



THREAT INSIGHTS 2024

TRENDS, VULNERABILITIES,
AND IMPACTS

VOLUME II

TABLE OF CONTENTS

Executive Summary	3
Emerging Threats	5
Mustang Panda	6
Profile	6
Attack Methods	7
Technical Analysis	8
Impact Assessment	8
Mitigation Strategies	9
Outlook	9
TA542	10
Profile	10
Attack Methods	11
Technical Analysis	12
Impact Assessment	12
Mitigation Strategies	13
Outlook	13
Scattered Spider	14
Profile	14
Attack Methods	15
Technical Analysis	16
Impact Assessment	16
Mitigation Strategies	17
Outlook	17
Vulnerabilities	18
CVE-2024-20353	18
Mitigation Strategies	18
CVE-2021-44529	19
Mitigation Strategies	19
CVE-2024-26248	20
Mitigation Strategies	20

EXECUTIVE SUMMARY

Adlumin's Cyber Threat Insights Report (Vol. II) highlights significant trends, cyberattacks, and vulnerabilities faced by U.S. and global sectors, as observed by Adlumin's Threat Research Team.

The report analyzes emerging threats, notable vulnerabilities for March, April and May 2024, and mitigation strategies that help organizations protect their assets. This volume covers three key threats that present unique challenges to cybersecurity professionals: Mustang Panda, TA542, and Scattered Spider.

EMERGING THREATS

Main Findings :

Mustang Panda

- Mustang Panda is a Chinese cyber espionage group that uses sophisticated phishing and custom malware to target governments (including state departments) and Non-Governmental Organization (NGOs).
- The group is focused on long-term intelligence gathering and their primary targets include entities in Southeast Asia, Europe, and North America.

TA5442

- TA542 is a cybercriminal group responsible for distributing the Emotet malware, primarily targeting the banking and financial services sectors.
- They deploy malware using sophisticated phishing techniques to steal sensitive information and deliver other malicious payloads, causing significant financial damage globally.

Scattered Spider

- Scattered Spider is a sophisticated cyber threat group known for very successful phishing and social engineering campaigns that target the healthcare, finance, and technology sectors.
- These attacks result in the theft of sensitive information and disruption of operations.
- Last year, Scattered Spider escalated to using ransomware, exemplified by its large-scale attack on MGM Resorts, which showcased its advanced capabilities and persistent threat.

VULNERABILITIES

The following are notable vulnerabilities highlighted in our report for Q2 of 2024.

CVE-2024-20353

- CVE-2024-20353 is a critical vulnerability affecting Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. It allows remote, unauthenticated attackers to craft HTTP requests to create Denial of Service (DoS) conditions.

CVE-2021-44529

- CVE-2021-44529 is a code injection vulnerability in Ivanti's Endpoint Manager Cloud Services Appliance (EPM CSA). It allows unauthenticated remote attackers to execute arbitrary code with limited permissions.

CVE-2024-26248

- CVE-2024-26248 is an elevation of privilege vulnerability in the Windows Kerberos PAC (Privilege Attribute Certificate) Validation Protocol, enabling attackers to spoof PAC signatures and bypass security checks to gain elevated privileges.



EMERGING THREATS

During Q2 2024, the Adlumin Threat Research Team identified areas of increased risk posed by three notable threat actors based on their tactics, techniques, and procedures (TTPs), ongoing operations, and potential impact on organizations of all sizes and U.S. critical infrastructure. By providing information about these adversaries, we aim to help your organization prepare for potential attacks and stay ahead of them.

**Mustang
Panda**

TA542

**Scattered
Spider**

Mustang Panda

Mustang Panda is a notorious Chinese cyber espionage group known for targeting governments, including in Taiwan, and non-governmental organizations (NGOs) worldwide. They employ sophisticated phishing techniques and custom malware to gain unauthorized access to sensitive information. Their operations are characterized by long term campaigns aimed at intelligence gathering and cyber surveillance.

Profile:

Mustang Panda, also known as “RedDelta,” emerged as a significant cyber espionage threat actor in the mid-2010s. Initially, their activities were focused on Southeast Asia, where they targeted government entities, think tanks, and NGOs. The group is believed to be based in China and has demonstrated a high level of sophistication in their attacks. Using spear-phishing emails with malicious attachments and links, Mustang Panda infiltrates networks to steal sensitive information.¹ Their campaigns have often been linked to the broader strategic interests of the Chinese state, particularly in terms of regional political influence and intelligence gathering.

Over the years, Mustang Panda has expanded its operations beyond Asia, targeting entities in Europe and North America. It has continuously evolved its tactics, techniques, and procedures (TTPs), employing custom malware like PlugX and Poison Ivy.

Their ability to adapt and persistent efforts in espionage have made them a significant concern for cybersecurity experts and national security agencies worldwide. Recent reports indicate that Mustang Panda has also been involved in exploiting vulnerabilities in widely used software to enhance the effectiveness of its attacks. This ongoing threat underscores the importance of robust cybersecurity



ATTACK METHODS

Mustang Panda's PlugX malware is a remote access trojan (RAT) that allows attackers to control infected systems remotely.

PlugX is highly versatile, capable of performing a range of functions from keylogging to data exfiltration.² The group has also been known to use other custom malware, such as Poison Ivy and a unique loader called PubLoad, which serves to obscure the initial infection vector and maintain persistence on compromised systems.

These tools enable Mustang Panda to carry out long term surveillance and data theft operations, often aligned with their sponsors' strategic interests.

Mustang Panda has also demonstrated a growing capability to exploit vulnerabilities in widely used software. For instance, they have taken advantage of zero-day vulnerabilities in popular applications, various VPN services and Microsoft, to gain initial access to target networks. This not only highlights their technical proficiency but also their commitment to staying ahead of security defenses. Once inside a network, they employ lateral movement techniques to expand access, often using legitimate administrative tools to avoid detection. This makes it challenging for defenders to identify and remediate the group's presence.

Mustang Panda's operational security is also noteworthy. They frequently update their malware and command-and-control infrastructure to evade detection. The group also utilizes encryption and other obfuscation techniques to protect their communications and payloads. This level of sophistication indicates a well-resourced, highly skilled group, capable of conducting prolonged and stealthy campaigns. Their persistent efforts to evolve and refine their attack methods underscore the importance of continuous vigilance and advanced defensive measures in cybersecurity.



NOTORIOUS ATTACKS IN 2024

Mustang Panda recently conducted a significant attack in April 2024. This attack, using sophisticated malware deployment and their signature Trojan (PlugX), targeted European and Russian organizations.

The TTPs used included a multi-stage infection process with a specially crafted document made to resemble an official European Union Report. A benign executable was responsible for loading a malicious DLL, which activated the PlugX payload.



TECHNICAL ANALYSIS

In recent months, Mustang Panda has continued its sophisticated cyber espionage operations, primarily using spear-phishing emails with decoy documents to deliver malicious payloads.

These payloads often include a benign executable that, through DLL side-loading, loads the PlugX malware, enabling persistent access to compromised systems. The group's use of fake documents, such as European Union reports or Ukrainian statements, highlights their focus on high-value targets and their ability to deceive victims.

Mustang Panda has demonstrated adaptability by employing new technologies and techniques. They have used a variant of PlugX called DOPLUGS to target entities like Taiwanese government organizations.³ This variant acts as a downloader for additional malware and includes backdoor commands for extensive system control. The group's use of LNK files and Meterpreter reverse-HTTP payloads further exemplifies their ability to innovate and evade detection.

Their attacks also involve complex obfuscation techniques, such as using JavaScript and BAT files executed through legitimate processes to establish persistence.⁴

The constant refinement of their tools, including adopting new programming languages like Nim, underscores their threat to cybersecurity defenses. Organizations are advised to enhance their email security, scrutinize attachments, and use behavioral detection systems to counter these sophisticated threats.



IMPACT ASSESSMENT

Mustang Panda's cyber espionage activities have significant national security and international relations implications. By targeting government entities, diplomatic missions, and NGOs, particularly in Asia and Europe, they threaten the confidentiality and integrity of sensitive information.⁵

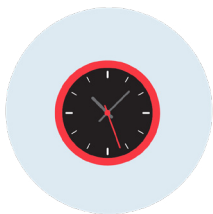
Their sophisticated techniques, including the use of advanced malware like PlugX and DOPLUGS, and their ability to adapt and innovate in response to cybersecurity measures, pose a persistent threat to targeted organizations. The economic and political impact of their operations can be profound, potentially leading to compromised state secrets, disrupted diplomatic efforts, and economic espionage that undermines competitive advantages.⁶



MITIGATION STRATEGIES

To mitigate the threat posed by Mustang Panda, organizations should implement a comprehensive cybersecurity strategy.⁷ Here are key measures to consider:

- **Email Security Solutions:** Use advanced email gateways with robust filtering to detect and block spear-phishing attempts. Educate employees on recognizing phishing attempts.
- **Endpoint Detection and Response (EDR):** Deploy EDR tools to identify and neutralize malware like PlugX and DOPLUGS.
- **Regular Updates and Patching:** Ensure all software and systems are regularly updated to fix known vulnerabilities.
- **Threat Intelligence Services:** Stay informed about the latest tactics, techniques, and procedures (TTPs) of Mustang Panda to proactively adjust defensive measures.
- **Network Segmentation and Least Privilege:** Enforce network segmentation and the principle of least privilege to limit lateral movement within a network if a breach occurs.
- **Security Audits and Penetration Testing:** Conduct regular security audits and penetration testing to identify and address potential weaknesses in defenses.



OUTLOOK

Looking ahead, Mustang Panda is expected to continue to evolve its tactics and expand its target range, driven by geopolitical and economic motivations. The group will likely refine its use of advanced malware like PlugX and DOPLUGS, incorporating new programming languages and obfuscation techniques to evade detection.⁸

Their persistent focus on high-value targets suggests that they will remain a significant threat in the cybersecurity landscape. As international tensions and cyber capabilities grow, Mustang Panda's operations will likely become more sophisticated, and will require enhanced defensive measures and greater international collaboration to effectively counter their activities.

TA542

TA542 is a notable cybercriminal group known for distributing the Emotet malware, primarily targeting sectors such as banking and financial services. The group employs sophisticated phishing techniques to deploy malware that can steal sensitive information and facilitate the delivery of other malicious payloads. Active since around 2014, TA542 has adapted its tactics over time, making it a persistent threat in the cybersecurity landscape.

Profile:

TA542, also known as “Mummy Spider” or “Gold Crestwood,” emerged in the cyber threat landscape around 10 years ago.⁹ The group quickly gained notoriety for its development and distribution of the Emotet malware, initially designed as a banking Trojan. Over time, Emotet evolved into a modular platform capable of delivering various payloads, making it a versatile tool for cybercriminal activities. TA542 primarily relied on extensive phishing campaigns, deploying convincing emails to trick victims into downloading malicious attachments or clicking on harmful links. These emails often mimicked legitimate communications from trusted entities, increasing their success rate and expanding the group's reach.¹⁰

TA542 has demonstrated a remarkable ability to adapt and innovate in its operational history. The group has continuously updated Emotet to evade detection by security systems and has expanded its capabilities to include data theft, network infiltration, and the deployment of other malware, such as ransomware. Despite numerous takedown efforts by international law enforcement, TA542 has resurfaced, showing resilience and persistence.¹¹ Their activities have caused significant financial damage globally, CISA reports that Emotet-related incidents could cost state, local, tribal, and territorial governments up to \$1 million per incident to remediate.¹² This highlights the ongoing threat posed by this group and the need for vigilant cybersecurity measures.



ATTACK METHODS

TA542 employs a range of sophisticated attack methods, primarily leveraging phishing campaigns to initiate their attacks. The group meticulously crafts emails that often appear to come from trusted sources, such as financial institutions, government agencies, or well-known companies. These emails contain malicious attachments or links designed to trick recipients into downloading and executing the Emotet malware. TA542 uses social engineering techniques to enhance the credibility of these emails, increasing the likelihood of successful infiltration. Once the victim opens the attachment or clicks on the link, Emotet is deployed, initiating the infection process.¹²

Once Emotet is installed on a victim's system, it acts as a downloader for other types of malware, expanding its reach and impact. The malware can steal sensitive information, such as credentials and financial data, which can be used for further attacks or sold on the dark web.

Emotet can also spread laterally within a network, infecting additional devices, and increasing the overall damage. TA542 has also collaborated with other cybercriminal groups, providing them access to infected systems where they deploy additional malware, such as ransomware or banking Trojans. This partnership significantly amplifies the threat posed by TA542, as it combines the capabilities of multiple threat actors.¹³

TA542 continuously updates its tactics to evade detection and maintain its effectiveness. The group frequently changes the structure and content of their phishing emails to bypass email security filters. They also use polymorphic techniques, regularly altering the code of Emotet to avoid signature-based detection by antivirus software.

In addition, TA542 leverages command and control (C2) servers to manage infected systems and deploy updates or new payloads. These servers are often located in different regions and frequently rotated to evade law enforcement.¹⁴ This level of sophistication and adaptability makes TA542 a persistent and formidable threat in the cybersecurity landscape.



NOTORIOUS ATTACKS IN 2024

A notable string of cyberattacks by TA542 occurred recently in April 2024, when organizations across Europe and the United States were targeted by a sophisticated campaign. Employees across these organizations received phishing emails with malicious attachments, which would download and execute the Emotet payload once the attachment had been opened. Once activated, the malware would reach out to the command and control (C2, C&C, etc.) server, establishing a link between the affected machines and the attackers. This allowed the attackers to download sensitive information, ransomware, etc.

In early June 2024, Europol issued a statement seeking information on one of TA542's leaders going by the nicknames "Odd," "Aron," "C700," and "Veron."



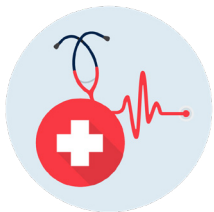
TECHNICAL ANALYSIS

Since early 2024, TA542 has been particularly active, with a notable resurgence in the deployment of the Emotet – exhibiting new tactics and techniques designed to increase its effectiveness and evasion capabilities.¹⁵

One significant development observed was the use of updated phishing campaigns that leveraged hijacked email threads to deliver malicious payloads. This approach made their emails appear more legitimate, thereby increasing the likelihood of successful infections. Additionally, TA542 has been integrating new modules into Emotet, such as those designed to steal credit card information stored in Google Chrome, further expanding their data theft capabilities.

Recent analyses indicate that TA542 has been using polymorphic techniques to frequently alter the code of Emotet, making it difficult for traditional antivirus solutions to detect the malware. The group has also been using advanced evasion tactics to avoid detection by security researchers and automated defenses. For instance, new modules like Systeminfo and Hardwareinfo collect extensive data from compromised systems to verify the legitimacy of the victims and to avoid sandbox environments used for malware analysis.¹⁶ These modules collect detailed system information and use it to distinguish between actual targets and security analysis environments, thus enhancing the stealth and persistence of their operations. This resurgence has led to a significant increase in the number of Emotet-related attacks.

In March 2024 alone, Emotet activity grew threefold, underscoring the group's ongoing efforts to expand its reach and impact. TA542's ability to quickly adapt and innovate poses a serious challenge to cybersecurity defenses. The combination of updated phishing strategies, advanced evasion techniques, and modular capabilities makes Emotet a highly versatile and dangerous tool in TA542's arsenal. Continuous monitoring and updated defensive measures are essential to mitigate the threats posed by this persistent cybercriminal group.



IMPACT ASSESSMENT

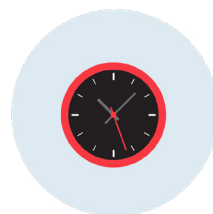
In 2024, TA542 significantly intensified its operations, with targeted campaigns against the United States and the United Kingdom. These attacks resulted in the compromise of numerous corporate and personal systems. Emotet's new modules, such as those for stealing credit card information and detailed system data, have amplified the impact, leading to significant data breaches and secondary infections with other malware like TrickBot and ransomware.¹⁷ This escalation underscores the persistent threat TA542 poses to global cybersecurity, necessitating enhanced vigilance and advanced defensive measures.



MITIGATION STRATEGIES

Organizations should adopt a comprehensive and multi-layered cybersecurity strategy to mitigate the threat posed by TA542 and Emotet. Here are key measures to consider:

- **Email Security and User Awareness:** Implement advanced email filtering solutions to detect and block phishing emails before they reach users' inboxes. Conduct regular cybersecurity awareness training for employees to recognize phishing attempts and avoid opening suspicious attachments or clicking on unknown links.
- **Endpoint Protection:** Deploy robust endpoint protection solutions that include behavior-based detection to identify and block Emotet and other malware. Ensure that all endpoints are regularly updated with the latest security patches and definitions.
- **Network Segmentation and Access Controls:** Implement network segmentation to limit the spread of malware within the organization. Use strict access controls to minimize user privileges and reduce the potential impact of a compromised account.
- **Incident Response Plan:** Develop and regularly update an incident response plan to quickly identify, contain, and remediate Emotet infections. This should include steps for isolating affected systems, removing the malware, and restoring operations.
- **Regular Backups:** Maintain regular, secure backups of critical data and systems. Ensure backups are stored offline or in a manner that prevents them from being targeted by malware. Regularly test the restoration process to ensure data integrity and availability.
- **Monitoring and Threat Intelligence:** Continuously monitor network traffic for signs of Emotet activity and leverage threat intelligence feeds to stay informed about the latest tactics, techniques, and procedures used by TA542. This proactive approach can help in early detection and prevention.



OUTLOOK

The outlook for TA542 suggests a continued evolution and persistence in their cybercriminal activities. Despite numerous law enforcement takedowns, TA542 has demonstrated a remarkable ability to adapt and re-emerge with enhanced tactics and tools. Their use of sophisticated phishing techniques and modular malware capabilities indicates they will likely continue to pose a significant threat to global cybersecurity. As they refine their methods to evade detection and enhance their data theft and malware distribution operations, organizations must remain vigilant and proactive in their defense strategies.¹⁸ The group's resilience and ability to innovate underscore the importance of ongoing cybersecurity awareness, advanced threat detection, and rapid incident response to mitigate potential impacts.

Scattered Spider

Scattered Spider is a highly organized and sophisticated cyber threat group known for its phishing and social engineering tactics. This actor targets a variety of industries, focusing on stealing sensitive information and disrupting operations. Their operations are characterized by advanced techniques and a persistent approach, making them a formidable adversary in the cybersecurity landscape.

Profile:

Scattered Spider emerged as a notable cyber threat actor in the mid-2010s, initially gaining attention for its adept use of phishing campaigns.¹⁹ This group, often linked to sophisticated social engineering tactics, managed to infiltrate a range of sectors, including healthcare, finance, and technology. Their early operations primarily involved stealing login credentials and sensitive data, which were then either sold on the dark web or used to further their cyber espionage activities. The group's adaptability and evolving techniques have allowed them to stay ahead of many traditional security measures, making them a persistent threat in the cybersecurity landscape.

Over the years, Scattered Spider's tactics have grown increasingly advanced. They have been observed using a combination of malware, phishing, and zero-day exploits to breach targeted systems.²⁰ Their ability to quickly pivot and exploit emerging vulnerabilities has made them a significant concern for organizations worldwide.

In addition to data theft, Scattered Spider has also been involved in disruptive activities, such as ransomware attacks, which further underline their capability and intent to cause widespread harm. The group's continuous evolution and sophisticated methods have established them as one of the more formidable adversaries in the realm of cyber threats.



ATTACK METHODS

Scattered Spider is renowned for its multifaceted attack methods, which combine traditional phishing techniques with advanced social engineering. Their initial attack vector often involves spear-phishing emails that are meticulously crafted to appear legitimate, targeting specific individuals within an organization. These emails frequently contain malicious attachments or links to fraudulent websites designed to harvest login credentials. By impersonating trusted entities or exploiting current events, Scattered Spider increases the likelihood of their targets engaging with these malicious elements, thus gaining initial access to internal systems.

Once inside a network, Scattered Spider employs a variety of tools to escalate their privileges and move laterally. They are known to use malware such as Remote Access Trojans (RATs) and custom scripts to maintain persistence and avoid detection. Their exploitation of zero-day vulnerabilities, which are previously unknown flaws in software, allows them to bypass conventional security defenses. Furthermore, the group often employs credential stuffing and brute-force attacks to gain control of additional accounts within the compromised environment. This multi-pronged approach ensures that they can extract valuable information while maintaining a foothold in the network.²¹

In recent years, Scattered Spider has also expanded its methods to include more destructive tactics such as ransomware. Encrypting critical files and demanding a ransom for their decryption caused significant operational disruptions for their victims. Additionally, they have been known to exfiltrate data before encryption, using the threat of public exposure as leverage to extort higher payments. This dual-threat model not only increases the chance of financial gain but also heightens the overall impact of their attacks. Scattered Spider's ability to blend espionage with sabotage makes them a particularly dangerous and unpredictable threat actor in the cyber landscape.



NOTORIOUS ATTACKS IN 2024

Scattered Spider struck in late April and early May 2024, targeting financial firms, including banks and insurance companies like Visa, PNC Financial Services Group, Transamerica, New York Life Insurance Co., and Synchrony Financial. Using advanced social engineering tactics, the threat actor redirected employees to specially crafted login pages through SMS messages and phishing emails, ultimately stealing the employees' credentials.



TECHNICAL ANALYSIS

In the past several months, Scattered Spider has demonstrated a significant evolution in their attack methods, particularly by incorporating ransomware into their repertoire. Initially known for sophisticated phishing and social engineering tactics, the group has now escalated its operations to include the deployment of ransomware, causing substantial disruption. One notable incident involved MGM Resorts last September, where they encrypted over 100 ESXi hypervisors, demonstrating their capability to execute large-scale ransomware attacks. This shift indicates a broader strategy aimed at both financial gain through extortion and the creation of operational chaos for targeted organizations.²²

Scattered Spider has also shown advanced techniques in maintaining persistence and escalating privileges once inside a network. They utilize everyday software and publicly available tools to explore and monitor compromised systems. For example, they have exploited tools like the CyberArk API and Azure penetration-testing tools to extract and utilize credentials from secure environments. By manipulating identity provider settings, they can gain single sign-on access to various applications within an organization, effectively broadening their reach and control within compromised networks.

Furthermore, Scattered Spider has targeted multiple sectors, including technology, finance, and hospitality, by leveraging a combination of phishing, malware, and ransomware. Their ability to adapt quickly to new vulnerabilities and exploit zero-day flaws has made them a persistent and formidable threat. The recent campaigns have underscored the necessity for robust cybersecurity measures, such as multi-factor authentication, vigilant monitoring of admin roles, and the use of phishing-resistant authentication methods to mitigate the risks posed by such advanced threat actors.²³



IMPACT ASSESSMENT

Scattered Spider has significantly escalated its cyber activities in the last several months, causing widespread disruption across multiple sectors.²⁴ The group has intensified its use of ransomware, notably encrypting over 100 ESXi hypervisors in an attack on MGM Resorts, leading to over \$100 million in financial losses for the company.

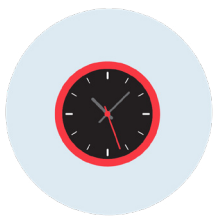
Additionally, Scattered Spider has exploited identity management systems by manipulating authentication flows, as seen in attacks on Okta customers, allowing them to gain high-level access and maintain persistence within networks.²⁵ These incidents highlight the group's growing sophistication and adaptability, underscoring the urgent need for enhanced cybersecurity measures to protect against such persistent threats.



MITIGATION STRATEGIES

To effectively mitigate the threats posed by Scattered Spider, organizations should adopt a multi-layered security approach that includes enhancing phishing defenses and enforcing strong authentication measures.²⁶ Here are key strategies:

- **Security Awareness Training:** Conduct regular training for employees so they are able to recognize and report phishing attempts.
- **Advanced Email Filtering Implementation:** Implement advanced email filtering solutions to prevent malicious emails from reaching users.
- **Multi-Factor Authentication (MFA):** Enforce multi-factor authentication (MFA) for privileged accounts and regularly update authentication protocols.
- **Identity and Access Management:** Utilize robust identity and access management (IAM) practices, including regular audits and least privilege principles.
- **Endpoint Detection and Response (EDR) Deployment:** Establish and regularly test comprehensive incident response plans.
- **Patch Management:** Keep all software and systems up to date with the latest security patches.²⁸



OUTLOOK

The threat outlook from Scattered Spider suggests that this threat actor will continue to evolve and adapt its tactics, posing significant challenges to cybersecurity defenses.²⁸

Given their recent shift towards ransomware and advanced identity exploitation techniques, they will likely further refine their methods to target critical infrastructure and high-value sectors. Organizations should anticipate increased sophisticated phishing campaigns and a higher incidence of attacks on identity and access management systems.²⁹

As Scattered Spider's techniques become more sophisticated, the need for advanced detection and response capabilities, along with proactive threat hunting, will become increasingly crucial to mitigate their impact.³⁰

Vulnerabilities

CVE-2024-20353 – Cisco Systems Vulnerabilities (CVSS 8.6 - High)

CVE-2024-20353 is a critical vulnerability affecting Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. This vulnerability is notable for allowing remote, unauthenticated attackers to craft HTTP requests to affected web servers, ultimately creating a Denial of Service (DoS) condition.

As far as active exploitation goes, this vulnerability has been seen in the past associated with an espionage campaign known as “ArcaneDoor”. These threat actors, which are state-sponsored, have been known to use this to infiltrate network perimeter devices, as well as critical infrastructure agencies and government organizations. The impact of this vulnerability, if successfully exploited, will ultimately cause the targeted device to reboot, due to the disruption of services that the vulnerability causes.

MITIGATION STRATEGIES

Mitigation strategies for this vulnerability have been addressed by the vendor, including software updates directly from Cisco. In addition, there are three main recommendations for this:

- **Update Affected Software:** Ensure that all Cisco ASA and FTD devices are updated to the latest software versions that contain the fixes for CVE-2024-20353.
- **Enhanced Monitoring:** Increase monitoring of web traffic and management interfaces to detect and respond to potential exploitation attempts.
- **Access Controls:** Strengthen access controls, including the use of multi-factor authentication (MFA) for accessing management interfaces.

CVE-2021-44529 – Ivanti Vulnerability (CVSS 9.8 – Critical)

CVE-2021-44529 is a code injection vulnerability stemming from Ivanti's Endpoint Manager Cloud Services Appliance (EPM CSA). This vulnerability allows unauthenticated remote attackers to execute arbitrary code with limited permissions, allowing for significant security breaches.

Since being actively exploited, this vulnerability has been noted in CISA's Known Vulnerabilities Catalog. Most noted for attacks featuring the ALPHA Spider group, this vulnerability has been connected with sophisticated cyber-espionage campaigns. Due to improper control of code generation, this vulnerability can attack web servers with a uniquely crafted HTTP request.

MITIGATION STRATEGIES

Mitigation strategies for this vulnerability include:

Update Software:

- Ensure all Ivanti Endpoint Manager CSA instances are updated to the latest versions that include patches for CVE-2021-44529.

Monitor for Indicators of Compromise:

- Actively monitor logs for any unusual activity or connections from unrecognized clients, which could indicate exploitation attempts.

Implement Strong Security Measures:

- Enhance access controls, apply network segmentation, and use intrusion detection systems to mitigate the risk of exploitation.

CVE-2024-26248 – Microsoft Vulnerability (CVSS 7.5 – High)

CVE-2024-26248 is an elevation of privilege vulnerability in the Windows Kerberos PAC (Privilege Attribute Certificate) Validation Protocol. This vulnerability allows attackers to spoof PAC signatures, potentially bypassing security checks and gaining elevated privileges.

This vulnerability is an extension to the Kerberos service tickets that contain user and privileged information, which is ultimately part of the Kerberos PAC. Left unchecked, this flaw can bypass the security checks through spoofed PAC signatures. With the potential impact to system security, this CVE received a score of 7.8 on the CVSS scale.

MITIGATION STRATEGIES

Mitigation strategies for this vulnerability include:

Update Systems:

- Ensure all Windows domain controllers and clients are updated with the security patches released on or after April 9, 2024.
- Regularly monitor for further updates from Microsoft to stay protected against this and related vulnerabilities.

Enable Enforcement Mode:

- After updating, configure your systems to enforce the new secure behavior by adjusting the registry settings as per the guidance provided in the official support documents. This includes setting `PacSignatureValidationLevel` and `CrossDomainFilteringLevel` to enforce mode values.

Monitor Systems:

- Use audit events to monitor the state of PAC validation and identify any devices that have not been updated or are not complying with the new security requirements.



REFERENCES

1. <https://blog.talosintelligence.com/mustang-panda-targets-europe/>
2. <https://www.bleepingcomputer.com/news/security/new-mustang-panda-hacking-campaign-targets-diplomats-isps/>
3. <https://www.techrepublic.com/article/cyberespionage-new-mustang-panda-campaign-targets-europe/>
4. <https://news.cloudsek.com/2024/02/mustang-pandas-plugx-variant-doplugs-malware-raises-cybersecurity-alarms-in-asia/>
5. <https://securityaffairs.com/159464/apt/mustang-panda-doplugs-backdoor.html>
6. <https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html>
7. <https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware>
8. <https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html>
9. <https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html>
10. <https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.htm>
11. <https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html>
12. <https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware#:~:text=Emotet%20infections%20have%20cost%20SLTT,evade%20typical%20signature%2Dbased%20detection>
13. <https://securityboulevard.com/2024/01/in-the-cyber-jungle-the-mighty-mustang-panda-phishes-tonight/>
14. <https://blog.malwarebytes.com/detections/trojan-emotet/>
15. <https://securityboulevard.com/2024/01/in-the-cyber-jungle-the-mighty-mustang-panda-phishes-tonight/>
16. <https://www.securityweek.com/emotet-resumes-activity-after-five-months-silence>
17. https://www.kaspersky.com/about/press-releases/2023_emotet-returns-lokibot-persists-kaspersky-reports-on-new-infection-methods
18. <https://www.welivesecurity.com/2023/07/06/whats-up-with-emotet/>
19. <https://www.cisa.gov/uscert/ncas/alerts/aa20-280a>
20. https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf
21. <https://www.bleepingcomputer.com/news/security/fbi-shares-tactics-of-notorious-scattered-spider-hacker-collective/>
22. <https://www.scmagazine.com/native/understanding-scattered-spider-and-how-they-perform-cloud-centric-identity-attacks>
23. https://www.theregister.com/2023/09/15/scattered_spider_snares_100_victims/
24. https://www.theregister.com/2023/09/01/okta_scattered_spider/
25. <https://www.darkreading.com/threat-intelligence/fbi-closes-in-scattered-spider-attacks-finance-insurance-orgs>
26. <https://socradar.io/major-cyber-attacks-in-review-march-2024/>
27. <https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks>
28. <https://phishgrid.com/blog/phishing-mitigation-strategies/>
29. https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf
30. <https://www.itpro.com/security/ransomware/scattered-spider-the-ransomware-group-behind-the-mgm-cyber-attack-is-still-on-a-rampage-and-authorities-are-ramping-up-efforts-to-catch-them>
31. <https://www.cisa.gov/news-events/alerts/2023/11/16/fbi-and-cisa-release-advisory-scattered-spider-group>



ILLUMINATE THREATS AND ELIMINATE RISKS

Learn more about how Adlumin's Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, eliminate cyber risk, and command authority; contact us today or schedule a demo at www.adlumin.com.



Adlumin is the security operations command center that simplifies complexity and keeps organizations of all sizes secure. Its innovative technology and seamless integrations create a feature-rich platform that includes everything a sophisticated security team needs, while empowering channel resellers, service providers and organizations of any size with the collaboration and transparency required to establish a coordinated and mature defense.

With a vendor-agnostic approach and preexisting integrations, Adlumin's Security Operations Platform obtains security telemetry from across an organization to provide greater insights into security alerts and streamline workflows. Organizations can use Adlumin's Security Operations Platform on their own or get full transparency and visibility while utilizing the 24/7 monitoring and response services provided by the Adlumin Managed Detection and Response (MDR) team. Whether organizations manage the platform on their own or with MDR, Adlumin consolidates all security needs for a unified experience.