Secureworks®

Learning from Incident Response: 2021 Year in Review

Secureworks® Counter Threat Unit™ Research Team

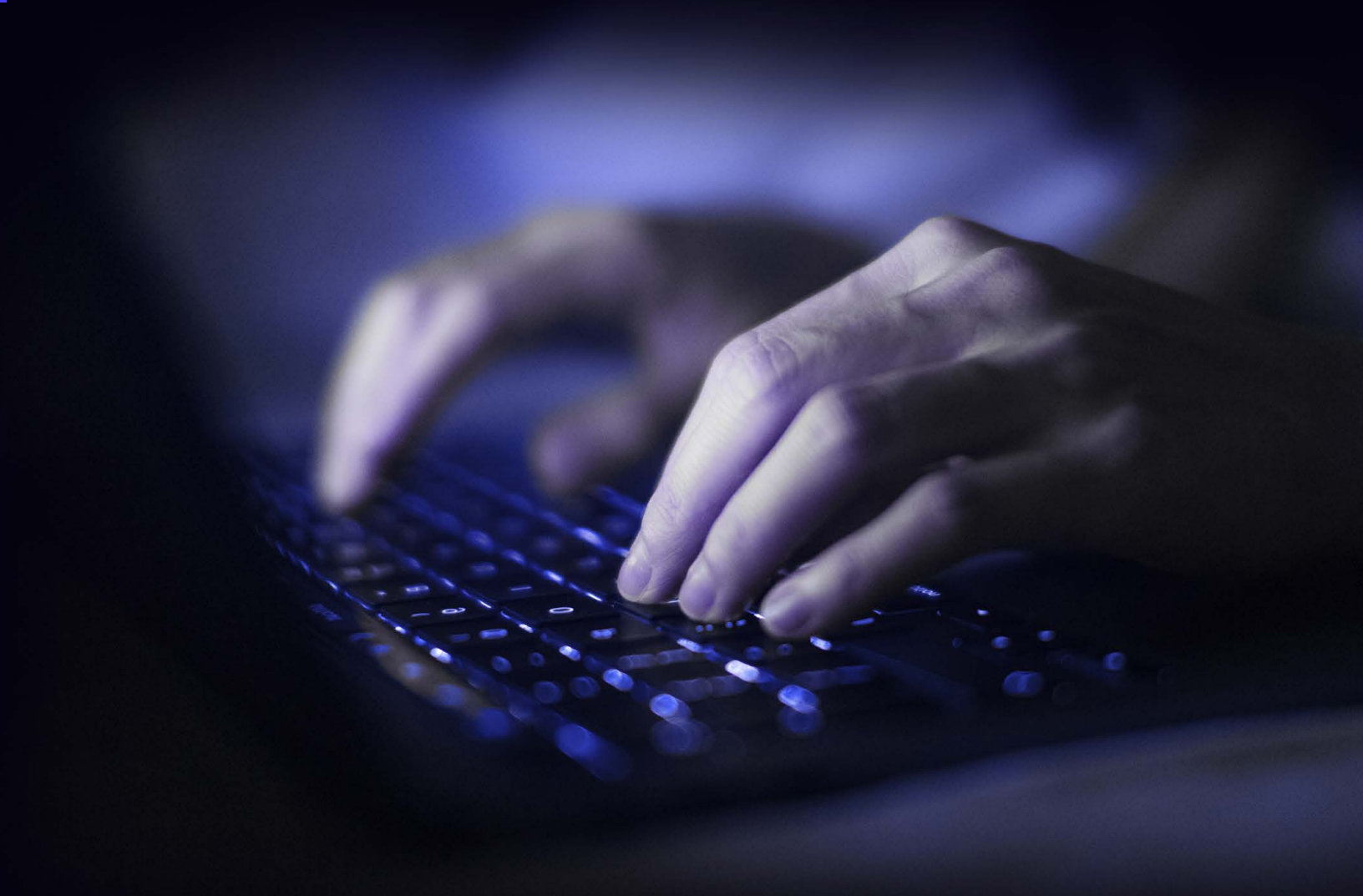
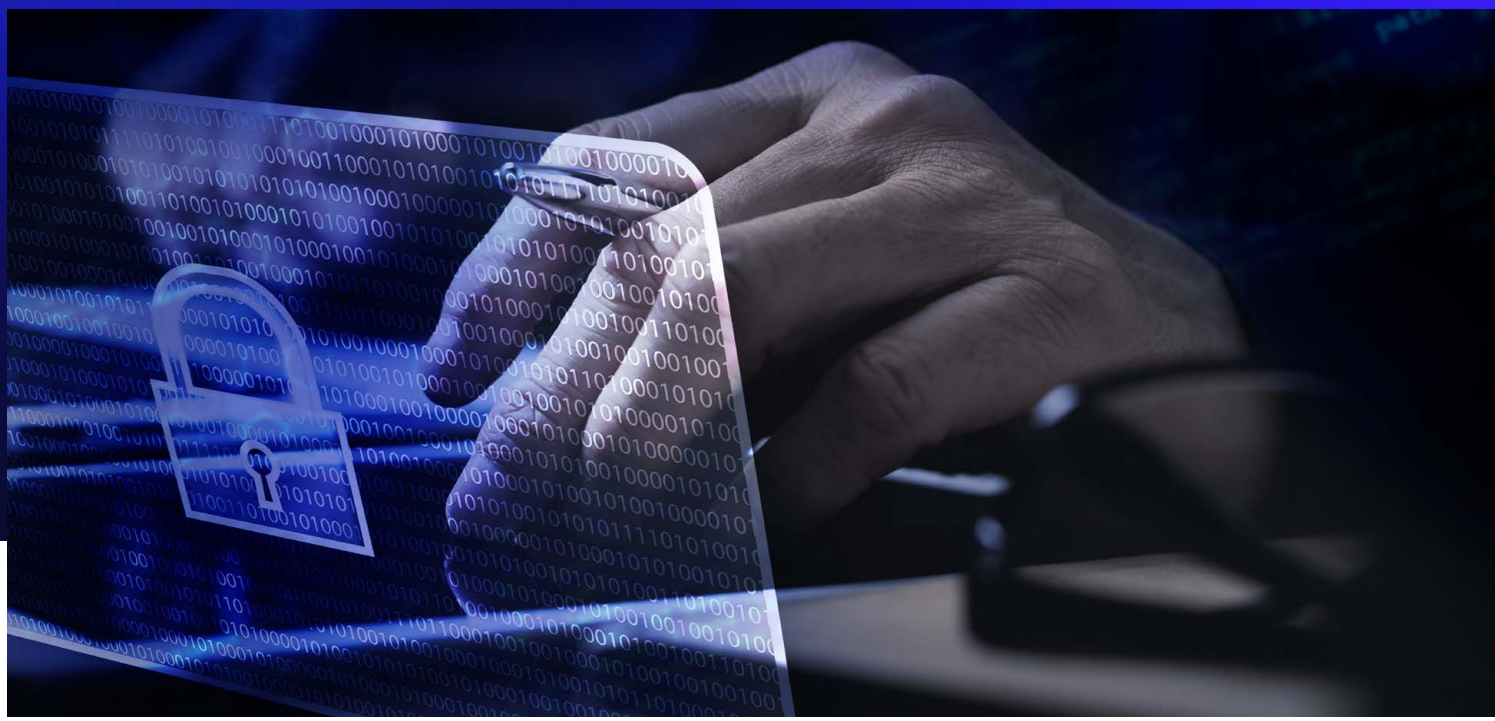


Table of Contents



Summary

Secureworks® incident response (IR) engagements in 2021 revealed trends about threats and threat actor behaviors. Between January and December 2021, Secureworks incident responders assisted in the containment and remediation of over 450 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 the greatest threat to organizations due to the very high impact these attacks can cause. There was no decrease in ransomware attacks in the latter half of 2021, despite increased law enforcement intervention following the Colonial Pipeline and Kaseya ransomware incidents. Ransomware groups increasingly adopted 'name-and-shame' tactics, threatening to publicly leak stolen data as additional leverage.

Exploitation of vulnerabilities in internet-facing systems (also known as scan-and-exploit attacks) replaced credential-based attacks as the most common initial access vector (IAV).

Multi-factor authentication (MFA) and cloud-based hosting offer security benefits. However, Secureworks IR engagements revealed that incidents can occur if these controls are not properly implemented.

Observed Trends

Cybercrime continued to represent the greatest threat to Secureworks customers, with approximately 85% of incidents attributed to financially motivated cybercriminals. By comparison, hostile government-sponsored activity was observed in approximately 5% of Secureworks IR engagements. The remaining approximately 9% is composed of deliberate or accidental actions by organizations' employees that resulted in a security incident. This proportional breakdown is broadly consistent with previous years (see Figure 1), with the exception of the very high number of financially motivated incidents in 2020.

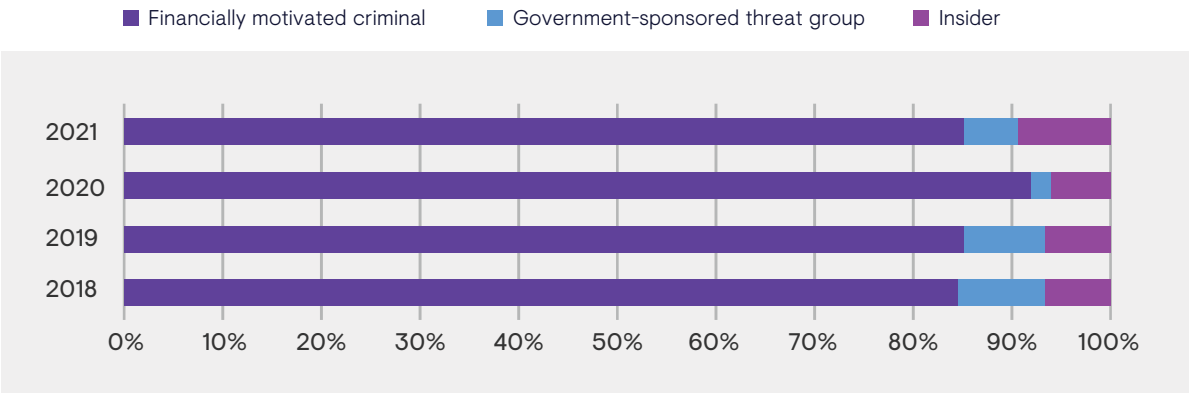


FIGURE 1. *Breakdown of threat actor types observed in Secureworks IR engagements from 2018 through 2021. (Source: Secureworks)*

The financially motivated incidents in 2021 involved threats such as ransomware, business email compromise (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

The most frequently observed initial access vector (IAV) in 2021 was the exploitation of vulnerabilities in internet-facing devices, which accounted for 48% of IR engagements where the IAV could be determined. The second-most common IAV was credential abuse, including the use of credentials that were stolen or purchased on the dark web, brute-force attacks, and password spraying (see Figure 2).

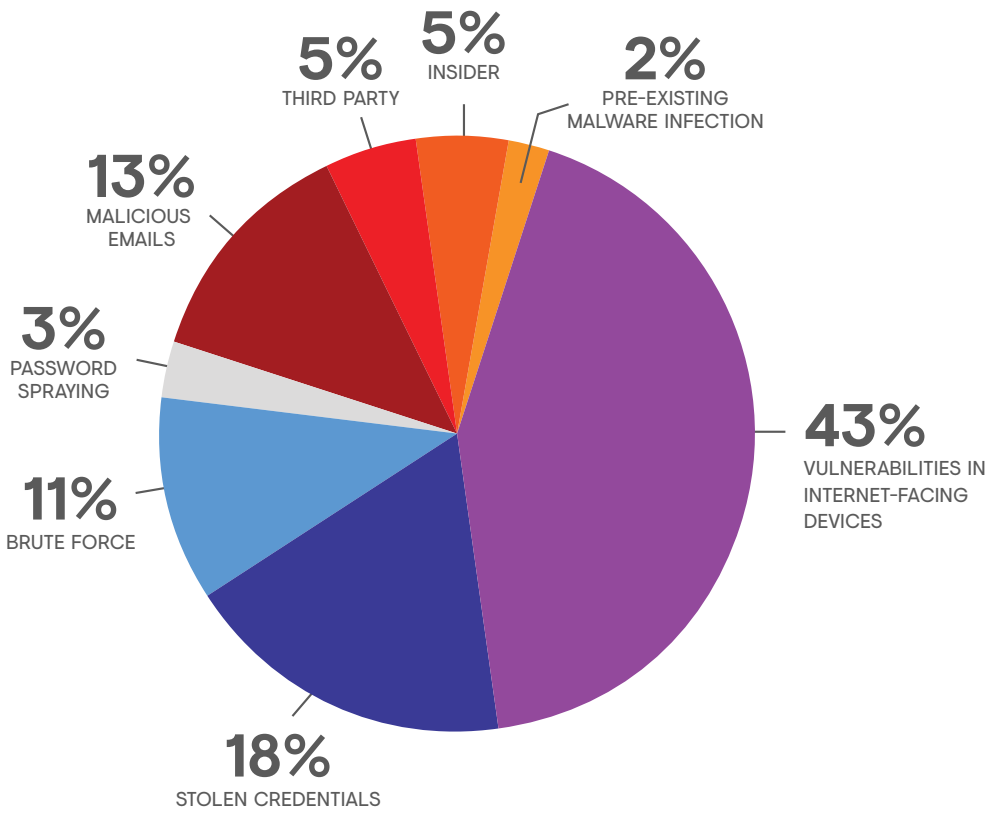
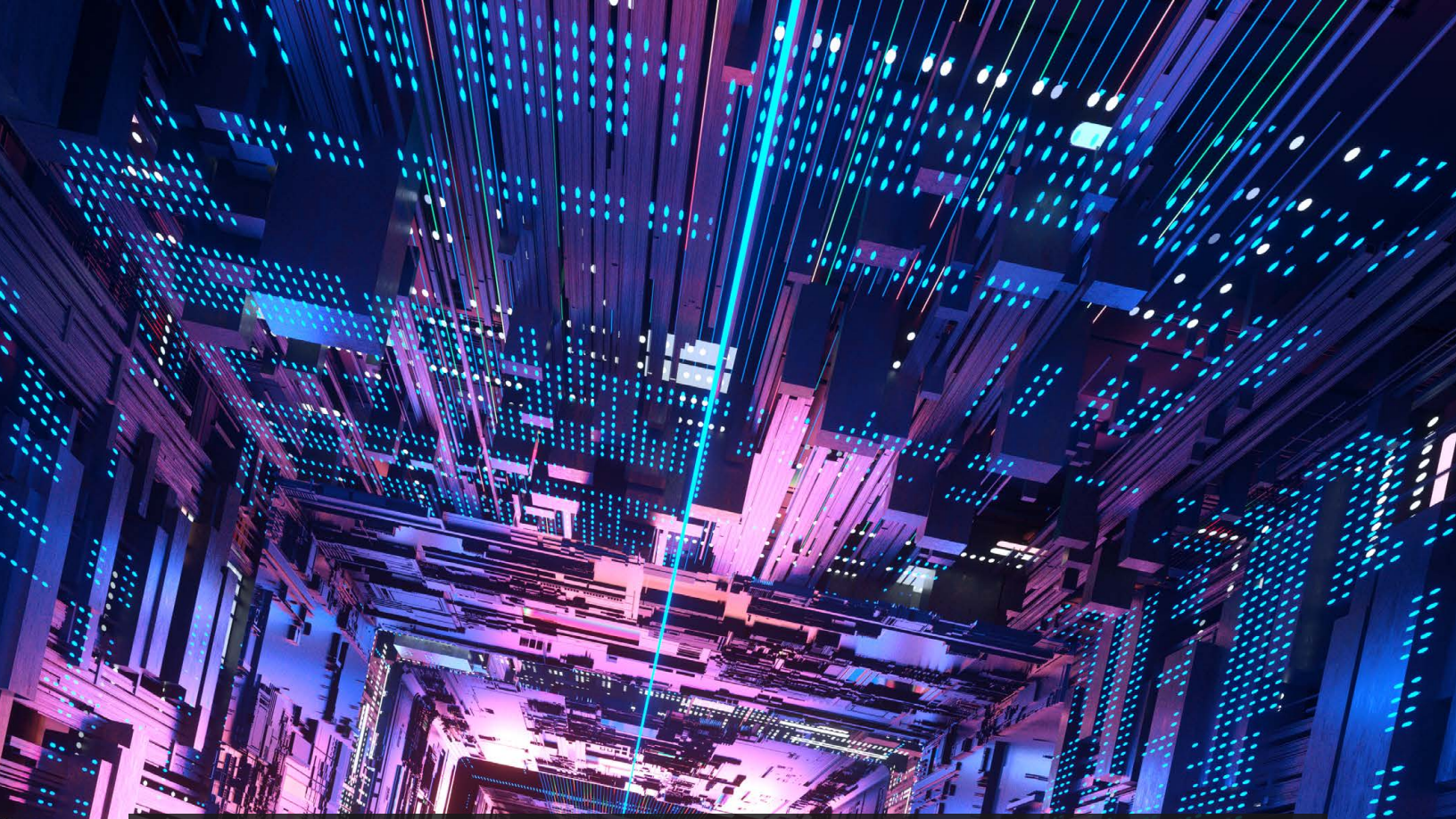


FIGURE 2. *IAVs observed during IR engagements in 2021. Due to rounding, the percentages may not add up to 100%. (Source: Secureworks)*



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

The predominance of exploitation of internet-facing systems is a noticeable change from 2020, when credential-based access was the most common IAV (see Figure 3).

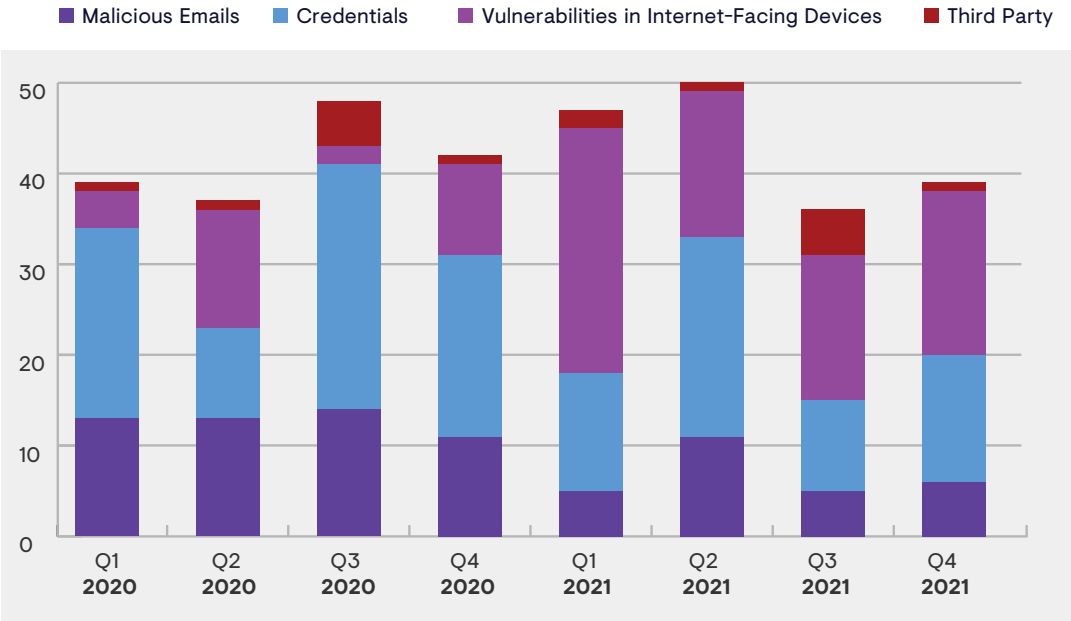


FIGURE 3. *Observed IAVs in 2020 and 2021. (Source: Secureworks)*

This shift is not likely to be quite so stark as the data suggests. CTU™ researchers observed an increase in the proportion of IR engagements where a vulnerability is exploited following the public exposure of high-profile issues. For example, multiple Secureworks IR engagements focused on the ProxyLogon vulnerability following its global exposure in early March. Even so, it is likely that there is a general increase in incidents resulting from exploitation of internet-facing systems.

One reason for this trend could be that increased implementation of multi-factor authentication (MFA) has led to a decline in attacks that use stolen credentials for their IAV. Microsoft has long claimed that MFA blocks the vast proportion of cyberattacks. In the overwhelming majority of Secureworks IR engagements involving credential abuse, the threat actors leveraged remote access solutions that did not enforce MFA. However, it is difficult to determine how many security incidents were prevented because the potential victim implemented MFA.

Another reason could be that threat actors weaponize proof-of-concept exploit code that the security testing community publishes shortly after vulnerabilities are publicly disclosed. Coupled with bulk scanning, threat actors can conduct widescale opportunistic exploitation of vulnerable devices.

2021: Year of the Exploit?

There were several high-profile incidents involving opportunistic mass exploitation of popular third-party software in 2021:

- The ProxyLogon vulnerability (CVE-2021-26855) disclosed in March and the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) disclosed in August impacted on-premises Microsoft Exchange servers. ProxyLogon was exploited by multiple Chinese threat groups in targeted attacks prior to the vulnerability being disclosed, quickly followed by more widespread opportunistic exploitation once exploit code became publicly available.
- A supply chain attack launched in July by an affiliate of the GOLD SOUTHFIELD threat group exploited a Kaseya VSA Remote Monitoring and Management vulnerability (CVE-2021-30116) to distribute REvil ransomware. The impact on affected organizations varied, depending on how widely Kaseya's software was deployed. In at least some cases, mitigation caused significant operational downtime.
- In December, threat actors performed mass scanning and attempted exploitation of a vulnerability (CVE-2021-44228, also known as Log4Shell) in the ubiquitous Log4j Java logging library. It transpired that the vulnerability was not as easy to reliably exploit as had initially been feared. However, there were widespread compromises of third-party applications that used Log4j, including VMware Horizon servers.

In addition, there were targeted attacks against vulnerable third-party software. Chinese threat actors targeted ManageEngine Desktop Central, financially motivated cybercriminals targeted SonicWall VPN appliances, and the Iranian COBALT GYPSY threat group targeted Microsoft SharePoint.

Observations on the Threat Landscape

Secureworks IR engagements in 2021 provided insights into trends in the threat landscape.

Ransomware landscape remains resilient

In May 2021, an affiliate of the GOLD WATERFALL threat group's Darkside ransomware-as-a-service (RaaS) operation targeted U.S. oil distributor Colonial Pipeline in an attack that caused a six-day outage and reportedly cost $4.4 million USD in ransom payments. The total monetary loss is likely millions more due to the lost revenue from the unavailability of operational systems and the recovery costs. U.S. law enforcement responded aggressively, seizing $2.3 million USD in cryptocurrency assets reportedly owned by GOLD WATERFALL. Following the July attack that leveraged Kaseya software to deploy REvil, the Biden administration put ransomware on the agenda for presidential-level talks between the U.S. and Russia. These developments, coupled with the 'retirement' (or more accurately, rebranding) of groups like GOLD WATERFALL inspired hope that Western law enforcement and government agencies could cause sustained disruption to the ransomware landscape.

Secureworks IR data does not indicate a reduction in ransomware activity following these actions. Of the 78 ransomware IR engagements in 2021, 37 occurred in the first half of the year and 41 in the second half (see Figure 4). However, four of the engagements in the most active month (July) were related to the Kaseya supply chain attack.

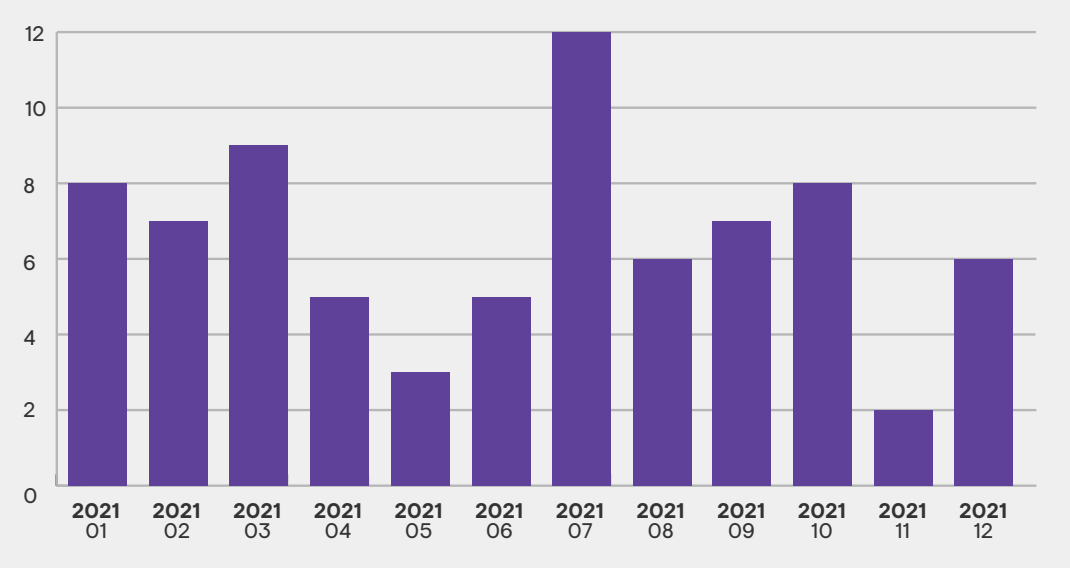


FIGURE 4. *New ransomware engagements in 2021. (Source: Secureworks)*

Data from ransomware leak sites also indicates that ransomware activity has persisted. While this data only reflects organizations that have been publicly named and likely represents only a fraction of total victims, it appears to show an increase in both the rate of new victims (see Figure 5) and the number of distinct active ransomware schemes (see Figure 6). This activity suggests that the ransomware landscape continues to thrive.

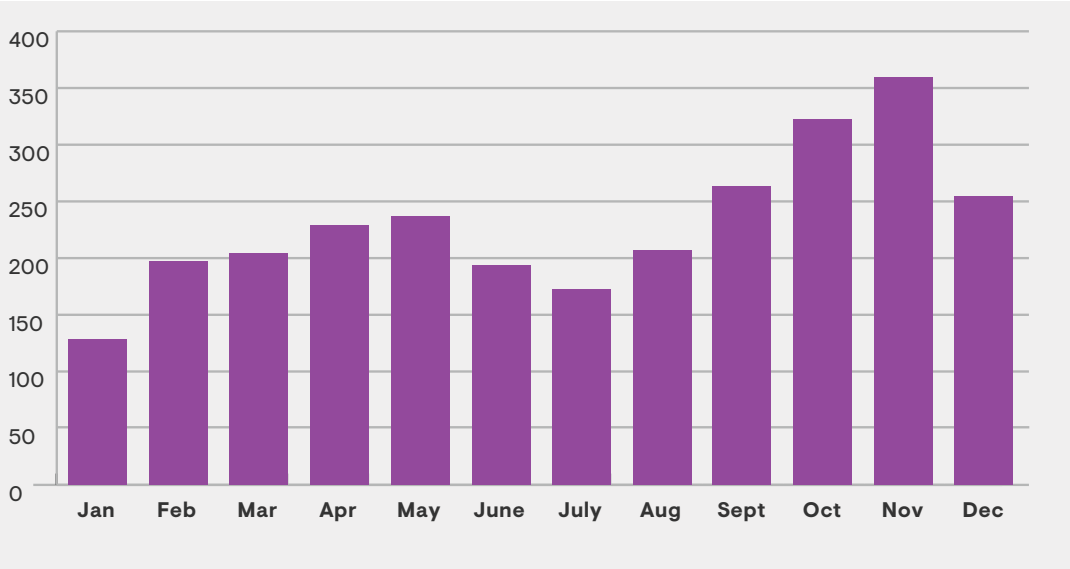


FIGURE 5. *New victims named on ransomware leak sites in 2021. (Source: Secureworks)*

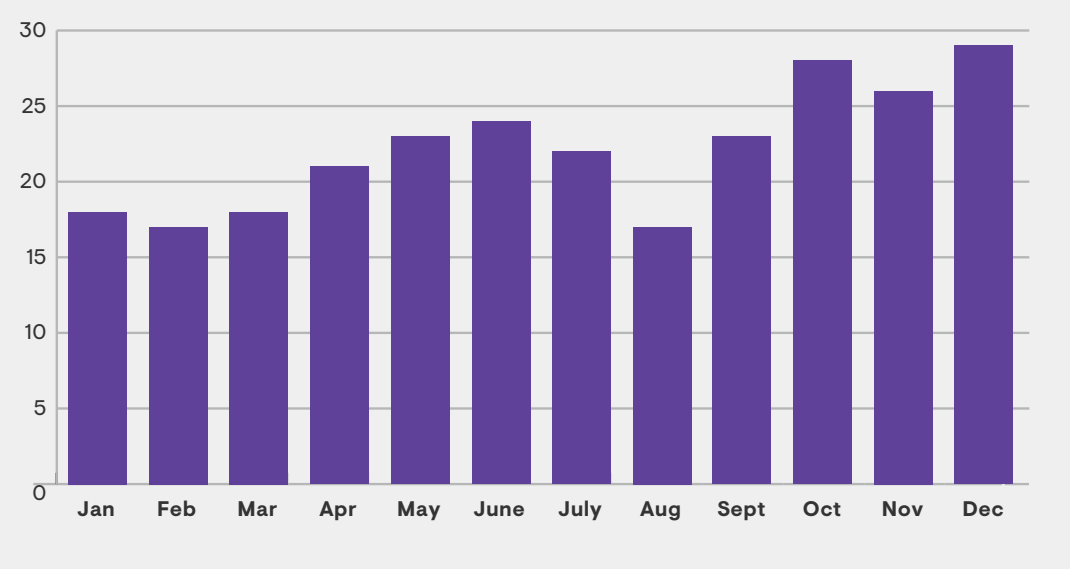


FIGURE 6. *Active name-and-shame ransomware schemes by month in 2021. (Source: Secureworks)*

Misconfigured MFA can be circumvented

Stolen credentials continued to represent a significant proportion of IAVs identified during Secureworks IR engagements. Most of these incidents were due to single-factor authentication on remote access solutions such as RDP gateways or VPN endpoints. Implementing MFA is therefore a popular recommendation made by Secureworks incident responders.

However, MFA is only effective if it is implemented properly and if users are trained how to respond to suspicious activity. As the adoption of MFA increases, there is evidence that threat actors are exploring ways to effectively bypass it. One common method is to exploit legacy authentication protocols such as the Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), or Messaging Application Programming Interface (MAPI). These protocols cannot enforce MFA and may not have been disabled by the organization. In the third quarter of 2021, a threat actor used this technique in a BEC attack that attempted to defraud an organization of hundreds of thousands or potentially millions of dollars.

User behavior can be a contributory factor in the failure of MFA as a preventative control. In one incident, a phishing email containing a link purportedly to a legitimate SharePoint site tricked a user into revealing their username and password. The threat actors then repeatedly attempted to log in, generating multiple MFA push notifications that the victim eventually approved. After gaining access, the threat actors abused the compromised email account to request a password reset on multiple social media accounts owned by the victim. The threat actors then sent convincing phishing emails to over 1,000 employees at the victim's organization in an attempt to compromise other accounts.

Another aspect of user behavior that impacts MFA is 'notification fatigue.' Frequent requests to re-authenticate to corporate systems can desensitize users from detecting suspicious activity. In one incident, a victim inadvertently granted threat actors access to an Office 365 email account in the mistaken belief that one of the victim's devices had generated the MFA approval request. The threat actors then used this access to send phishing emails internally to compromise other user accounts. Using MFA notifications that require the user to enter a code rather than choosing 'confirm' or 'approve' is one way to mitigate this risk.

Although these attack techniques are basic, they remain effective. Until organizations increase their security maturity to render the techniques ineffective, threat actors will keep using them. Meanwhile, threat actors have employed more advanced, although not necessarily sophisticated, techniques. For example, Secureworks incident responders have encountered threat actors enrolling their devices on accounts that are not protected by MFA. In mid-June, an organization first learned that this technique was leveraged against it when an investigation into suspicious activity on a user account identified two phone numbers used to enroll for MFA, neither of which belonged to the victim.

Cloud is not a panacea

For most organizations, shifting resources into managed cloud solutions provides access to the security controls offered by the cloud providers. However, those controls need to be implemented correctly. Secureworks incident responders often investigate intrusions where fundamental security controls were absent. In those situations, critical data assets hosted on managed cloud solutions are no more secure than on-premises configurations, with the added disadvantage of potentially having less access to critical forensic data.

In one incident, an Azure virtual machine (VM) was inadvertently exposed to the internet with no firewall protection. A threat actor accessed the host using stolen credentials and deployed Sharebyy (also known as InfoDot) ransomware to approximately 200 hosts. A lack of logging in the cloud infrastructure meant that it was not possible to determine when the user credentials were compromised. In another incident, a customer became aware of suspicious connections into one of their AWS accounts. The investigation revealed unauthorized access by employees of a third party whose contract with the compromised organization had been terminated. Failure to revoke the third party's access following termination enabled the incident.

Organizations must consider cloud environments in their IR procedures. For example, rapidly restoring virtualized systems to a known-good backup is an attractive design feature of managed cloud solutions. However, this capability can hinder an IR investigation that seeks to understand how a threat actor gained access. In one incident, an organization's managed service provider (MSP) rapidly restored systems and lost data. As a result, the IR investigation was unable to determine the IAV. Consequently, the organization could not verify that it properly addressed residual risk from a threat actor regaining access in the same manner.

Recommendations

The top 20 recommendations made by Secureworks incident responders in 2021 (see Figure 7, next page) reflect the main threats that face Secureworks customers. Regular vulnerability scanning to identify and reduce the external attack surface is a key component of defending against scan-and-exploit attacks. Several of the recommendations focus on preventing or reducing the impact of post-intrusion ransomware attacks, such as implementing IP address allow lists, segmenting networks, improving backup strategies, and removing generic accounts. Monitoring for newly registered spoofed domains, limiting mail-forwarding functionality, and implementing DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) authentication mitigate email-based threats and BEC attacks, which continue to cost victims millions of dollars.

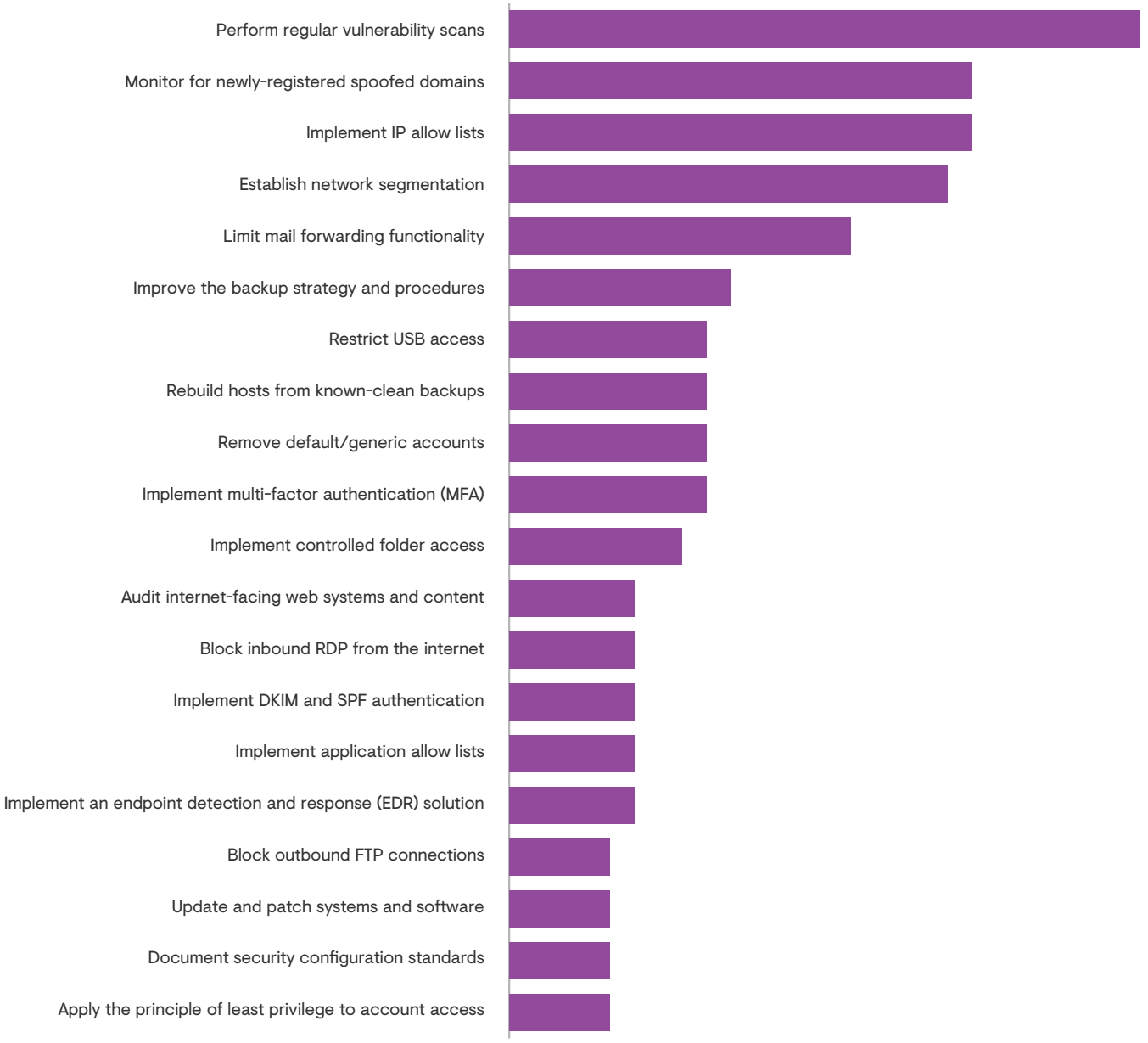
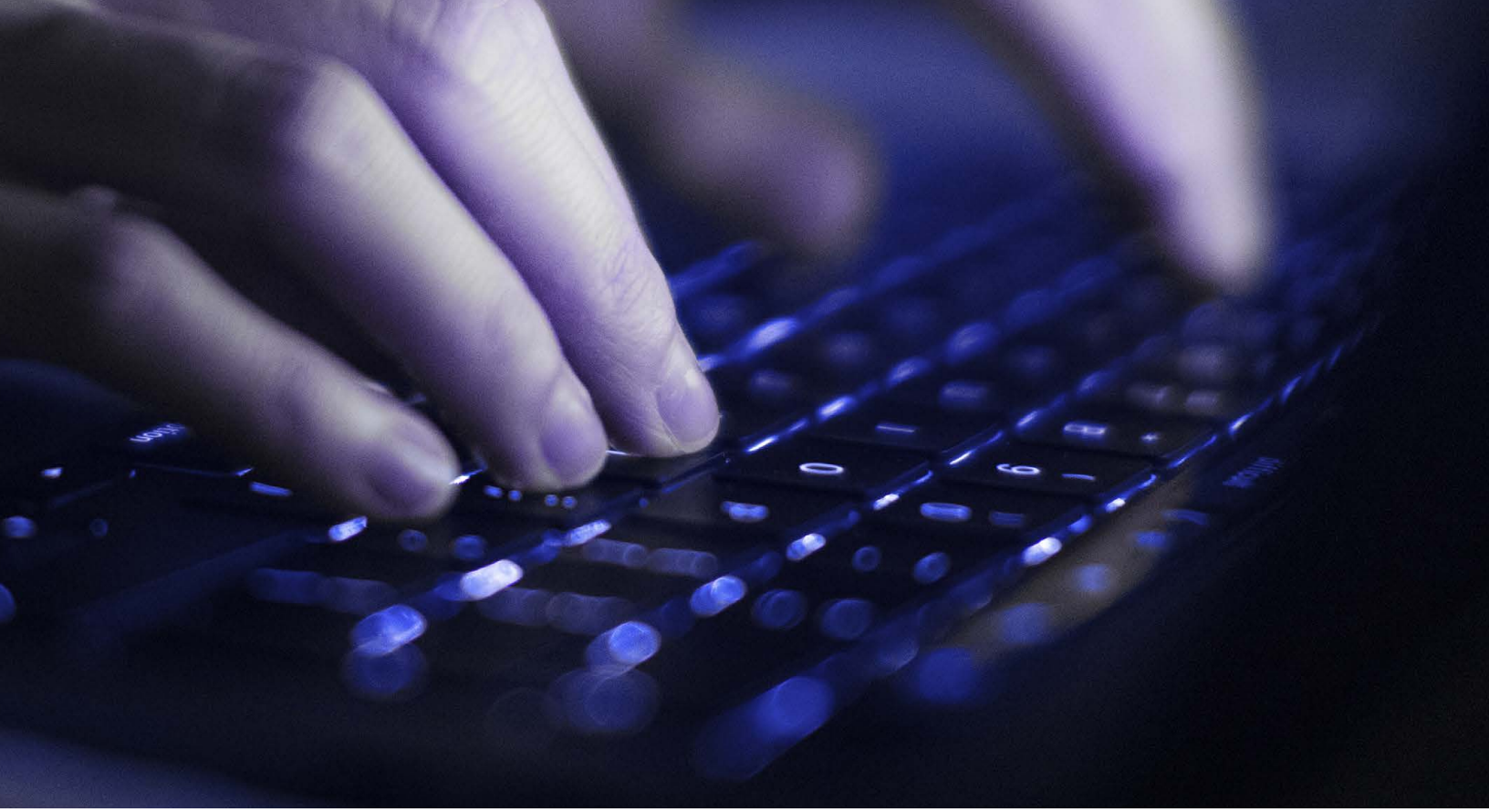


FIGURE 7. *Top 20 recommendations provided during Secureworks IR engagements in 2021. (Source: Secureworks)*



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.

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

Sources

Bussewitz, Cathy. "Colonial Pipeline confirms it paid $4.4M to hackers." Associated Press. May 19, 2021.

Greve, Joan E, and Bekiempis, Victoria. "Colonial pipeline reaching full capacity after cyberattack, Biden says." The Guardian. May 13, 2021.

Kaseya. "VSA advisory." August 4, 2021.

Maynes, Melanie. "One simple action you can take to prevent 99.9 percent of attacks on your accounts." Microsoft. August 20, 2019.

Secureworks. "Log4j Vulnerability FAQs." December 17, 2021.

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

Secureworks. "REvil/Sodinokibi Ransomware." September 24, 2019.

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

Tidy, Joe. "Swedish Coop supermarkets shut due to US ransomware cyber-attack." BBC. July 3, 2021.

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

Tung, Liam. "FBI: Hackers are actively exploiting this flaw on ManageEngine Desktop Central servers." ZDNet. December 21, 2021.

United States Department of Justice. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." June 7, 2021.