Threat Intel Roundup: Phar, SEO Poisoning, ScreenConnect, Lockbit

Week in Overview[20 Feb-27 Feb] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1.ScreenConnect Vulnerabilities (CVE-2024-1709, CVE-2024-1708) for Malware Delivery: ConnectWise ScreenConnect, a remote desktop solution, was affected by two critical vulnerabilities (CVE-2024-1709, CVE-2024-1708) in its server component. CVE-2024-1709 enabled authentication bypass, allowing attackers to create admin accounts, while CVE-2024-1708 facilitated remote code execution through path traversal. Exploitation of these vulnerabilities led to the delivery of various malware payloads, including ransomware, RATs, and remote access clients. ConnectWise promptly released patches, urging users to upgrade to secure versions (v23.9.8 and later) to mitigate the risks associated with these vulnerabilities.

2. SilentCryptoMiner and UnamWebPanel: A Comprehensive Overview: SilentCryptoMiner is a native cryptocurrency miner capable of mining various cryptocurrencies silently. It features injection into system processes, idle mining, stealth mode, and remote configuration capabilities. UnamWebPanel complements SilentCryptoMiner by providing a web-based interface for monitoring and managing multiple miners efficiently. The panel is easy to set up, requiring a web server with PHP support. It allows users to remotely configure miner settings and monitor mining activity.

3. Sonar's Discovery: XSS Vulnerabilities in Joomla Exploiting PHP Bug: Sonar's Vulnerability Research Team discovered XSS vulnerabilities in Joomla, tracked as CVE-2024-21726, exploiting a PHP bug. Attackers leveraged these vulnerabilities to execute remote code by tricking administrators into clicking malicious links. Joomla released patches (v5.0.3/4.4.3) to mitigate the vulnerabilities. The underlying PHP bug (fixed in PHP 8.3 and 8.4) remained unpatched in older PHP versions. The exploitation of these vulnerabilities highlights the importance of keeping Joomla and PHP versions up-to-date to prevent security risks.

4.Gootloader Saga: SEO Poisoning to Domain Control: The Gootloader saga continued with threat actors exploiting SEO poisoning techniques to compromise websites and distribute malware. The attack involved delivering the Gootloader malware through poisoned search results, leading to the deployment of a Cobalt Strike beacon payload. Threat actors targeted domain controllers, backup servers, and other key servers to conduct reconnaissance and data exfiltration activities. While specific data exfiltration was not confirmed, the attack demonstrated the sophistication of Gootloader operations.

5. Hyper Realistic Re-Enactment of Lockbit CVE-2023-3824 Attack: A hyper-realistic re-enactment of the Lockbit CVE-2023-3824 attack was conducted, simulating the exploitation of a vulnerability in PHP. The attack involved crafting a PHP script to execute arbitrary code, leading to unauthorized access and potential data breaches. Insights from PHP internals experts were used to create an accurate portrayal of the attack, highlighting the importance of vulnerability management and security awareness.

6. North Korea's Lazarus Group Targets Defense Sector via Supply Chain Compromise: North Korea's Lazarus Group targeted the defense sector through a supply chain compromise, leveraging sophisticated tactics to infiltrate networks. The attack involved the distribution of malware payloads via compromised software vendors, allowing attackers to gain access to sensitive information and conduct espionage activities. The incident underscores the evolving threat landscape and the need for robust supply chain security measures to mitigate risks.

7. Season 2 Premiere of FBI vs Lockbit Ransomware Group: The season 2 premiere of FBI vs Lockbit Ransomware Group showcased ongoing efforts by law enforcement agencies to combat ransomware threats. The episode highlighted recent developments in the investigation and strategies employed to disrupt ransomware operations. It emphasized collaboration between international law enforcement agencies and private sector partners to dismantle ransomware infrastructure and hold threat actors accountable.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- ScreenConnect Vulnerabilities (CVE-2024-1709, CVE-2024-1708) for Malware Delivery
- SilentCryptoMiner and UnamWebPanel: A Comprehensive Overview
- Sonar's Discovery: XSS Vulnerabilities in Joomla Exploiting PHP Bug
- Gootloader Saga: SEO Poisoning to Domain Control
- Hyper Realistic Re-Enactment of Lockbit CVE-2023-3824 Attack
- North Korea's Lazarus Group Targets Defense Sector via Supply Chain Compromise
- Season 2 Premiere of FBI vs Lockbit Ransomware Group

🚨 Vulnerability of the Week

Joomla CVE-2024-21726

Sonar's Vulnerability Research Team has uncovered a critical security issue affecting the widely used Content Management System (CMS) Joomla. Multiple Cross-Site Scripting (XSS) vulnerabilities were discovered in Joomla's core filter component, presenting a significant risk to websites running vulnerable versions. Tracked as CVE-2024-21726, the vulnerability stems from an underlying inconsistency in how PHP's mbstring functions handle invalid multibyte sequences. Exploiting this flaw could allow attackers to execute remote code by tricking administrators into clicking on malicious links.

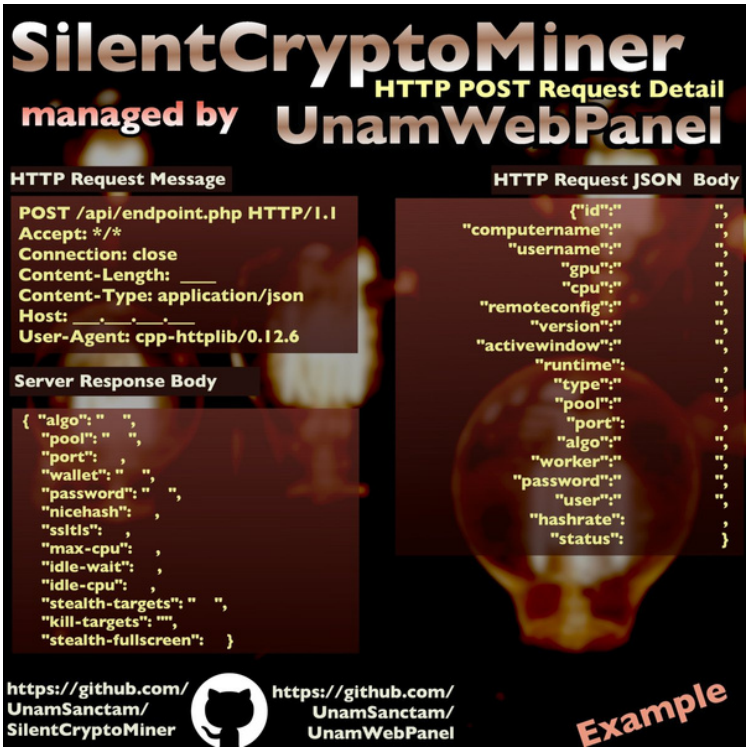
Key Information:

1. Vulnerability Discovery:
   - Sonar's research revealed XSS vulnerabilities in Joomla's core filter component, traced back to a PHP bug. The bug, identified with the help of SonarCloud, allows attackers to bypass input sanitization and execute arbitrary code.
2. Exploitation and Impact:
   - Attackers can exploit the vulnerability by crafting malicious links that, when clicked by administrators, trigger the execution of arbitrary code.
   - Joomla versions 5.0.2/4.4.2 and below are susceptible to the XSS vulnerabilities, potentially leading to remote code execution.
   - Although the PHP bug was addressed in PHP versions 8.3 and 8.4, it remains unpatched in older PHP versions, leaving systems vulnerable.
3. Patch and Mitigation:
   - Joomla promptly released version 5.0.3/4.4.3, which mitigates the XSS vulnerability regardless of the PHP version used.
   - The patch involves replacing the mbstring functions with PHP's regular string functions, ensuring consistent behavior and enhancing security.
   - SonarCloud has reported the inconsistent behavior of mbstring functions to PHP maintainers, although the patch has not been backported to older PHP versions.

Technical Details:

- The XSS vulnerability arises from Joomla's core filter logic, which fails to properly sanitize user input due to the inconsistent behavior of PHP's mbstring functions.
- Attackers exploit this inconsistency to offset the index returned by StringHelper::strpos, allowing the insertion of arbitrary HTML tags and bypassing Joomla's sanitization measures.
- By crafting malicious links, attackers can inject JavaScript payloads, leading to remote code execution when administrators interact with the compromised links.
- Joomla's patch involves replacing mbstring functions with PHP's regular string functions, addressing the underlying PHP bug and enhancing security across Joomla deployments.

😰 Malware or Ransomware



https://twitter.com/Jane_0sint/status/1760278859960741917

SilentCryptoMiner and UnamWebPanel, developed by UnamSanctam, represent a comprehensive solution for cryptocurrency mining management. SilentCryptoMiner is a versatile, native cryptocurrency miner capable of mining various cryptocurrencies silently, while UnamWebPanel serves as a web-based monitoring and management platform for SilentCryptoMiner and potentially other projects. This report provides an overview of the features, setup, and implications of these tools.

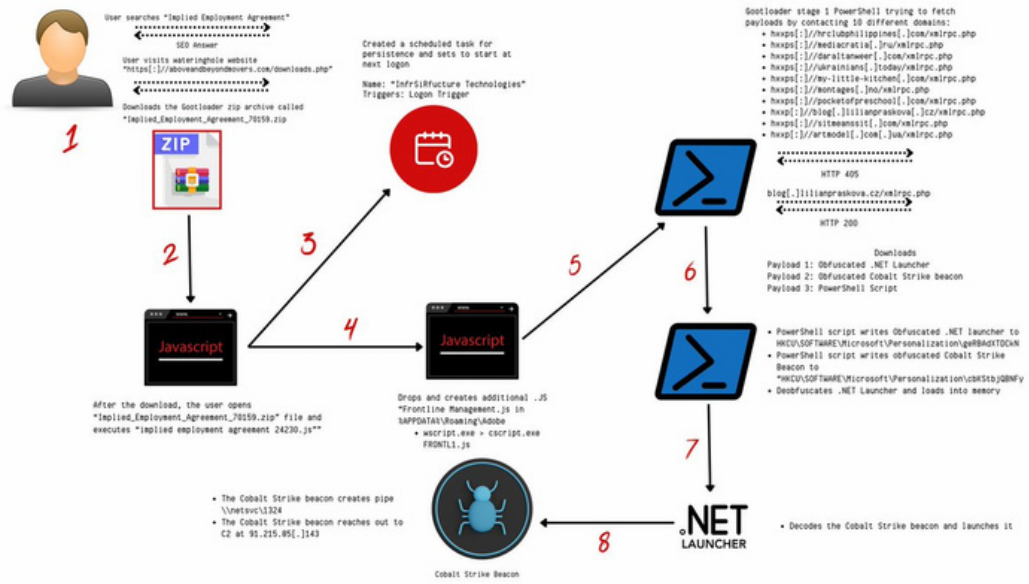
SilentCryptoMiner:
SilentCryptoMiner (v3.4.0) is a free, native cryptocurrency miner offering a range of features tailored for silent mining operations. Key features include:

- Native C++ implementation: Fully coded in C++ with no runtime requirements, ensuring compatibility with 64-bit operating systems.
- Injection capabilities: Capable of hiding the miner within other processes such as conhost.exe, explorer.exe, and svchost.exe, enhancing stealth.
- Idle mining configuration: Allows users to customize CPU and GPU usage thresholds for mining during system idle periods.
- Stealth mode: Pauses the miner and clears GPU memory and RAM when specified programs are open, increasing stealthiness.
- Watchdog functionality: Monitors miner processes and system startup entries, ensuring continuous operation by restoring the miner if tampered with.
- Remote configuration: Can retrieve miner settings remotely from a specified URL, facilitating efficient management.
- Windows Defender exclusions: Automatically adds exclusions to Windows Defender to evade detection.
- Multiple miners support: Enables simultaneous mining with multiple instances for different cryptocurrencies.
- CPU and GPU mining: Supports mining on both CPU and GPU (Nvidia & AMD), providing flexibility.
- Process killer: Constantly monitors and terminates specified processes to maintain mining performance.

UnamWebPanel:
UnamWebPanel (v1.8.0) is a web-based management platform designed to monitor and manage SilentCryptoMiner installations. Key features include:

- Easy setup: Requires only a web server with PHP support for deployment.
- Password protection: Utilizes password authentication to restrict access to the web panel.
- Monitoring and configuration: Allows users to monitor miner hashrates, status, and connection settings, as well as change miner settings remotely.
- Compatibility: Can be hosted on both self-hosted and online web hosts, providing flexibility in deployment.

Art of Detection



https://twitter.com/NathanMcNulty/status/1762307981994316023

The ongoing saga of the Gootloader malware continues with a recent intrusion that demonstrates the sophisticated tactics employed by threat actors to compromise networks. The attack, which commenced in February 2023, involved the exploitation of SEO poisoning techniques to lure unsuspecting users into downloading malicious files. Subsequently, the Gootloader malware facilitated the deployment of a Cobalt Strike beacon payload, leading to the compromise of domain controllers, backup servers, and other critical infrastructure components. Despite the extensive infiltration, it remains uncertain whether any data was exfiltrated during the attack.

Key Points:

1. Initial Access:
   - The intrusion began when a user clicked on a SEO-poisoned search result related to employment agreements, leading them to a compromised website masquerading as a user forum.
   - The user was prompted to download a zip file containing a JavaScript file, which initiated the execution process for the Gootloader malware.
2. Execution:
   - Gootloader malware executed a series of stages, including the creation of additional JavaScript files, establishment of scheduled tasks for persistence, and deployment of obfuscated PowerShell scripts.
   - Nine hours after the initial infection, Gootloader facilitated the download and execution of a Cobalt Strike beacon payload directly into the host's registry, allowing for further exploitation.
3. Persistence:
   - Gootloader established persistence by creating scheduled tasks and logon triggers, ensuring continuous operation within the compromised environment.
   - Additionally, the threat actor deployed SystemBC, a PowerShell script, and ensured its persistence through an autorun key named 'socks_powershell'.
4. Domain Control Compromise:
   - The threat actor leveraged SystemBC to tunnel RDP access into the network, enabling access to domain controllers and other critical servers.
   - Despite attempts to disable Windows Defender and deploy additional payloads, the attacker's efforts were partially thwarted by security measures.
5. Interactive Review and Data Access:
   - The threat actor conducted an interactive review of sensitive files using RDP sessions, although no concrete evidence of data exfiltration has been confirmed.
   - Access to backup servers and exploration of file shares for password-related documents were observed, indicating attempts to gather sensitive information.

THREATRADAR
By HADESS

TTP Analysis

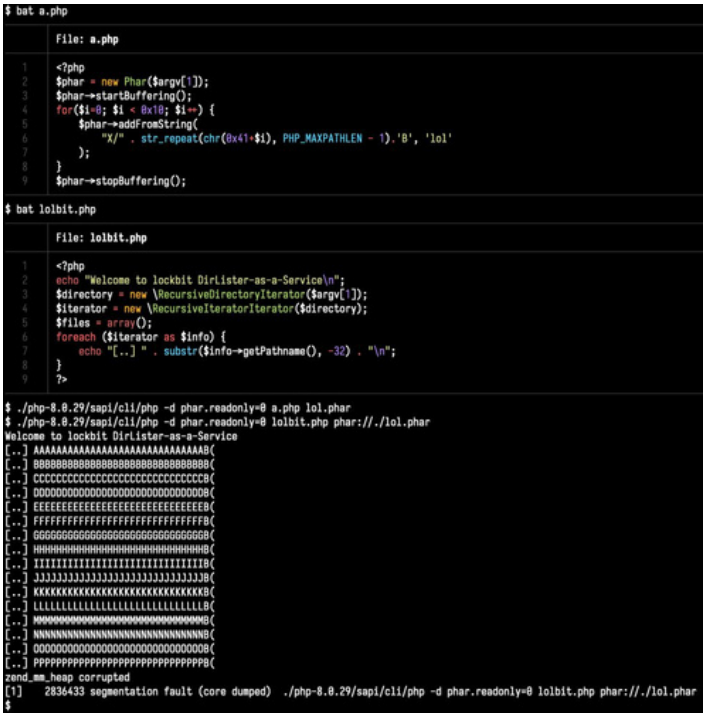
A recent joint advisory by Germany's BfV (Federal Office for the Protection of the Constitution) and the Republic of Korea's NIS (National Intelligence Service) sheds light on a sophisticated supply chain compromise orchestrated by North Korea's Lazarus Group. The operation was aimed at infiltrating the defense sector, specifically targeting research related to submarine development. The advisory highlights the group's utilization of advanced tactics to infiltrate a maritime research organization's website maintenance and repair supplier, ultimately aiming to steal trade secrets and deploy malicious software.

Key Points:

1. Supply Chain Compromise: Lazarus Group targeted a website maintenance and repair supplier of a maritime research organization, exploiting the trusted relationship between the supplier and the defense sector entity. This allowed Lazarus to gain unauthorized access to the target's web server, leveraging stolen SSH keys for entry.
2. Deployment of Malicious Software: Using the compromised web server, Lazarus deployed a malicious payload named "NukeSped" via patch management systems (PMS). The payload was disguised as a legitimate patch named "EncryptModule_Patch.exe" and was designed to steal sensitive information, execute code, and collect system data.
3. TTPs (Tactics, Techniques, and Procedures): Lazarus utilized a variety of techniques to maneuver within the network, including the use of SSH for lateral movement, TCP Dump for network data collection, and the theft of employee credentials. The group also accessed the Security Manager's mailbox to understand patch management procedures and facilitate the deployment of the malicious patch.
4. Detection and Prevention: The Security Manager identified the malicious activity and prevented the deployment of the NukeSped malware, averting potential damage to the defense sector's research efforts. The incident underscores the importance of robust security controls, particularly in the context of legacy remote working arrangements exacerbated by the COVID-19 pandemic.
5. Legacy Remote Working and Security Risks: The advisory highlights the risks associated with legacy remote working arrangements, which may lack sufficient security controls and inadvertently provide adversaries with unattended access to critical servers. Lazarus exploited these vulnerabilities to persist within the network and execute their malicious objectives.

https://twitter.com/Intel_Ops_io/status/1761030666186068431

1Day



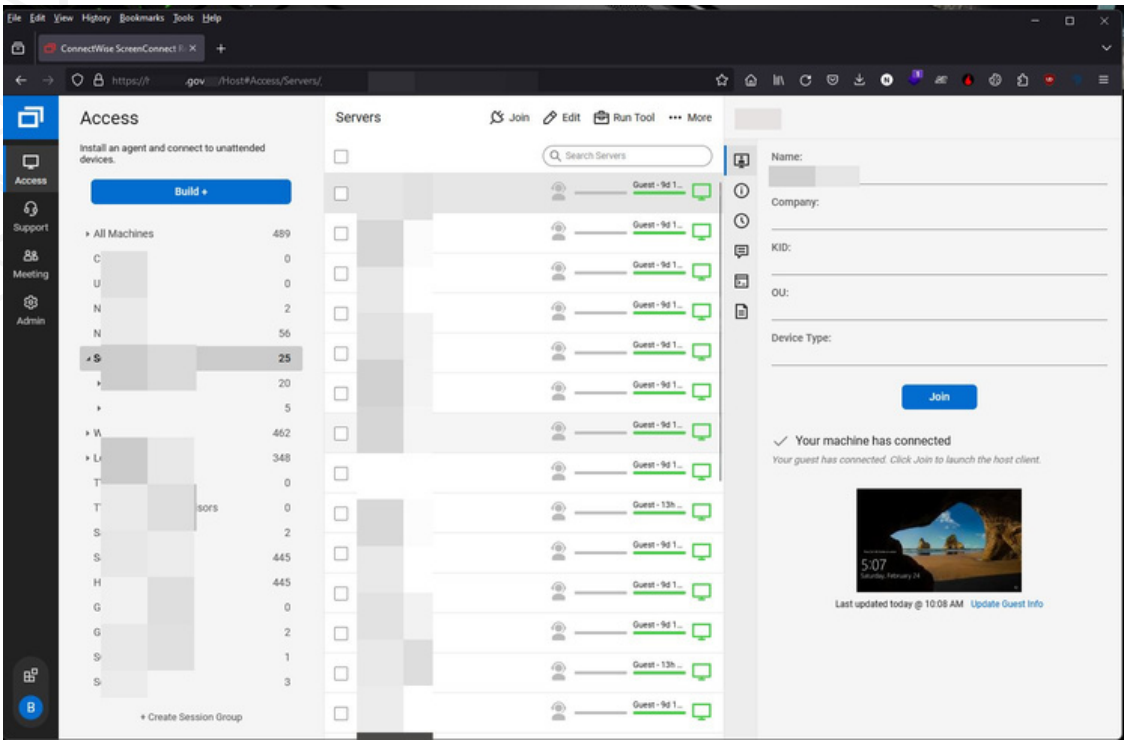
https://twitter.com/bl4sty/status/1759960424785547570

A hyper-realistic re-enactment of the Lockbit CVE-2023-3824 attack has been successfully created, leveraging insights from a PHP internals expert. This simulation demonstrates the intricate techniques utilized by threat actors to exploit vulnerabilities within the PHP environment, specifically targeting the Phar extension. The attack scenario involves the creation and manipulation of Phar archives to execute malicious code, ultimately facilitating unauthorized access to sensitive systems.

Key Points:

1. Attack Simulation:
   - The re-enactment begins with the creation of two PHP files: "a.php" and "101bit.php."
   - "a.php" utilizes the Phar extension to create a Phar archive named "lo1.phar" by adding strings of specific lengths to the archive.
   - The Phar archive construction includes a loop iterating through a range of values to generate strings with variable lengths, exploiting the vulnerability outlined in CVE-2023-3824.
   - Once the Phar archive is constructed, the buffering process is stopped, and the malicious archive is ready for deployment.
2. Deployment and Execution:
   - "101bit.php" serves as the entry point for the attack, functioning as a "DirLister-as-a-Service."
   - Upon execution, the script welcomes users to the Lockbit DirLister service and proceeds to list the contents of a specified directory.
   - The script recursively iterates through the directory structure, printing out filenames while obscuring their paths.
   - The Phar archive "lo1.phar" is deployed using PHP's CLI interpreter with specific directives to disable Phar readonly mode.
   - Through the deployment of the malicious Phar archive, the Lockbit attack is initiated, potentially granting unauthorized access to critical systems.
3. Insights from PHP Internals Expert:
   - The success of the re-enactment is attributed to insights provided by a PHP internals expert, enabling the accurate portrayal of the attack scenario.
   - Leveraging expertise in PHP internals, the simulation demonstrates a deep understanding of the underlying vulnerabilities and exploit techniques employed by threat actors.

🌶️ Trending Exploit



https://twitter.com/helpnetsecurity/status/1762077550203789795

ConnectWise ScreenConnect, a popular remote desktop solution, recently patched two critical vulnerabilities (CVE-2024-1709, CVE-2024-1708) affecting its server component. These vulnerabilities have been actively exploited by threat actors to deliver various types of malware, posing significant risks to affected organizations.

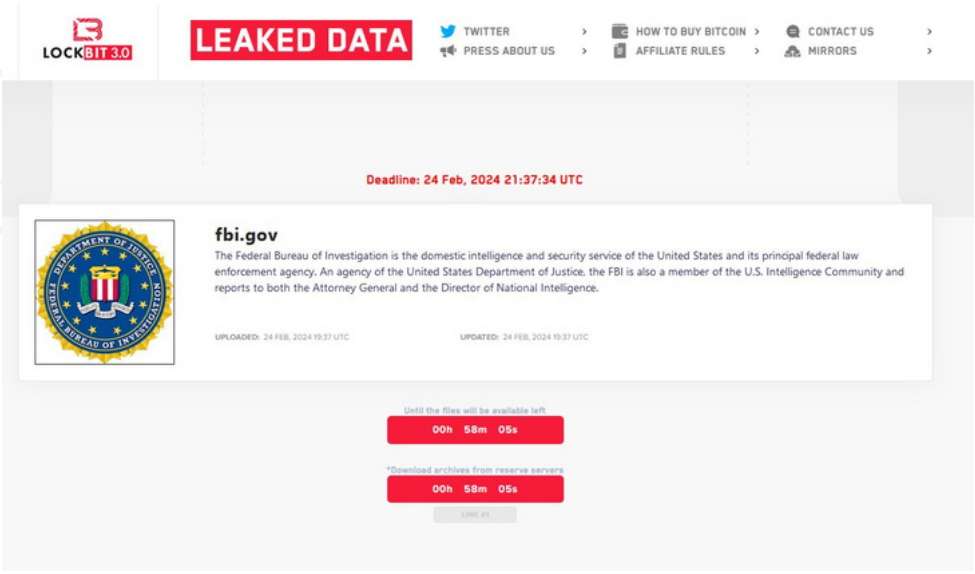
ConnectWise ScreenConnect comprises server and client elements, facilitating remote access to endpoints for technical assistance and data center management. While it is widely used for legitimate purposes, its accessibility also makes it an attractive target for attackers seeking to compromise enterprise endpoints.

The vulnerabilities affect ConnectWise ScreenConnect server versions 23.9.7 and earlier. CVE-2024-1709 allows authentication bypass, enabling attackers to create system admin accounts for malicious activities. CVE-2024-1708 permits remote code execution through path traversal.
ConnectWise promptly patched its cloud environments and urged customers to upgrade on-premises instances to version 23.9.8. Subsequently, versions 23.9.10.8817 and 22.4 were released, addressing the vulnerabilities for all users, including those not under maintenance.

Following the public availability of proof-of-concept exploits for CVE-2024-1709, threat actors targeted vulnerable ScreenConnect servers to infiltrate enterprise networks. Exploitation has led to the deployment of ransomware, infostealers, RATs, worms, Cobalt Strike payloads, and remote access clients.
Mandiant, Sophos X-Ops, and Huntress researchers have observed mass exploitation, with attackers employing multifaceted extortion tactics, ransomware deployment, and various malware payloads.

Organizations that failed to patch their ScreenConnect instances face the daunting task of identifying compromises, assessing the extent of intrusion, and cleaning affected systems. Immediate isolation of vulnerable servers and clients, patching, and thorough investigation are recommended by security experts.
Sophos advises organizations to be vigilant for ongoing attacks targeting both servers and client machines, emphasizing the importance of patching alongside comprehensive security assessments and remediation efforts.

The Topic of the Week



https://twitter.com/vxunderground/status/1761491834436476937

The highly anticipated Season 2 premiere of the FBI's battle against the Lockbit ransomware group is set to debut in approximately one hour. Lockbit, a notorious cybercriminal organization, has recently restored its servers utilizing new Tor domains. Moreover, the group intends to issue a statement to the FBI regarding the events surrounding the previous week's takedown.

Key Points:

1. Season 2 Premiere: The commencement of Season 2 marks a new chapter in the ongoing saga between law enforcement agencies and cybercriminal entities. Viewers can expect heightened tensions, strategic maneuvers, and unforeseen twists as the FBI continues its pursuit of Lockbit.
2. Lockbit's Server Restoration: Despite facing setbacks from the recent takedown operation, Lockbit has swiftly rebounded by restoring its servers. The adoption of new Tor domains suggests the group's resilience and adaptability in the face of adversity.
3. Planned Statement to the FBI: In a bold move, Lockbit plans to issue a statement directly addressing the FBI regarding the recent events. The nature and content of this statement remain unknown, adding an element of suspense to the unfolding narrative.
4. Stay Tuned: As the Season 2 premiere approaches, audiences are encouraged to stay tuned for further developments in this high-stakes cyber conflict. The next episode promises to deliver gripping action, intricate plotlines, and the continuation of the epic struggle between the FBI and Lockbit.

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Threat Radar
WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.