to dominate.

Initial access vectors

In 2022, exploitation of vulnerabilities in internet-facing devices and phishing were the most common IAVs observed in Secureworks IR engagements. They each accounted for approximately one-third of the incidents where the IAV could be determined (see Figure 2).

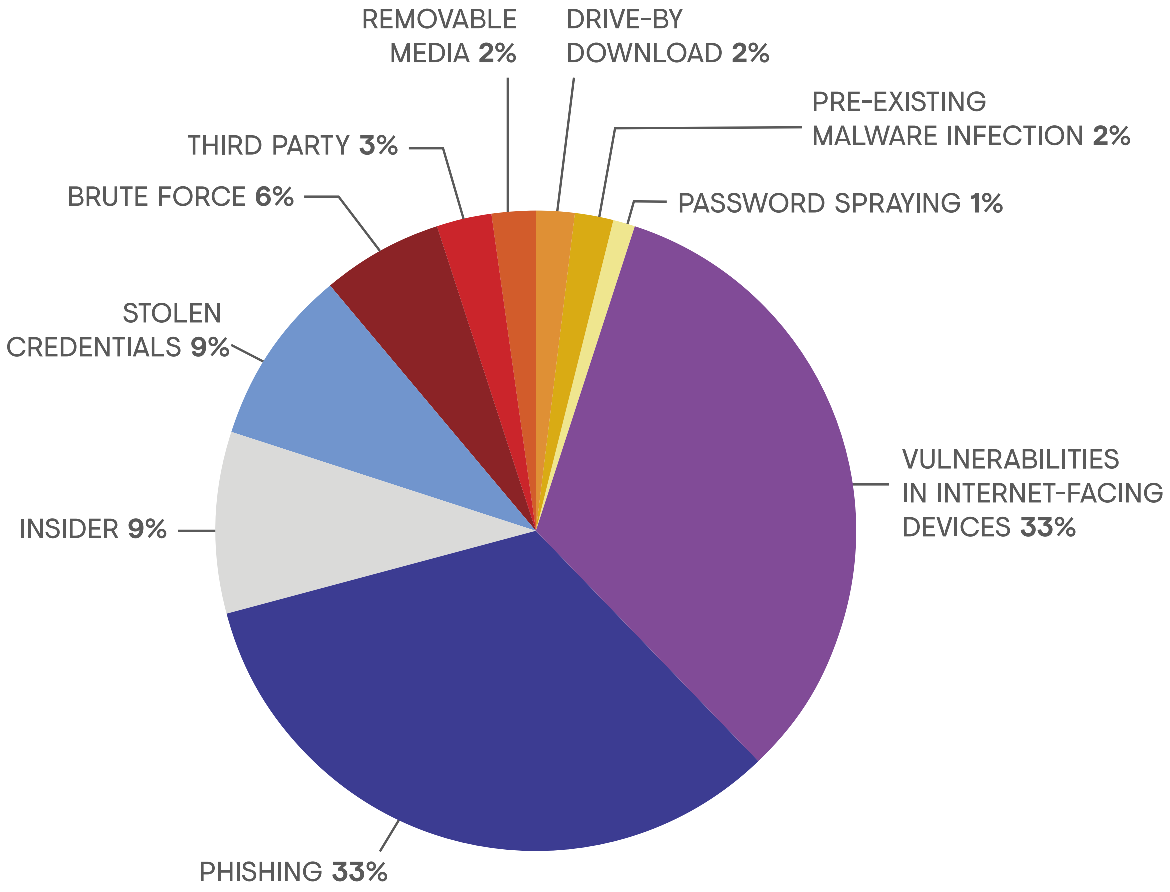
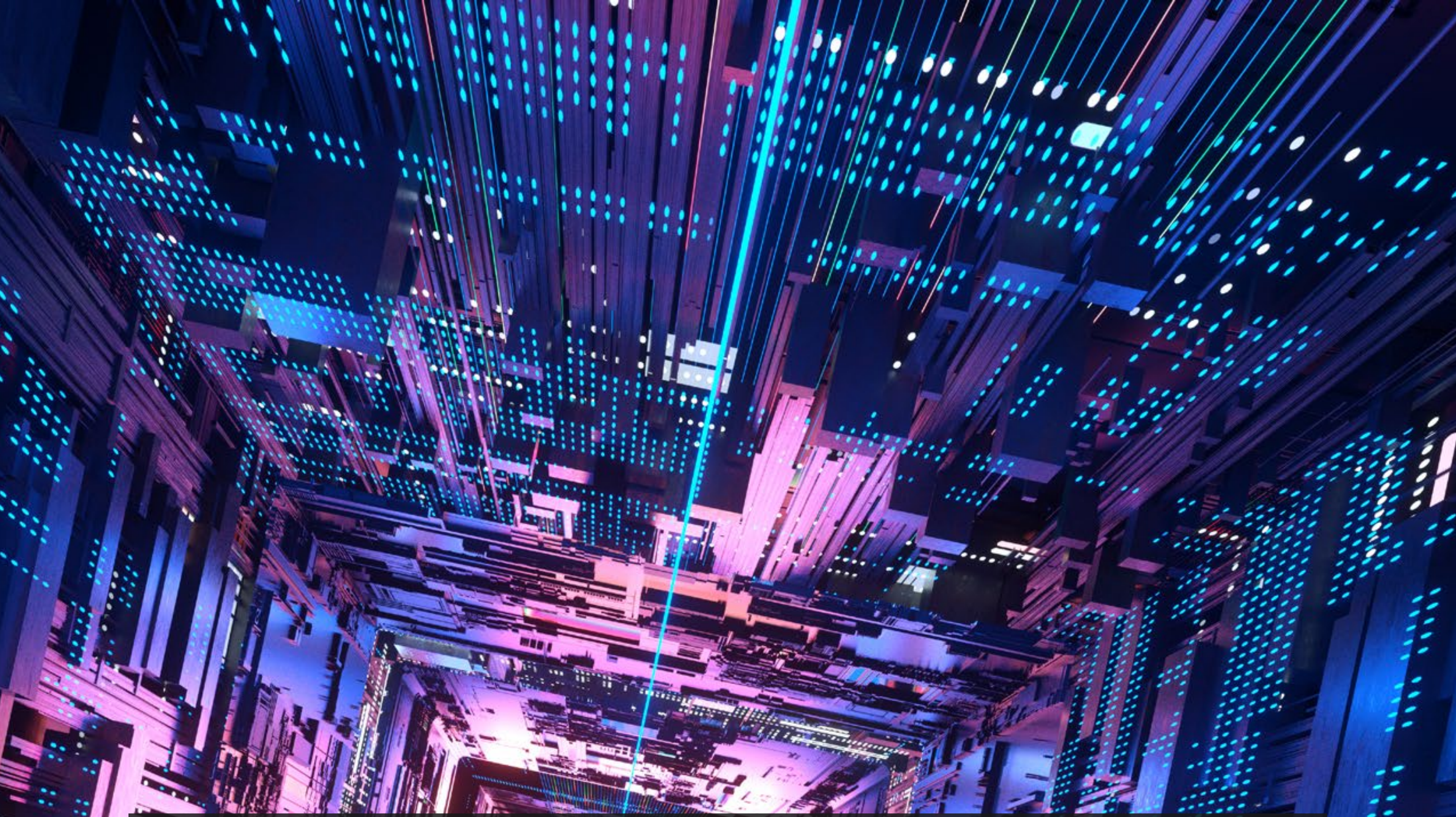


FIGURE 2. *IAVs observed during IR engagements in 2022. (Source: Secureworks)*



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
Phishing	Phishing Spearphishing Attachment Spearphishing Link Spearphishing via Service
Third-party access	Supply Chain Compromise Trusted Relationship
Pre-existing malware infection	Develop Capabilities
Drive-by download	Drive-by Compromise

The proportion of total Secureworks IR engagements where the threat actor used phishing as the IAV increased significantly from 2021 (see Figure 3). This increase is largely due to the total number of observed BEC incidents more than doubling between 2021 and 2022, as phishing was identified as the IAV in 85% of the 2022 BEC incidents. In most cases, the threat actors sent phishing emails to thousands of recipients that sometimes spanned multiple organizations.

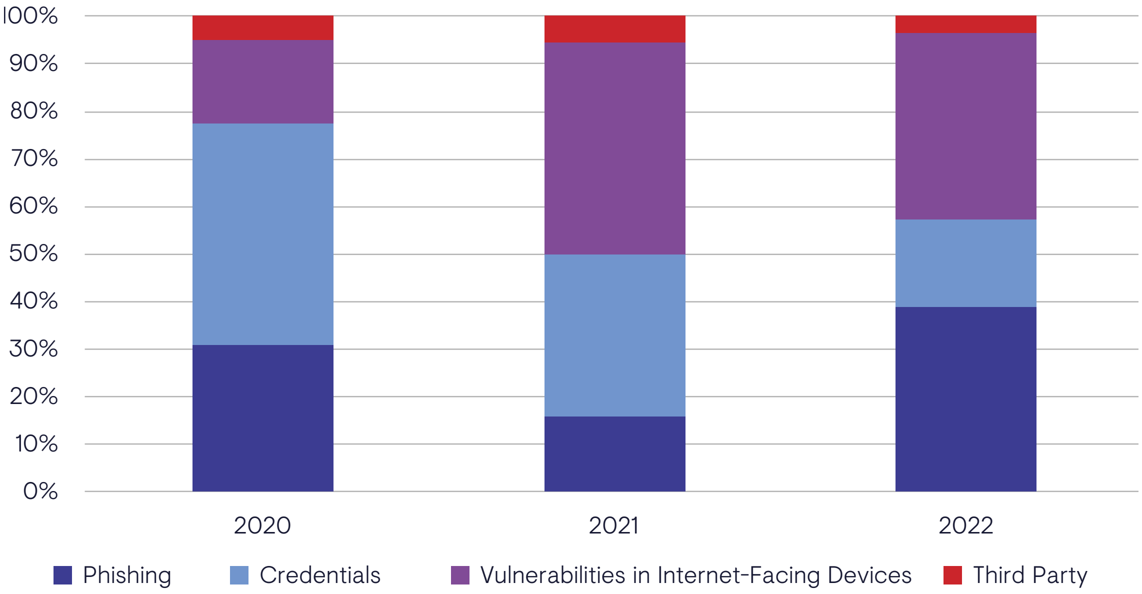


FIGURE 3. *Observed IAVs from 2020 to 2022. Credential abuse encompasses stolen credentials, brute-force attacks, and password spraying. (Source: Secureworks)*

As of this publication, BEC poses the largest monetary threat to organizations. In 2022, the U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported an increase of 65% in identified global exposed losses from BEC attacks between July 2019 and December 2021. While the payouts appear to be increasing, the technical aspects of BEC schemes remain relatively simple. News of the potential profits and low barrier to entry likely inspired other groups with little to no technical capabilities to begin conducting BEC attacks.

The proportion of Secureworks IR engagements involving the exploitation of vulnerable internet-facing devices dropped slightly in 2022 but was still significantly higher than in 2020. Secureworks observed both financially motivated and government-sponsored threat actors using this IAV. In many incidents, the threat actors leveraged publicly available information rather than identifying the vulnerabilities and developing exploit code themselves. Specifically, they weaponized proof-of-concept exploit code that security researchers published after the vulnerabilities were publicly disclosed and could then conduct bulk scanning to identify and opportunistically exploit vulnerable devices. Sometimes devices remain vulnerable for years before they are exploited. In 2022, CTU™ researchers continued to observe high-profile vulnerabilities such as ProxyLogon, ProxyShell, and Log4Shell exploited in third-party software despite patches being available since 2021.

China: Keeping vulnerability discoveries in the family

Among China, North Korea, Iran, and Russia — the most active countries conducting cyberespionage impacting Secureworks customers — China stands out for the sheer scale of its targeting. In 2022, Chinese threat actors were responsible for over 90% of the government-sponsored activity investigated by Secureworks incident responders. Chinese threat groups conduct cyberespionage in support of China's national political, military, and economic priorities. A significant proportion of Chinese threat group activity also targets organizations to steal intellectual property and trade secrets in support of China's economic development goals.

Chinese threat groups predominantly compromise networks by exploiting vulnerabilities in internet-facing devices. In 2022, Secureworks observed Chinese threat actors targeting third-party products and devices such as Zoho ManageEngine, Microsoft Exchange, Pulse Secure, and custom applications. Although much of this activity leveraged known vulnerabilities for which patches were available, the mass exploitation of Microsoft Exchange servers in March 2021 highlights the threat posed by Chinese threat actors armed with knowledge of zero-day vulnerabilities.

China-based vulnerability researchers historically dominated global contests to exploit previously unknown vulnerabilities. However, the Chinese government implemented regulations in 2017 to prohibit Chinese researchers from attending these contests. Chinese individuals and companies are also required to report vulnerabilities to the government within two days of discovery. These regulations provide the Chinese government with potentially exclusive access to zero-day vulnerabilities that could be leveraged by government-sponsored threat groups.

Understanding the attack surface of your organization's network perimeter and implementing a robust process for patching known vulnerabilities are key components of a defense-in-depth approach to network security. Implementing an endpoint detection and response (EDR) solution can be effective for identifying activity associated with exploitation of zero-day vulnerabilities. This activity may include abnormal parent-child process relationships or lateral movement.

Observations on the Threat Landscape

Secureworks IR engagements in 2022 provided insights into trends in the threat landscape.

A drop in ransomware activity?

There were 57% fewer Secureworks IR engagements involving ransomware in 2022. In addition to the potential impact on cybercrime from the Russian invasion of Ukraine, there are several other possible explanations for this seeming decrease in ransomware activity:

- Ransomware groups seek to maximize their revenue and simultaneously avoid high-impact, high-profile intrusions that attract the attention of government and law enforcement agencies. The U.S. government's response in 2021 to high-profile attacks against Colonial Pipeline, JBS, and Kaseya inflicted significant costs on the ransomware groups responsible. Law enforcement agencies around the world pursued these ransomware groups as well as others, in some cases arresting individuals linked to malicious activity. To avoid a similar fate, some ransomware groups proactively shuttered existing schemes and rebranded.
- It is possible that ransomware groups are targeting lower-profile organizations that may not enlist external incident response resources during an intrusion. This targeting could explain why third-party reporting shows an overall reduction in ransomware payments in 2022. These organizations likely pay a lower ransom, if any.
- Organizations could be implementing EDR solutions that identify ransomware precursor activity. These solutions thwart follow-on ransomware deployment by detecting the Cobalt Strike adversarial framework and other tactics, techniques, and procedures (TTPs) common to many ransomware groups.

However, predictions of the imminent demise of ransomware-as-a-service (RaaS) operations failed to come true in 2022. The number of victims listed on ransomware leak sites monitored by CTU researchers did not significantly decrease from 2021 to 2022, although there were monthly fluctuations (see Figure 4).

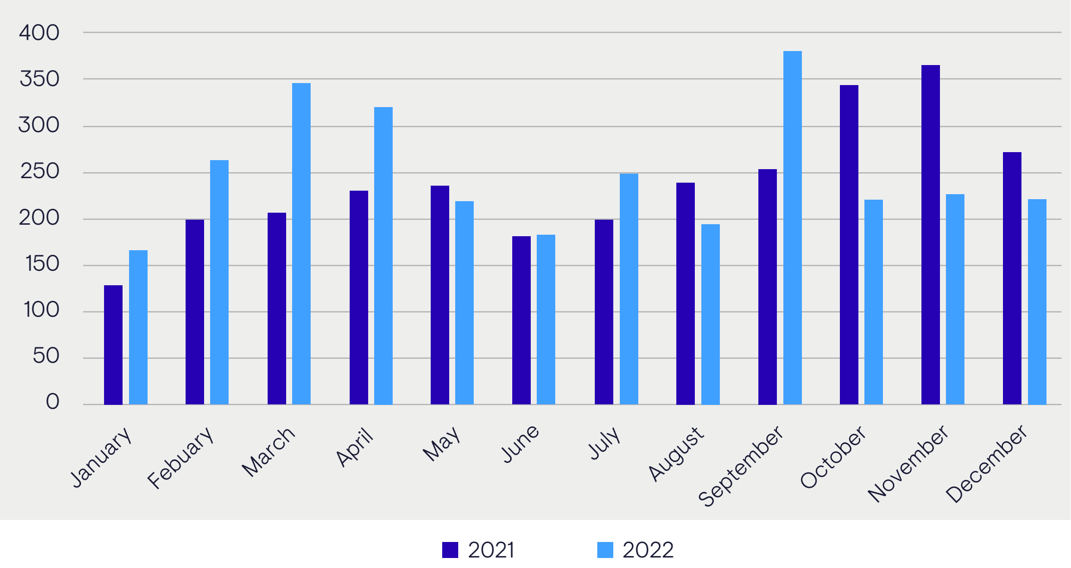


FIGURE 4. *Victims added to ransomware leak sites in 2021 and 2022. (Source: Secureworks)*

CTU analysis of trends in the name-and-shame ransomware landscape revealed RaaS operations that continued to impact a large number of victims. The financially motivated GOLD MYSTIC threat group published 920 victim names to its LockBit leak site in 2022, representing nearly 33% of the total number of victims posted across all ransomware leak sites during the year. In September alone, 228 LockBit victims were added. The increased activity could be linked to an alleged GOLD MYSTIC representative's claims that LockBit 3.0 included improved features and an expanded infrastructure.

Other prolific ransomware operations included ALPHV (also known as BlackCat), Conti, and Black Basta. In November, Secureworks investigated multiple intrusions where Qakbot malware led to Black Basta deployment. The GOLD REBELLION threat group that operates Black Basta posted the first victim to its leak site in April. In the analyzed incidents, data exfiltration and ransomware deployment occurred within 24 hours of initial access. CTU researchers recommend that organizations review the TTPs from these incidents and verify that their security controls will mitigate these threats. In particular, network defenders should implement controls to detect and block Qakbot.

MFA not a 'fire and forget' security control

Multi-factor authentication is one of the most effective ways to mitigate credential-based attacks and reduce the likelihood of a network compromise. An increase in the number of organizations implementing MFA could be why Secureworks incident responders observed a decline in stolen credentials as an IAV in 2022. However, as more organizations adopt MFA, threat actors are discovering innovative ways to bypass it or to focus their attention on other IAVs.

In 2022, Secureworks IR engagements revealed BEC actors attempting to bypass MFA using various techniques. BEC actors have successfully bypassed MFA by sending authentication requests that the victim approves without verifying. In MFA fatigue attacks, which may be increasing in popularity, a threat actor repeatedly attempts to log in to the same account using stolen credentials. This behavior sends multiple MFA push requests to the account owner's mobile device, and the influx can lead to the account owner approving the authentication request.

In one incident, a threat actor obtained an organization's Office 365 usernames and passwords via phishing. The threat actor then gained access to some accounts after subjecting users to an MFA fatigue attack. The organization detected this activity and quickly remediated the intrusion. This incident highlights the importance of monitoring access to key corporate resources even when fundamental security controls such as MFA are in place. One way to mitigate the risk of MFA fatigue attacks is to implement MFA notifications that require the user to enter a code rather than choosing 'confirm' or 'approve.' Fortunately, many of these attacks fail because the user appropriately denies the request or reports the incident to their organization.

While this incident involved corporate devices, the harvesting of corporate data from personal devices using infostealers is a growing threat to organizations. Personal devices often have weaker security controls than corporate-owned devices and may contain corporate credentials that could be used in MFA fatigue attacks or provide an IAV into the corporate network. Threat actors have also demonstrated MFA interception capabilities such as phishing campaigns that prompt a user to visit a website masquerading as a legitimate corporate site and enter their credentials and the second-factor code from their device. Network defenders should consider implementing phishing-resistant MFA such as physical tokens to prevent this type of attack.

Threat actors updating tradecraft for cloud technologies

The COVID-19 pandemic accelerated the shift toward managed cloud-based solutions for many organizations. These solutions were often implemented in haste and without full consideration of the security implications. Organizations can benefit from the security controls offered by these cloud providers, but those controls need to be implemented correctly. Secureworks incident responders often investigate intrusions where fundamental security controls were absent or misconfigured. Even when security controls are in place, cloud environments may still present vulnerabilities that threat actors could leverage to gain a foothold.

As organizations transition to cloud-based services, threat actors are forced to develop new tradecraft to achieve their post-intrusion objectives. Secureworks incident responders discovered a likely Chinese cyberespionage group pivoting from a compromised on-premises network to the organization's Azure Active Directory (AD) tenant when the two systems were synchronizing accounts. The threat actor gained initial access to the on-premises network by exploiting the ProxyShell vulnerabilities on an internet-facing Microsoft Exchange server. After accessing the Azure AD tenant, the threat actor registered a single-tenant application with Exchange Web Services (EWS) API permissions that enabled them to access the organization's mailboxes from Exchange Online.

Regardless of whether an organization's environment is on-premises, cloud-based, or a hybrid solution, it is only as strong as its weakest link. This example reinforces the fundamental need for network defenders to mitigate risks based on this changing attack surface. CTU researchers recommend that network defenders understand what data their logs are collecting from cloud environments and how the data is retained. Appropriate logging, ideally in a centralized and managed logging platform, provides visibility into user activity in a cloud environment and across the organization's estate. Log data can reveal unusual activity and provide insight into the scope and impact of an intrusion, which is essential for effective remediation.

Recommendations

Following IR engagements, Secureworks provides granular recommendations about security controls that would have minimized the impact of the incident, advising the customers to prioritize these controls to avoid reoccurrence. Security controls that are often lacking in compromised environments include comprehensive deployment of an EDR solution; centralized log retention and analysis across host, network and cloud resources; and reputation-based web filtering and network detection for suspicious domains and IP addresses.

Conclusion

CTU researchers track threats and behaviors observed 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

Abrams, Lawrence. "MFA Fatigue: Hackers' new favorite tactic in high-profile breaches." Bleeping Computer. September 20, 2022.

Asokan, Akshaya. "Microsoft Exchange Flaw: Attacks Surge After Code Published." GovInfoSecurity. March 20, 2021.

Chainanalysis. "Ransomware Revenue Down As More Victims Refuse to Pay." January 19, 2023.

Dignan, Larry. "Colonial Pipeline cyberattack shuts down pipeline that supplies 45% of East Coast's fuel." ZDNET. May 8, 2021.

Hageman, Mitchell. "Secureworks CTU identifies increase in stolen credential sales." SecurityBrief Asia. December 5, 2022.

Makortoff, Kalyeena. "World's biggest meat producer JBS pays $11m cybercrime ransom." The Guardian. June 10, 2021.

Microsoft. "HAFNIUM targeting Exchange Servers with 0-day exploits." March 2, 2021.

Red Hot Cyber. "RHC interviews LockBit 3.0. 'The main thing is not to start a nuclear war'." July 26, 2022.

Secureworks. "Azure Active Directory Flaw Allows SAML Persistence." January 18, 2023.

Secureworks. "BRONZE STARLIGHT Ransomware Operations Use HUI Loader." June 23, 2022.

Secureworks. "How to Prevent Multi-factor Authentication Bypass." June 7, 2022.

Secureworks. "Kaseya VSA Software Under Active Attack." July 3, 2021.

Secureworks. "Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?" December 17, 2021.

Secureworks. "Secureworks FAQ: Russian Activity in Ukraine." February 24, 2022.

Secureworks. "Think MFA is Hack-Proof? Think Again." April 30, 2020.

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 (CISA). "Implementing Phishing-Resistant MFA." October 2022.

U.S. Federal Bureau of Investigation. "Business Email Compromise: The $43 Billion Scam." May 4, 2022.