ARCTIC WOLF LABS

ARCTIC WOLF LABS

THREAT REPORT 2023

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The economics of cybercrime took a real hit, too, as the average loss from a successfully executed BEC attack was 'only' $79,000 USD, significantly less than the typical demands for ransomware.

As crucial as these insights are, applying them is often left for the practitioner to figure out on their own. This report aims to help you plan for:

- The major threat landscape shifts powered by AI and economic instability
- The long, long tail of the vulnerability lifecycle, starring the seemingly immortal Log4Shell and ProxyShell from 2021
- The growth of as-a-service-driven ransomware
- The five most successful tactics, techniques, and procedures (TTPs) in 2022 and what that means for you in 2023

Cybersecurity is a team game that aims to reduce risk and increase resilience. Protecting yourself in isolation, without

INTRODUCTION

INTRODUCTION

The 2023 Arctic Wolf Labs Threat Report aims to combine our security researchers', data scientists', and security developers' most forward-thinking ideas with practical guidance you can apply to protect your organization.

The Arctic Wolf Security Operations Cloud, with its open XDR architecture fuels this report, processing 3+ trillion security events weekly and generating 4.8+ petabytes of data from endpoints, networks, cloud, identity, human sources, and more. We aim to provide insights that transcend any technology or attack surface by combining this vast dataset with Arctic Wolf's threat and malware intelligence data and findings from our digital forensics and incident response work.

Our predictions and insights on the year ahead focus on the macro and micro changes to the threat landscape, including incident response, investigations, insights, and trends. Though the threat landscape is constantly evolving, and the threat actors regularly change their tactics, techniques, and procedures (TTPs), the unfortunate victims of cybercrime give everyone in the security community the opportunity to learn from and react to the

CYBERSECURITY PREDICTIONS

01 Geopolitical Instability and Economic Stress Will Drive Cybercrime Increases

During times of economic strife and political instability, new opportunities and incentives are created for cybercriminals.

With the long tail of the COVID-19 pandemic, high rates of inflation, and major conflicts such as the ongoing war between Russia and Ukraine, we predict that more individuals with technical skills will be incentivized to resort to cybercrime. These individuals will seek to reap the profits of illicit activity such as BEC, phishing, ransomware, extortionware, and other tactics.

Research for the Arctic Wolf State of Cybersecurity: 2023 Trends Report showed that small and midsize businesses (SMBs) are more severely impacted by cybercrime in the current economic climate because their budgets tend to either stay the same or decrease, making the payment of ransom demands more costly. On the other hand, enterprise scale organizations tend to increase spending on their cybersecurity efforts.

The release and rise of ChatGPT, and now GPT-4, by OpenAI has been greeted with much fanfare and mainstream press, but the real implications of its potential are not yet fully known.

ChatGPT and GPT-4 are OpenAI's fourth-generation Generative Pre-Trained Transformers, which are based on natural language techniques that provide answers in a conversational way and have been noted for its extensive capabilities.

With the broader public awareness of, and access to, AI of this nature, we expect to see more bots and automation spread disinformation across the web. We expect to see AI-generated imagery and videos used by threat actors to spread propaganda, influence public opinion, and launch advanced social engineering campaigns.

We predict that threat actors will harness AI technologies, such as ChatGPT and other AI tools to create malware. Early reports on OpenAI's generative AI applications have supported this prediction, demonstrating that the barrier to entry

AI is not the only disruptive technology that will change the cybercrime landscape.

Decentralized finance (DeFi), which leverages public blockchain ledgers to process financial transactions via smart contracts, offers an alternative to centralized financial (CeFi) systems.

While DeFi isn't inherently a new technology, 2022 has been the year that's brought DeFi to the mainstream — and there's a lot more to DeFi than just cryptocurrency. This includes non-fungible tokens (NFTs), smart contracts, tokenization, and potential token-based peer-to-peer exchanges that allow individuals to bypass centralized institutions to swap collateralized tokens.

DeFi offers threat actors a means by which they can exchange illicitly obtained crypto funds (either washed or mixed funds, or services to be rendered later via smart contracts). Beyond the exploitation of this technology also lies the potential compromise of it.

Smart contracts, for example, are just programs

03 Disruptive Technologies Will Create New Opportunities and Threats (cont.)

Web3 allows for new social engineering tactics.

Other emerging cyber environments that have increased potential for exploitation are organizations hosting virtual reality (VR) and augmented reality (AR) data.

As more data is collected through VR/AR devices, sensors, cameras, etc., and stored on servers and databases connected to the internet, these become rich targets of potentially large amounts of personal data on the user such as eye tracking data for ads and many other examples.

There is an emerging opportunity for new social engineering attacks in VR applications in Web3 applications, providing even more incentive to support DeFi services.

What it looks like in the real world

Web3 technology develops, and threat actors leverage emerging AI technologies to enhance their

With the cybercrime industry raking in $1.5 trillion USD in revenue annually, criminal groups and organizations are only gaining strength and growing in sophistication.

e103 51C>1076</L10.51 TBg 110.167.667.611 116</L05D.7.167.6 0 0 C 000g903B008930 12 16745 0.3496003B0

What it looks like in the real world

In 2019, ransomware groups found another way to put pressure on victims — a double-extortion ransomware attack.

This style of attack is where the threat actor makes a copy of some or all the data before encrypting it. If the victim refuses to pay a ransom, the sensitive data stolen from the network will be made public or sold on the black market.

Since this discovery, ransomware groups have become even more creative, adding one more layer to their attacks — a triple-extortion ransomware attack —where a victim's associates (such as partners, customers, or patients) are threatened with data leaks if the original victim refuses to pay a ransom.

These kinds of attacks increase the likelihood that an organization will pay and offer cybercriminals another route if the business doesn't play along.

Threat actors will continue to identify new ways of gaining initial access to vulnerable organizations.

Here we review several relevant techniques that we expect to see more of in 2023:

IoT/ICS being used for initial access

Threat actors may try to take advantage of appliances not supported by endpoint detection response (EDR) products, such as VoIP gateways, firewalls, or Internet of Things (IoT) devices.

In 2022, Cybersecurity and Infrastructure Security

What it looks like in the real world

Attacks targeting ICS/SCADA devices have recently been observed in Russia, Ukraine, and the US, for example. IoT devices are often left unsecure on the network, as digitization outpaces security implementations, and are therefore targeted to gain initial footholds. We expect this type of behavior to increase with the increased adoption of IoT in network environments across manufacturing, healthcare, and other industries.

Remote monitoring and management tool abuse will continue.

Remote monitoring and management (RMM) tools such as Microsoft Remote Desktop Protocol, ConnectWise Automate, and others have been a mainstay for threat actors, and we don't expect that to change any time soon.

We've also observed incidents where threat actors abused native ConnectWise functionality in social engineering campaigns against unsuspecting victims.

These types of attacks are particularly effective in environments where users expect to see ConnectWise Automate activity from their network administrators, leaving them less suspicious when confronted with an illegitimate activity that looks similar.

We expect threat actors to get more creative in

Sophisticated attacks may garner most of the attention, but more familiar email-based attacks will also continue to evolve.

BEC, already a go-to attack method for cybercriminals, will increase in frequency and cumulative financial costs, as it continues to deliver lucrative payouts for threat actors.

In fact, the FBI Internet Crime Complaint Center (IC3) [2] lists BEC as one of the most financially damaging forms of cybercrime. In 2021, reported

What it looks like in the real world

Organizations in industries such as finance, insurance, and business services regularly rely on email correspondence for invoicing and payment. These industries will continue to be a prime target for BEC attacks, as the volume of payments and wire transfers commonly conducted via email in these sectors occurs at a higher rate, presenting more opportunities for bad actors to insert themselves in these transactions.

07 High Impact Software Vulnerabilities

In 2022, only a handful of vulnerabilities were harnessed by ransomware threat actors for initial access, but the sheer volume of vulnerabilities has grown significantly year over year.

While this trend will continue in 2023, even several years old vulnerabilities have been, and will continue to be exploited by threat actors if there's a large enough unpatched installation base. Software hosted on-premises will continue to present challenges for organizations as they struggle to stay on top of patching the most impactful vulnerabilities. It's important to note that a CVSS score alone does not serve as a definitive measure of how attractive an exploit is to threat actors; a large unpatched base may be more lucrative than a singular critical vulnerability.

Supply chain exploits are expected to grow in volume as new vulnerabilities continue to be found by security researchers and threat actors. These kinds of attacks are attractive due to their centralization and large blast radius. A single vulnerable entry point in the supply chain can expose hundreds or thousands of customers and subsequent organizations to an attack.

09

It’s no secret that organizations are migrating to the cloud.

It’s cost-effective and reduces on-premises risks. However, the same enthusiasm hasn’t manifested when it comes to cloud security. According to our annual **The State of Cybersecurity: 2023 Trends** report, only 38% of respondents believe they are effectively securing their cloud resources. In addition, 42% of respondents stated that cloud security gaps were their primary area of worry, and in a positive trend, 46% of respondents would like to learn more about cloud security and evolving infrastructures.

t it looks like in the real world

are being taken in the right direction, but that doesn’t mean organizations should let down their d when it comes to cloud security. Between misconfigurations and the rise of cybercriminals eting the cloud specifically, we expect this gap to lead to breaches in the future.

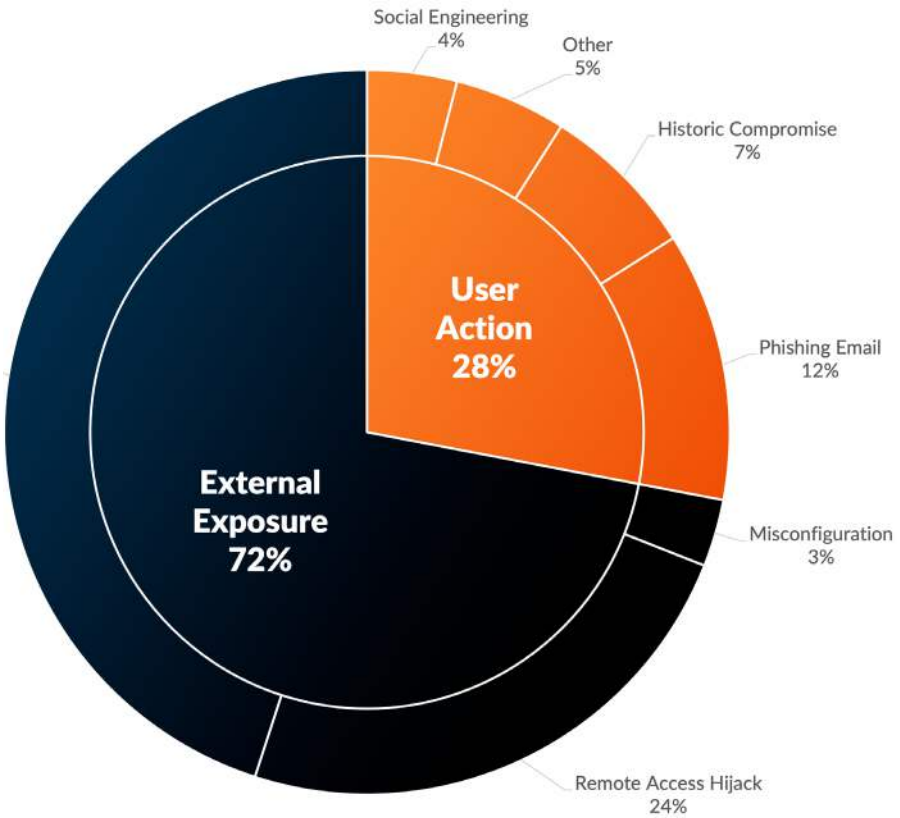
KEY THEMES

KEY THEMES

The predictions and real-world scenarios shared above aim to forecast what is coming next for security teams, while in this section we will look back at the past year to see what can be learned from the thousands of incidents we have responded to. Learning from the experiences of other teams and organizations is where you build resilience, focus tactics, and short-term priorities that can help you avoid becoming a victim of similar incidents.

Leveraging data from the Arctic Wolf Security Operations Cloud, and working in close collaboration with Arctic Wolf's Incident Response and Security Services Teams, Arctic Wolf Labs have compiled these key themes based on threat intelligence gathered from our data set.

These key themes tell a clear story of a shifting threat landscape. The headline-grabbing dangers of ransomware and BEC attacks remain a top concern, but just as important are how threat actors get their initial foothold in the environment with a simple user action or by leveraging a handful of critical vulnerabilities. While others



Root Point of Compromise – External Exposure Deep Dive

Arctic Wolf Labs has determined that a handful of solutions and vulnerabilities are responsible for a significant portion of incidents responded to by the Arctic Wolf Incident Response. Of the top five vulnerabilities leveraged by threat actors in 2022, four of them were published in 2021:

VMWare Horizon (Log4Shell – CVE-2021-44228)

Microsoft Exchange (ProxyShell – CVE-2021-34473)

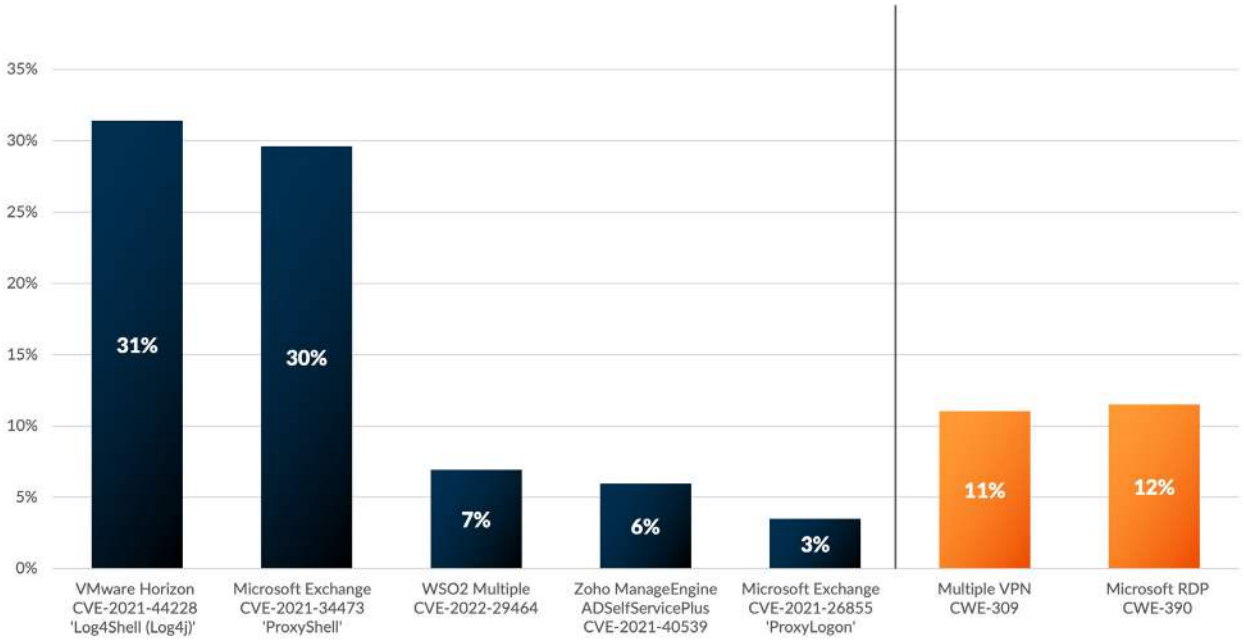
WSO2 Multiple (CVE-2022-29464)

Zoho Managed Engine AD Self Service Plus (CVE-2021-40539) and

Microsoft Exchange (ProxyLogon – CVE-2021-26855)

Older vulnerabilities can be enticing for threat actors because the vulnerabilities are well researched and public exploits are validated, taking the guess work out of exploitation. Furthermore, exploit modules are developed for penetration software, such as Metasploit, making exploitation easier.

With respect to external remote access tools, Microsoft RDP (CWE-390) and Multiple VPN (CWE-309) continued to be the root point of compromise for a significant number of incidents (23%) in 2022.



RANSOMWARE

RANSOM DEMANDS BY INDUSTRY

Based on ransomware incidents investigated by the Arctic Wolf Incident Response the median initial ransom demand across all industries was $500,000 USD.

Ransom demands vary across industries due to many factors, including the victim organization's size, revenue, data, and, in some cases, their insurance policy maximums. Some ransomware groups actively seek out cyber insurance policies in a victim's environment to better inform their ransom demands, typically asking up to the maximum the insurance policy will cover.

Ransomware-as-a-Service Dominates with LockBit Ahead of Other Variants

In 2022, ransomware threat actors demonstrated an increased adoption of the RaaS model.

In this model, RaaS operators offer technical resources (e.g., encryption software, leak site) and

LockBit

LockBit ransomware was first observed in mid-2019 as ABCD ransomware, due to the encrypted ".abcd" file extension the threat actors used before changing to ".lockbit."

The group is known for its self-propagating ransomware and short dwell times. While other ransomware groups may spend days or weeks manually conducting reconnaissance after gaining initial access to a network, LockBit has automated these tasks and has been observed dwelling in the network for as little as a matter of hours. This helps explain why they have 3.5 times more activity than the second-most-prevalent ransomware variant on our list — ALPHV (BlackCat).

ALPHV (BlackCat)

The ALPHV (BlackCat) ransomware variant was first identified in November 2021.

The name and imagery used in the ransomware variant's branding stem from Russian folklore around a similarly named street gang[3] dating back to the Soviet era. Attacks observed thus far have employed the "double extortion" method to both encrypt victims' systems and exfiltrate their data,

Strategic and Technical Insights into Ransomware Groups

In 2022, Arctic Wolf Labs conducted extensive research into TTPs leveraged by ransomware and extortion threat groups.

The research allowed us to provide customers and the security community with strategic and technical insights into their operations.

By applying these insights to an organization's environment, IT and security leaders could reduce risk, prevent or minimize disruption to business operations, and increase understanding of specific threats to help prevent future attacks.

In addition, these insights would help organizations prevent financial loss by making timely, informed decisions to prevent system downtime.

The Karakurt Web: Threat Intel and Blockchain Analysis Reveals Extension of Conti Business Model

In early 2022, the Arctic Wolf Incident Response partnered with Chainalysis to use digital forensics and blockchain analysis to reveal clear **connections between the extortion group Karakurt** and the ransomware groups Conti, Ryuk, and Diavol.

Conti Connections: Having worked on over a dozen Conti re-extortion cases, the Arctic Wolf Incident Response team recognized that Conti relied primarily on Fortinet SSL VPNs as the root point of compromise in re-extortion cases. This same technique was also found to be commonly used by Karakurt.

There are other overlaps seen between Conti-related re-extortion attacks and Karakurt intrusions, including the use of the same tools for data exfiltration, the creation of a file listing of exfiltrated data, and the use of the same hostname when remotely accessing victims' networks. Arctic Wolf Incident Response also identified connections between Karakurt attacks and the Ryuk ransomware variant.

To further support these connections, Chainalysis, in partnership with Arctic Wolf, identified evidence of Karakurt wallets sending significant sums of cryptocurrency to wallets owned by Conti, indicating a financial connection between the two groups.

Diavol Connections: The Arctic Wolf Incident Response discovered operational security errors made by Karakurt operatives which revealed a connection to Diavol ransomware, another group which emerged around the same time as Conti (July 2021) and has been associated with the use of Trickbot malware.

Our responders observed adversary actions across multiple cases which proved shared use of tools and


MARCH 2022
Lorenz ransomware exploits Mitel device, placing Chisel Tunnel in devices to establish reverse shell.
MARCH 2022
Researchers have identified the vulnerability and reported it to Mitel.
JUNE 2022
Observed by Arctic Wolf Labs that Lorenz exploits the Mitel device, placing a Chisel Tunnel on devices to establish a reverse shell. Primary detections have been created and implemented in
APRIL 2022
The vulnerability was assigned CVE-2022-29499.
MARCH 2022
Mitel MiVoice Connect product team identified this vulnerability as a zero-day exploit and patched it.

THE CONTINUED SCOURGE OF BUSINESS EMAIL COMPROMISE

THE CONTINUED SCOURGE OF BUSINESS EMAIL COMPROMISE

One of the most notable trends in the threat landscape was a significant uptick in the number of successful business email compromise (BEC) attacks observed in 2022 compared to 2021.

Business email compromise attacks continue to be endemic in the industry, and the large payouts threat actors can steal continues to motivate them to conduct this type of attack.

Business email compromise — also known as email account compromise (EAC) — is a type of email cybercrime scam in which an attacker impersonates a trusted contact then deceives victims into transferring funds or revealing confidential information.

Vendor Impersonation

Vendor payment is a pretense that is often used to trick victims with access to company finances.

In these BEC attacks, threat actors pose as legitimate vendors requesting fraudulent payments. Employees should be on guard to question and double-check unusual or unexpected financial requests.

Data Theft

These types of attacks often target HR departments, given their access to sensitive data.

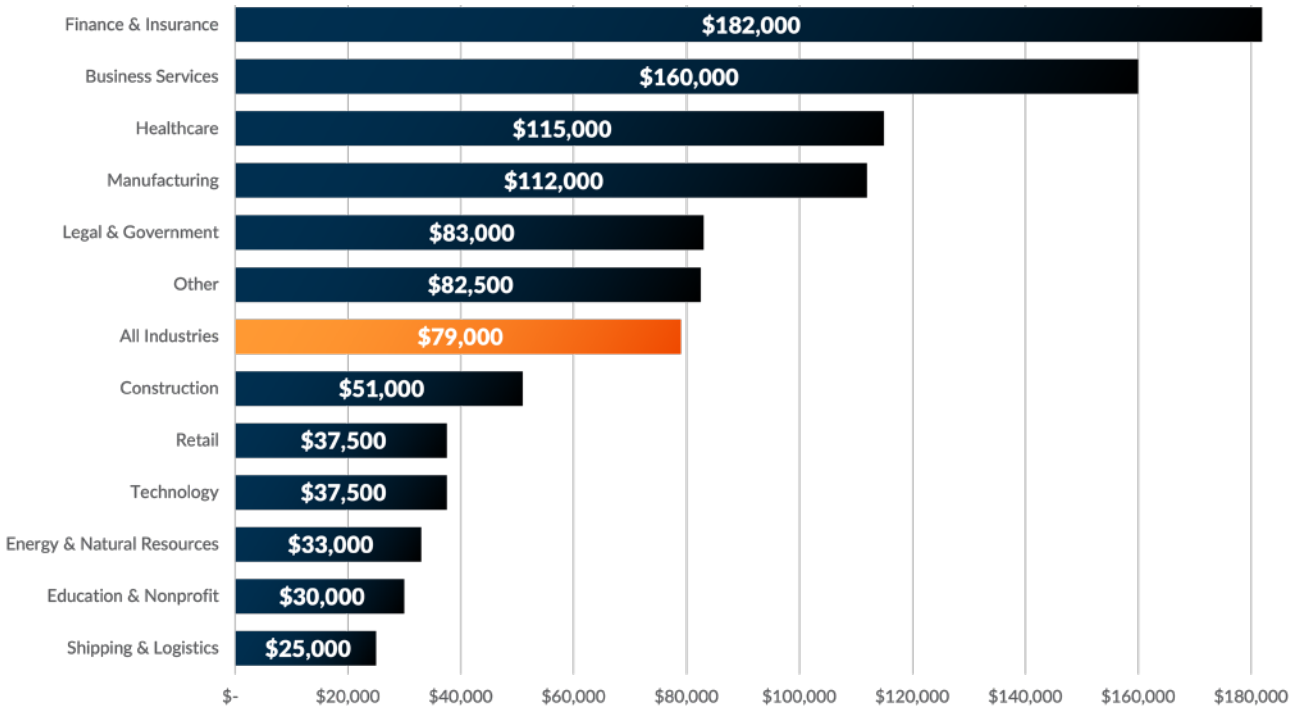
Threat actors attempt to obtain personal or sensitive information about individuals within the company, such as CEOs and executives. Gathered data can then be leveraged for future attacks. In some instances, threat actors may attempt to extort victims into paying to keep sensitive information from being revealed publicly.

Attorney Impersonation

Lower-level employees are commonly targeted through these types of BEC attacks, where attackers impersonate a lawyer or legal representative.

The goal of these types of attacks is often to elicit the transfer of funds to a bank account controlled by a threat actor.

While threat actors often launch BEC attacks against many industries at once, industries such as finance, insurance, and business services were particularly impacted in 2022.

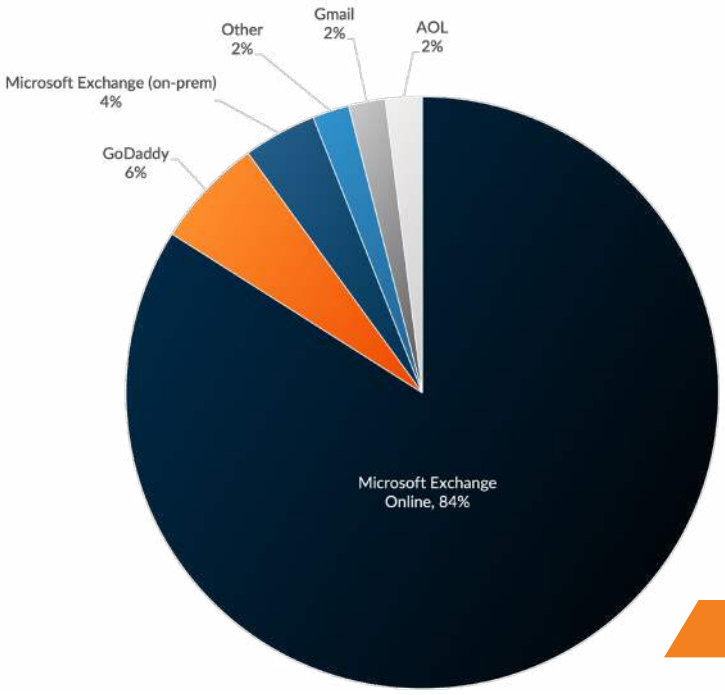


The ongoing exploitation of compromised credentials in BEC attacks highlights the importance that MFA and dark web monitoring play in securing organizations.

With MFA in place, exploitation of compromised credentials becomes more challenging.

Even if a threat actor has a known username and password pair, the account remains inaccessible without a second factor of authentication such as an app push notification, text message, or security token. As a next layer of defense, dark web monitoring can alert organizations if credentials have been exposed.

In addition to the need for MFA, the ongoing exploitation of compromised credentials in BEC attacks underscores the need for organizations to have robust security awareness training programs, focused on increasing user vigilance of fraudulent credential requests, in addition to 24x7 monitoring. This user vigilance training is critical due to the increasing number of phishing toolkits that prompt users to enter MFA tokens.



Interactive Incident Timeline:

Arctic Wolf Security Operations Cloud

FIVE NOTABLE EMERGING THREAT ACTOR TTPs

FIVE NOTABLE EMERGING THREAT ACTOR TTPs

Threat actors are constantly adapting their tactics, techniques, and procedures (TTPs) to evade defenses and exploit novel initial access vectors.

We reviewed threat intelligence from various sources to identify several key TTPs over the course of 2022. Data sources included threat intelligence data resulting from incident response activities and digital forensics, as well as from our Managed Detection and Response solution.

PowerShell remained a favorite of threat actors in 2022.

Numerous other ATT&CK TTPs depend on PowerShell, which provides several features that are attractive to threat actors:

1. PowerShell comes preinstalled on most Microsoft Windows systems targeted by threat actors, including across desktop and server devices.
2. PowerShell provides a means for obfuscation, serving as an evasion against detection by endpoint protection and monitoring solutions.
3.

03 T1190 - Exploit Public-Facing Application

In 2022, remote code execution vulnerabilities in major web applications have continued to serve as a potent initial access vector for threat actors.

This list includes a diverse variety of products, such as Microsoft Exchange, Fortinet firewalls, and Meraki VoIP devices.

Due to the wide variety of affected products, organizations find it challenging to prioritize patching of the most urgent affected applications and prevent these kinds of attacks. In many instances, major vulnerabilities that had been disclosed years ago continue to be exploited.

04 T1133 - External Remote Services, T1021 - Remote Services and T1021.001 - Remote Services: Remote Desktop Protocol

Threat actors have continued to show a tendency to rely on remote access solutions such as Microsoft Remote Desktop Services, AnyDesk, ConnectWise Control (formerly known as ScreenConnect), and many others.

The continued advantage of this approach for threat actors is that legitimate software is more likely to

THE LONG TAIL OF LOG4SHELL

THE LONG TAIL OF LOG4SHELL (LOG4J) BACKGROUND

Log4j is a Java-based logging library maintained by the Apache software foundation. Software developers use the Log4j framework to record user activity and review application behavior.

This library is one of the most used libraries for logging and is likely present in millions of java applications. The vulnerability is especially dangerous because Log4j is used as a backend dependency in many cloud-based services.

In early December 2021, Log4Shell (CVE-2021-44228 and CVE-2021-45046) was first identified as a zero-day remote code execution (RCE) vulnerability in Apache Log4j 2. An unauthenticated, remote threat actor can exploit this flaw by sending a specially crafted request to a server running a vulnerable version of Log4j.

Arctic Wolf's Response

After this vulnerability was discovered, Arctic Wolf Labs built the Log4Shell Deep Scan Tool to detect this

RECOMMENDATIONS FOR A STRONGER SECURITY POSTURE

RECOMMENDATIONS FOR A STRONGER SECURITY POSTURE

Though the cybercrime landscape is continuously evolving, that doesn't mean organizations are on their own when it comes to protection.

Cybersecurity continues to evolve as well, and there's a myriad of ways organizations can better their own security posture and put themselves in a strong position to fight off immediate or future threats.

A robust cybersecurity strategy is one that is not only unique to the organization's needs but focuses on proactive and reactive strategies that work before and after an incident occurs. This strategy should also be scalable and comprehensive, relying on more than just an abundance of software tools. Regardless of an organization's maturity level or security needs, the following recommendations would help address the troublesome trends seen over the last year and strengthen cybersecurity postures going into 2023.

One of the most important pillars of an organization's security posture is understanding the breadth of the attack surface.

02 Monitor Critical Log Sources for Security Threats

Arctic Wolf has consistently recognized that a lack of visibility allows security threats to go unnoticed and cause significant damage to organizations.

Log monitoring is critical to detect major threats. This includes logs from intrusion detection systems (IDS)/ network detection response (NDR) systems, firewalls, EDR solutions, IAM systems, and the cloud-hosted services used in your environment.

Expanding environmental visibility to these types of log sources increases the likelihood of detecting potential threats at an early stage, allowing for those threats to be stopped before they have a chance to incur significant damage.

Log monitoring also allows organizations to utilize the full potential of their cyber threat intelligence. Insight gained from the logs can illustrate which TTPs threat actors are using against their targets. That intelligence is critical for identifying Indicators of Compromise (IOCs) and mapping out the adversary's kill chain, ultimately helping analysts understand the motives and goals of threat actors which can assist in decision-making about how to best respond to an incident.

03

04 Employ a Zero Trust Security Strategy

As organizations continue to migrate to the cloud by the masses and implement remote or hybrid work, implementing Zero Trust strategies becomes an important consideration.

Zero Trust focuses on the user, not the perimeter, and limits all access unless it can be verified. This tactic — which includes strong identity and access management strategies — can reduce the attack surface and prevent an attacker's ability to move laterally through an organization's network.

There are multiple ways to implement Zero Trust strategies, including implementing multi-factor authentication and other identity management tools like Zscaler or Okta.

Utilizing a Zero Trust strategy, and relevant solutions will reduce the risk of account takeovers and will provide additional security for organizations.

05 Understand the Shared Responsibility Model **and Eliminate Misconfiguration**

It's important to recognize where a cloud provider's security responsibilities end, and an organization's security responsibilities begin.

CONCLUSION

References:

1. https://securityboulevard.com/2022/03/by-the-numbers-the-cost-of-insider-data-breach-vs-the-cost-of-protection/
2. https://hsdl.org/c/2021-internet-crime-report/
3. https://researchgate.net/publication/332870814_Legends_of_the_Black_Cat_Gang_as_a_Reflection_on_the_Phenomenon_of_Criminal_Myths_in_Russian_Public_Consciousness
4. https://justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
5. https://sans.org/about/awards/difference-makers/