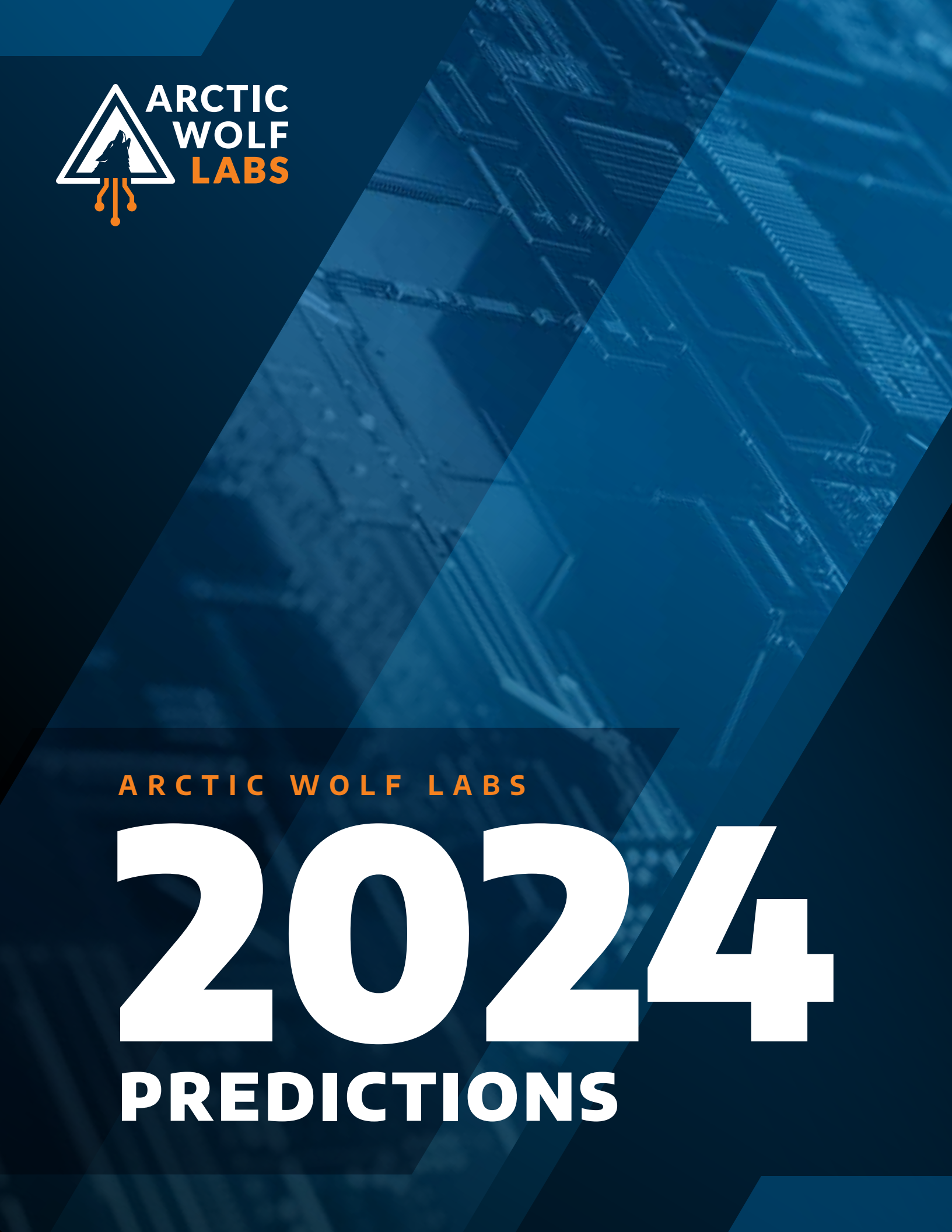

2024 PREDICTIONS

INTRODUCTION

Evolution Is the Underlying Theme Moving Into 2024

The term 'evolution' implies the gradual growth of something from simple to complex, and it perfectly sums up our Arctic Wolf Labs' 2024 Predictions. Our predictions are based on the current cybersecurity trends and insights gathered from our data, and so our predictions really trace the development of several trends based on their earlier, simpler iterations and anticipate which ones are poised to take significant steps forward in the year ahead. This report also represents the next stage in Arctic Wolf annual reporting by presenting predictions ahead of next year's annual Arctic Wolf Labs Threat Report.

Based on the trends we have monitored, **we have five core predictions for 2024:**

01 **Election-focused cyber activity will continue to grow.**

02 **Ransomware-as-a-service (RaaS) will likely see continued specialization.**

03 **Organizations will have to continue to harden themselves against state-sponsored actors to defend their intellectual property.**

04 **Microsoft Active Directory security will remain a focus.**

05 **AI-generated code will introduce new security vulnerabilities.**

These predictions are the work of several of our brightest minds who aim to prepare security teams for the challenges of the year ahead to mitigate the risks posed by threat actor activity.

ARCTIC WOLF LABS

About Arctic Wolf® Labs

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence, including machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings.

With their deep domain knowledge, Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community-at-large.

FIVE CORE 2024 PREDICTIONS

01 Increased Cyber Activity Around 2024 Elections Worldwide

As many countries around the world hold elections, including presidential elections in the United States, Russia, and potentially Ukraine (if martial law is lifted), as well as a general election in the United Kingdom, and a European parliamentary election in Germany, state-sponsored and espionage threat groups will use the elections for phishing lures and social engineering.

Ransomware-as-a-service groups may also target election infrastructure in an effort to disrupt election preparations for financial gain. Election systems that house voter registration and other voting information will likely be a target of interest for all groups attempting to interfere in the 2024 elections due to the sensitive information they contain.

Foreign governments often attempt to influence the political landscape and policies of other countries to benefit their political and economic interests. These activities can directly or indirectly affect an election. We will likely see disinformation campaigns and influence operations attempting to influence political sentiment or public discourse in countries holding the elections. We will also likely see threat actors leverage large language models (LLM) and AI-generated deepfakes to augment disinformation campaigns and fabricate content that appears legitimate. As AI-generated content continues to improve, fabricated content will be nearly indiscernible from valid information, including video and audio. Disinformation campaigns may include pushing misleading or unsubstantiated allegations against candidates, political parties, or voters to media organizations or social media in an attempt to legitimize disinformation and amplify its impact.

A recent example of this occurred during Slovakia's 2023 election, where an AI-generated audio recording imitating Slovakia's Progressive party leader Michal Šimečka's voice circulated social media two days before the election. In the two-minute recording, the voice of Šimečka was heard discussing how to rig the election by buying votes. Shortly after it began circulating the audio was denounced by Šimečka and **deemed a hoax by AFP**, the fact-checking department of the multilingual and multicultural news agency Agence France-Presse. We expect this theme to continue into the 2024 election cycle with varying media types, including print, video, and audio.

Although election infrastructure is typically heavily safeguarded to prevent disruption and maintain election integrity, nation states such as Iran and Russia may seek to create or amplify false claims of cybersecurity issues to cause public discourse and erode confidence in the election processes and results. Both countries have well-documented histories of interfering in the elections of nations they view as adversaries.

01 Increased Cyber Activity Around 2024 Elections Worldwide

In July 2018, **the U.S. Department of Justice (DOJ) indicted** 12 Russian GRU officers for their roles in interfering with the 2016 U.S. elections. The officers obtained access to the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC), and the presidential campaign of Hillary Clinton, and stole documents, subsequently staging releases of the documents to interfere with the 2016 U.S. presidential election.

In November 2021, **the U.S. Department of the Treasury sanctioned** the Iranian cyber company Emennet Pasargad for attempting to influence the 2020 U.S. presidential election by spreading disinformation on social media and sending threatening emails. Notably, in 2019, Emennet Pasargad was sanctioned under a different name (Net Peygard Samavat Company) for supporting Iran's Islamic Revolutionary Guard Corps (IRGC).

RECOMMENDATIONS

- Conduct user awareness campaigns to inform users of potential election-themed phishing emails. Be cautious of emails from unknown email addresses that make suspicious or blatantly false claims about the election process.
- Do not click links or open attachments from unsolicited emails. During previous election cycles, threat actors sent invoice-themed phishing emails that contained links to websites intended to steal login credentials. The emails shared similar attachments and used compromised email addresses to disseminate them.
- Ensure employees know the correct process to report suspicious emails to the security team.
- Verify information about election-related incidents and voter information compromise through multiple, reliable sources. The same due diligence should be conducted before sharing or interacting with social media posts or accounts.

02 Ransomware-as-a-Service and Data Exfiltration Ecosystem Will Continue To Evolve

The ransomware-as-a-service business model has created an entire ecosystem connected to monetizing intrusions and will continue to be an attractive offering to cybercrime actors.

Many threat actors within the ecosystem rely on specialized services and offerings to conduct intrusions, and we expect those offerings to expand and evolve in 2024 to bypass security controls.

As we have observed historically with ***double extortion*** in ransomware campaigns, threat actors adopt tactics, techniques, and procedures (TTPs) from other threat actors. Based on the success of CL0P, the ransomware group behind the exploit of a zero-day SQL injection vulnerability within MOVEit Transfer, a widely used Managed File Transfer (MFT) application, we will likely see additional threat actors attempt to exploit Managed File Transfer systems and file servers. MFTs are commonly used to manage and automate the transfer of documents between organizations and customers. Due to their nature, it is common for MFT servers to sit on the network perimeter with file transfer ports exposed, making them a prime target for threat actors.

Furthermore, these solutions have access to potentially sensitive data, making a data exfiltration campaign simpler. By compromising an MFT solution, threat actors have access to company data without needing to conduct lateral movement or other activity to obtain it.

Additionally, we will likely see more threat actors, especially ransomware groups, leverage new techniques, such as ***torrents***, to publish victim data because it does not require a complex website to host and disseminate the data, making it easier to set up. Decentralized torrents can also be a much more efficient way to distribute the exfiltrated data as users are not hindered by the slow and sometimes inconsistent Tor connection. Notably, even if the original seeder is taken offline a new device can be used to seed the data making it more difficult for law enforcement to remove it.

RECOMMENDATIONS

- Create a baseline of expected network flow and user behavior to detect potential data exfiltration activity. In most cases threat actors compile the stolen data and attempt to exfiltrate it out of the network as quickly as possible, which would deviate from normal user behavior.
- Block network connections to cloud storage and file hosting services not used by your organization. Additionally, ensure end-users leverage company-approved services to share and store files.
- Most MFT solutions contain a reporting component. Ensure alerts and audit functions are properly configured in your MFT solution and are being actioned when triggered.
- Consider leveraging a Cloud Access Security Broker (CASB) to enforce your organization's cloud security policy, govern cloud usage, and prevent the loss of sensitive data across all cloud services within your environment.

03 Industrial Espionage and Intellectual Property Theft Campaigns Will Be Aggressively Pursued via China's Cyber Operations

In 2023, the U.S. Office of the Director of National Intelligence said that "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."

This underscores the importance of keeping current with new developments in the tactics, techniques, and procedures employed by China-nexus threat actors.

In recent years, China's cyber activities have focused on technological advancement through industrial espionage. Additionally, through its foreign policy efforts, China has worked to disrupt sources of potential opposition to the Chinese Communist Party (CCP) by controlling the flow of information domestically, while also conducting influence operations abroad. These operations comprise an interconnected network of organizations from private industry, academia, and the political sphere. The breadth of involved stakeholders in this apparatus provides China with plausible deniability when other parties attempt to hold them accountable. Such activities are a mainstay of China's modus operandi and have, in fact, been gradually refined since the pre-digital 1920s.

In the cyber domain, **the U.S. Department of Justice has alleged** that China is leveraging intellectual property theft to support the "Made in China 2025" economic initiative. In 2018, **the U.S. DOJ unsealed indictments** against members of APT10, a state-sponsored Chinese espionage group, for targeting 45 U.S. companies in a campaign focused on industrial espionage. APT10, which has shown an interest in trade secrets from manufacturing and a variety of other industries, has been documented as using so-called living off the land (LOTL) attacks using system binaries to evade detection.

In 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published an advisory stating that living off the land attacks were one of the primary tactics, techniques, and procedures relied upon by People's Republic of China (PRC) state-sponsored cyber activity. By employing such techniques, threat actors can evade detection more readily from endpoint monitoring software. These TTPs are by no means limited to use by China and represent an attractive threat surface for financially motivated threat actors as well.

03 Industrial Espionage and Intellectual Property Theft Campaigns Will Be Aggressively Pursued via China's Cyber Operations

To remain undetected for as long as possible, China-nexus threat actors are **known to target hypervisors and perimeter devices** such as firewalls. These types of devices present threat actors with an opportunity for extended dwell time on targeted networks owing to a lack of endpoint visibility as well as increased difficulty in securing forensic images for further analysis. Zero-day exploits targeting these types of devices provide an avenue for initial access and long-term persistence that do not require human interaction, further reducing the likelihood of detection.

For its part, Chinese threat actors show no signs of reducing their activities and have only become more active in the last few years. We expect this trend to continue as China aggressively pursues its publicly stated self-sufficiency objectives.

RECOMMENDATIONS

- The focus for defenders should be on identifying unusual patterns in the invocation of living off the land tools, as well as remediating vulnerabilities **known to be actively exploited** by China-nexus threat actors.
- Review CISA's Joint Cybersecurity Advisory on **People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection**, implementing outlined recommendations where possible.
- Implement external logging and a monitoring security solution to stay on top of any active threats detected.

Due to the recency of the name change of Azure Active Directory to Microsoft Entra ID in regards to the publish date of this report, we have chosen to continue to use Active Directory in this section for reader clarity.

04 Active Directory Security Configuration Will Continue To Represent a Significant Threat

Securing a Microsoft Active Directory environment is no small feat.

Unauthorized access to even unprivileged user accounts allows threat actors to pivot through Active Directory environments, allowing for privilege escalation and lateral movement. Active Directory is not secure by default, requiring system administrators to spend inordinate amounts of time on configuration changes, which carries its own operational challenges.

Considering that a significant proportion of compromises involve stolen credentials, Active Directory will continue to be a relevant attack surface for defenders to focus on for hardening. Stolen credentials are frequently sold on the dark web, making it easy for threat actors to purchase access through an ***initial access broker*** to organizations of interest. Once legitimate credentials are abused by threat actors, it becomes critical to quickly identify subsequent unusual behavior associated with those accounts. There are too many privilege escalation and credential access methods for Active Directory to comprehensively list in this report; popular methods in this category include Kerberoasting, Pass-the-Hash, DCSync, and numerous others. Proactive efforts should be made to harden Active Directory configurations so that attacks are stopped as early as possible.

When the attack surface extends across both on-premises and cloud-based environments in a hybrid deployment, the amount of complexity is increased further, which in turn increases the opportunities for exploitation. Managing on-premises and cloud instances of Active Directory increases a network's complexity and can double an organization's attack surface.

In addition to the management of additional Active Directory instances, organizations also must add additional security controls to user data and implement controls to manage risk in two environments, both on-premises and in the cloud, adding to the environment's complexity. According to **IBM's 2023 Cost of a Data Breach Report**, organizations with complex environments reported an average breach cost that was 31.6% higher ($1.44M USD) than those with less complex environments. Complex IT networks contain additional avenues and entry points threat actors can abuse and exploit. Additionally, complexity can introduce inconsistent security measures that are implemented ad hoc or incorrectly.

RECOMMENDATIONS

- Proactively harden security configuration of Active Directory and Entra ID (formerly known as Azure AD) deployments.
- Employ real-time logging and monitoring solutions to ensure that crucial security alerts are caught by humans before threat actors can take hold in corporate environments.
- Consider using off-the-shelf auditing tools such as PingCastle and Bloodhound to improve Active Directory security hygiene before a threat actor exploits the same information for their gain.

05 AI-Generated Code Will Introduce Security Vulnerabilities Into the Development Process

As organizations continue to adopt and rapidly deploy AI into their software development processes, developer productivity will increase, but so will security risks. We will likely see an increase in security vulnerabilities linked to AI-generated code.

AI-generated code can inadvertently introduce security vulnerabilities into the development process, especially if the AI model has not been trained on secure coding practices and the code is not thoroughly reviewed and tested. AI-powered coding tools are trained using existing source code typically available publicly, such as in GitHub repositories. Public repositories are focused on providing different assets, such as tooling, scripts, and documentation which can help the open-source community. Security, however, is not the primary focus. The systems will only produce source code as secure as the code their models are trained on.

Additionally, the reliability of training datasets will need to be taken into consideration for code generation models, given that even small amounts of adversarial inputs may skew model outputs maliciously in a manner that is difficult to detect. Although multiple risks associated with AI are present, such as malicious use by threat actors and data poisoning, we assess the most immediate threat to organizations will be the introduction of vulnerable AI-generated code into production environments.

As AI-generated code continues to be adopted and deployed, DevSecOps will continue to play an increasingly crucial role in secure software development. Furthermore, according to IBM's 2023 Cost of a Data Breach Report, organizations that have adopted a high-level of DevSecOps had a significantly lower than average cost when subjected to a data breach.

RECOMMENDATIONS

- Ensure AI-generated code is subject to the same code review process as developer-generated code. The code should be thoroughly tested and audited before it is deployed into a production environment or shipped to customers.
- Create an acceptable use policy to govern what developers and users are allowed to do when using AI tools and services within your organization. Careful consideration should be given to how AI-generated code is used to minimize risk to the organization.
- Ensure the AI and machine learning (ML) models used to generate business critical code are trained in alignment with secure coding practices.

CONCLUSION

Evolution Means We Can Anticipate Connections and Proactively Plan Responses

As cybercrime continues to evolve, the web of connections between state-sponsored actors, ransomware-as-a-service operators, and organized cybercriminals is becoming increasingly complex. The cycle between uncovering new knowledge, launching successful TTPs, and broader threat actor adoption are likely to shorten as cybercriminals become savvier.

As CL0P proved that Managed File Transfer (MFT) servers are an attractive attack surface considering that MFT servers sit on the network perimeter with file transfer ports exposed, it may accelerate industrial espionage and IP-theft efforts by threat actors of varying levels of sophistication.

As China's looming spectre occupies the mind-space of national authorities and cybersecurity agencies, especially with the U.S. election (and several other high-profile international elections) occurring in 2024, this may provide some additional breathing room and green space for organized cybercriminals and ransomware-as-a-service operators to take bolder actions while targeting the most difficult to defend attack surfaces, such as Active Directory.

Then, throw into the mix the potential to introduce new vulnerabilities via AI-powered coding tools, there are certainly more than enough distractions and opportunities at hand to keep law enforcement and security teams hard at work to fend off attackers.

BUT...

By tracing the development of these trends, we can also get faster at responding to these threats. Defenders are also growing their repository of counter-TTPs, and looking at the year ahead, we've seen challenges like these before. Especially, as we anticipate the lurking challenges on the horizon for 2024, we can take action now to prepare our defenses to increase the cost to attackers and to proactively mitigate these threats.

Even though new techniques are always being developed and refined by threat actors, defenders have plenty of opportunities to detect and mitigate the threat of such activities.

First, by thoroughly and proactively reviewing security configurations and software inventory, defenders can better understand risks associated with assets under protection. With this insight in hand, defenders can prioritize risks by severity, focusing on proactively hardening the security configuration of specific areas.

Secondly, by monitoring environments in real-time, defenders can increase the likelihood that threat actors will be thwarted early in the kill chain. Malicious activities leave traces across different types of logging telemetry, and XDR monitoring provides a holistic view of digital environments. The visibility afforded by these types of services provides valuable insight into the movement of threat actors through networks, making it harder for them to remain undetected.

GLOSSARY

DOUBLE EXTORTION

Double extortion in ransomware campaigns is the practice of exfiltrating data and then encrypting an environment via ransomware and then using these two points of leverage to extort payment from the organization. These two points of leverage are demanding payment to:

1. not sell, share, or distribute the exfiltrated data and
2. to decrypt the environment to give access back to the organization.

TORRENTS

Torrents are files that are distributed (uploaded and downloaded) via the BitTorrent protocol in a practice called "torrenting." Instead of uploading or downloading files to/from a central server, torrenting is a decentralized activity. When an endpoint "seeds" or hosts a torrent file, it functions as server/node from which content can be downloaded. Each subsequent endpoint that downloads the data can become an additional host to enable further distribution, with hosts referred to as seeders. This network of seeders enables downloaders to acquire this data from multiple nodes simultaneously, creating a distributed network of file hosts that is resilient to take down activities.

INITIAL ACCESS BROKERS

Initial access brokers are threat actors who specialize in infiltrating systems and networks and then selling that access to other cyber criminals. They are an integral member of the cyber crime supply chain, enabling other threat actors to specialize in their own domain expertise, e.g., developing ransomware-as-a-service.

HOW ARCTIC WOLF CAN HELP

Cybersecurity is a team sport, and we hope the insights and recommendations in this report can help you practically reduce risk and increase resilience for your organization.

But if you feel overwhelmed by the sheer volume of priorities your security team already had before this report, you are not alone.

No organization can protect itself in isolation. We, as a community, rely on each other for sharing, learning, and providing expertise. It's impossible to go it alone in today's threat landscape. We believe we are all stronger together. We believe in having each other's backs — that everyone is safer when running as a pack.

Our customers rely on us every day to secure their organization against threats. We help level the playing field against attackers — ensuring that every organization of every size has the technology, tools, and processes needed to defend itself. If you aren't getting the outcomes you're looking for from the solutions you have today, or if you just need some support in putting your existing investments to work, we would love to help.

This is why we are proud to bring and demonstrate the wolf pack mentality, working with our customers and peers in the cybersecurity community, doing what it takes to secure organizations and ensure they survive the ever-increasing incident count.

For more information about Arctic Wolf, visit arcticwolf.com.

About Arctic Wolf®

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit arcticwolf.com.

REQUEST A DEMO

ARCTIC WOLF