Threat Intel Roundup: XWiki, clOp, HTML Smuggling

Week in Overview(21 Aug-28 Aug)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

XWiki Remote Code Execution (CVE-2023-35150)
The XWiki vulnerability (CVE-2023-35150) involves improper input validation within the "Invitation Application." Authenticated attackers can exploit this flaw by manipulating requests, leading to arbitrary code execution. XWiki's scripting feature, used to create web applications, includes an "Invitation Application" facilitating email notifications for user registration. The vulnerability arises when unvalidated user data renders a link based on unsanitized request-URIs. Successful exploitation allows an attacker to execute arbitrary code.

Malware Analysis and Dynamic Extraction of Xworm Payload
In this analysis, a Golang file is examined, dynamically extracting an Xworm payload. Techniques such as Procmon, Process Hacker, Entropy Analysis, and Debuggers are used. The 1.5GB Golang file is debloated using "pe-debloat" tool, reducing its size to 960KB. Process monitoring reveals the malware's activities, including scheduled tasks, library loading, and code execution. The loaded .NET assemblies are scrutinized using Dnspy, revealing capabilities such as keylogging and system enumeration. Decoding encrypted configuration yields insight into Xworm malware's intent.

Threat Analysis Report - StealC Malware Campaign via "Request Booking" Spam Email
This report delves into a malware campaign using "Request Booking" spam emails to spread the StealC malware. It covers the payload, URLs, and C2 server. The spam email prompts victims to download a password-protected ZIP file containing a malicious .cmd script. Upon execution, the script downloads a PowerShell script from GitHub, initiating malware infection. The report details the infection chain and offers detection guidance for the campaign's artifacts.

Threat Analysis Report - Metamorfo (Casbaneiro) Campaign Targeting Mexico
This analysis focuses on a Metamorfo (Casbaneiro) campaign targeting Mexico. It outlines the attack's execution chain, from phishing to payload execution. Victims are lured to a URL, leading to a .rar file and a series of scripts. AutoIT and other techniques are exploited for persistence, eventually leading to the execution of Metamorfo DLLs. The report provides insights into the attacker's tactics and detection suggestions.

Incident Analysis Report - Nokoyawa Ransomware Campaign with HTML Smuggling and Rapid Execution
This incident analysis report examines a Nokoyawa ransomware campaign utilizing HTML smuggling for domain-wide ransomware deployment. The attack chain involves Excel macro and IcedID malware, with Nokoyawa ransomware executed within 12 hours of initial compromise. The report details the intrusion timeline, attacker actions, lateral movement, and the ransomware's execution. The rapid progression from compromise to ransomware highlights the threat's sophistication.

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:

- **XWiki Remote Code Execution (CVE-2023-35150)**
- **Loss of Funds Due to Malicious Blur Bid in NFT Auction**
- **Nokoyawa Ransomware Campaign with HTML Smuggling and Rapid Execution**
- **StealC Malware Campaign via "Request Booking" Spam Email**
- **Malware Analysis and Dynamic Extraction of Xworm Payload**

Cyber Threat Map

XWiki: CVE-2023-35150

Winrar Lazy Exploit

cl0p: 7 new target based on moveit

Xworm Malware

🚨 Vulnerability of the Week

XWiki

CVE-2023-35150

This vulnerability report delves into a recently patched remote code execution flaw identified in the XWiki free wiki software platform. The analysis, conducted by Simon Humbert and Lucas Miller of the Trend Micro Research Team, elucidates the nature of the vulnerability, its exploitation vectors, and its potential consequences. This report offers insights into the discovered vulnerability's characteristics and the measures taken to mitigate its impact.

Vulnerability Overview:

1. **CVE Identifier:** CVE-2023-35150
2. **Affected Software:** XWiki
3. **Type:** Remote Code Execution
4. **Discoverer:** Michael Hamann
5. **PoC Source:** Manuel Leduc

Exploitation Details:
The vulnerability in XWiki arises due to improper input validation when processing a link within the Invitation Application. An authenticated attacker can exploit this flaw by submitting manipulated requests to the target server, eventually leading to the execution of arbitrary code.

XWiki's Scripting and Invitation Application:
XWiki, a second-generation wiki with integrated application development capabilities, supports scripting languages like Velocity, Groovy, and Python. Its scripting feature allows users to create complex web applications within XWiki pages, making it a versatile platform. The "Invitation Application" facilitates email notifications for user registration, enabling the user to follow a link to register.

Vulnerability Exploitation:
The vulnerability stems from inadequate validation of user data presented by the "Invitation Application." While requests to this application often include multiple parameters, the "action" parameter dictates the actions to be taken. If the "action" parameter is absent, the server constructs a link based on the request-URI without sanitization. An attacker can inject malicious script code into the request-URI, which is then executed during link rendering. This allows the attacker to execute arbitrary code.

Source Code Analysis:
The vulnerable code is found in the **InvitationGuestActions.xml** file. The XML snippet reveals the handling of various actions and configuration settings within the "Invitation Application." Vulnerable code sections include the evaluation of script code and the rendering of links based on unsanitized request-URIs.

Detection Guidance:
To detect an ongoing attack exploiting this vulnerability, monitoring devices must parse traffic over HTTP (port 8080/TCP) and HTTPS (port 8443/TCP). Detection involves inspecting requests with the string **/xwiki/bin/view** in the request-URI. Specific request parameters with the names "sheet" (with the value "Invitation.InvitationGuestActions") and "xpage" (with the value "view") are also examined. Suspicion arises when the request-URI contains the characters **{{** or their URL-encoded equivalent **%7B%7B**.

⛳ Leakage Insight

https://twitter.com/SOSIntel/status/1694343808559784176

The following domains have been identified as affected by the data leakage incident:

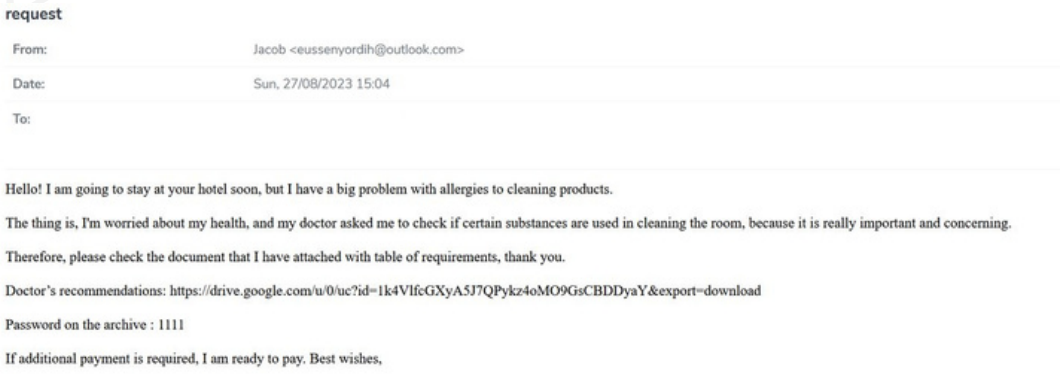
1. sapiens.com
2. enstargroup.com
3. cpiai.com
4. digitalinsight.no
5. fisglobal.com
6. hornbeckoffshore.com
7. clicksgroup.co.za

Incident Overview:

A data leakage incident involves the unauthorized exposure or access to sensitive and confidential information belonging to an organization. In this case, the aforementioned domains have been identified as experiencing data leakage. The nature and scope of the compromised data may vary among the affected domains, but the potential impact on each organization's security and reputation is significant.

The cl0p ransomware group has demonstrated an evolving and adaptable modus operandi in targeting organizations for financial gain. Their focus on targeting the MOVEit File Transfer System indicates a strategic shift towards exploiting critical data transfer systems, potentially leading to the encryption of sensitive files and significant operational disruption.

Malware Distribution Sites



request

From: Jacob <eussenyordih@outlook.com>

Date: Sun, 27/08/2023 15:04

To:

Hello! I am going to stay at your hotel soon, but I have a big problem with allergies to cleaning products.

The thing is, I'm worried about my health, and my doctor asked me to check if certain substances are used in cleaning the room, because it is really important and concerning.

Therefore, please check the document that I have attached with table of requirements, thank you.

Doctor's recommendations: https://drive.google.com/u/0/uc?id=1k4VlfcGXyA5J7QPykz4oMO9GsCBDDyaY&export=download

Password on the archive : 1111

If additional payment is required, I am ready to pay. Best wishes,

https://twitter.com/JAMESWT_MHT/status/1695831298000949256

This threat analysis report examines a new variant of the StealC malware campaign, which is being distributed via "Request Booking" spam emails. The campaign utilizes malicious payloads to compromise victims' systems and potentially steal sensitive information. The report provides a detailed breakdown of the attack vectors, malware samples, and potential impact, along with recommendations to enhance defenses against this evolving threat.

Attack Vector:

The attack vector for this StealC campaign involves "Request Booking" spam emails, luring victims to interact with malicious content. The email prompts recipients to open a malicious link, leading to the download and execution of malicious payloads.

Malware Samples:

1. **Sample Payload #1:** A sample payload with the password "1111" has been identified. The sample is available at: https://bazaar.abuse.ch/sample/a342176ba19085a68ccb25363001ede0ad9d5302fef17ef4efbd4543c4c57782/
2. **Sample Payload #2 (Payload):** The payload associated with the campaign can be found at: https://bazaar.abuse.ch/sample/7083e4774a68e23dd2f9239e5108f6615ff945a0673e7e975ab2ca2d4cb297d3/

Payload URL: The payload is distributed via the following URL: [**https://drive.[google.com/u/0/uc?id=1k4VlfcGXyA5J7QPykz4oMO9GsCBDDyaY&export=download**]

Command and Control (C2) Server: The malware communicates with a C2 server located at **http://45.9.74.]92/7a03fb9d4773da33.php**
Attack Breakdown:

Spam Email: Victims receive a "Request Booking" spam email, enticing them to interact with malicious content.

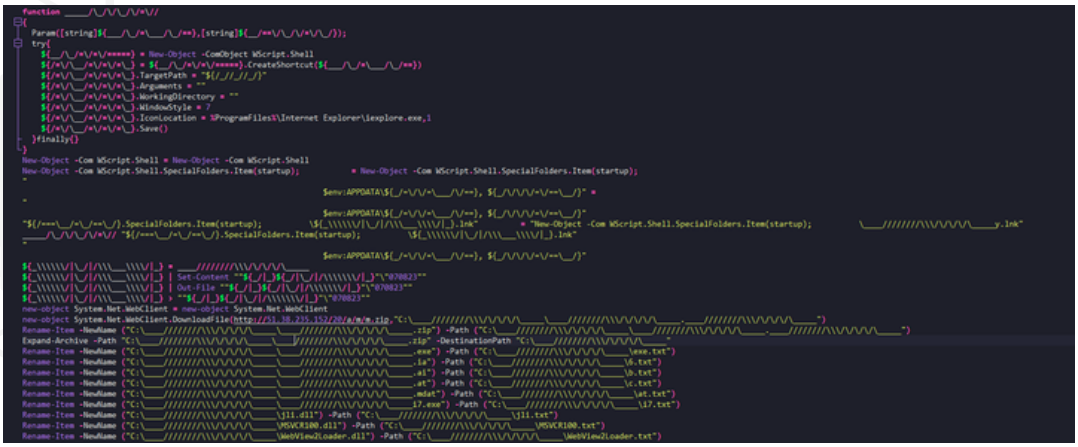
Malicious Link: Recipients are prompted to click on a malicious link leading to the payload download URL.

Payload Download: The malicious payload is downloaded from the provided URL.

Payload Execution: The payload is executed on the victim's system, potentially compromising their security.

C2 Communication: The malware communicates with the C2 server, establishing a connection to a remote attacker.

Proxylife



https://twitter.com/0xToxin/status/1694756006889206044

This threat analysis report examines a recent cyberattack campaign attributed to the Metamorfo (also known as Casbaneiro) malware targeting Mexico. The campaign involves a multi-stage execution chain, encompassing phishing, payload download, malicious script execution, and the deployment of Metamorfo malware. This report provides a detailed breakdown of the attack stages, tactics, and potential impacts, along with recommendations to enhance defenses against such attacks.

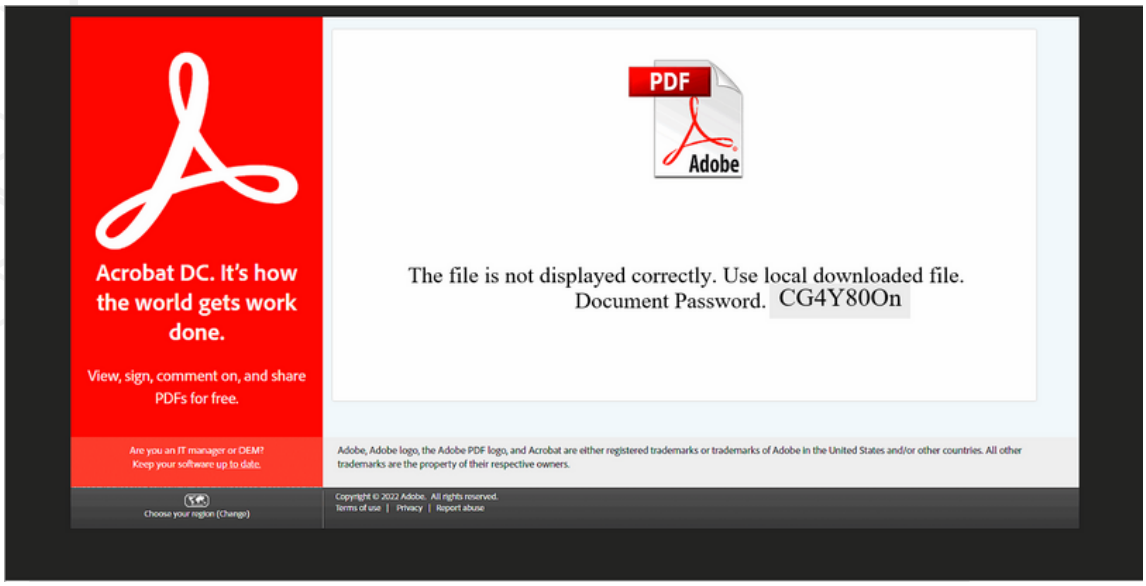
Attack Chain Overview:

1. **Phishing:** Victims are lured through a simple phishing email containing a URL that initiates the download of a malicious .rar archive.
2. **Payload Download:** The downloaded .rar archive contains a .cmd script that executes a PowerShell command to download another script hosted on GitHub.
3. **Malicious Script Execution:** The downloaded PowerShell script, likely containing malicious code, is executed, leading to the download and execution of an AutoIT script.
4. **AutoIT Execution:** The AutoIT script forces a system shutdown and establishes persistence through autorun mechanisms.
5. **Metamorfo (Casbaneiro) Deployment:** The attack culminates in the execution of Metamorfo (Casbaneiro) Dynamic Link Libraries (DLLs), enabling the malware's malicious activities.

Attack Stages Breakdown:

- **Phishing:** Victims are directed to a malicious URL (hxxps://agost[.]shop/aZ1Tta) through a phishing email. The URL triggers an auto-download of a malicious .rar archive.
- **Payload Download:** The .rar archive contains a .cmd script responsible for executing a PowerShell command. This command downloads a PowerShell script from GitHub (hxxps://github[.]com/factu1/factu1/blob/main/8.txt).
- **Malicious Script Execution:** The downloaded PowerShell script is executed, initiating further malicious activities.
- **AutoIT Execution:** An AutoIT script is executed, causing a force shutdown of the system. This stage aims to establish persistence through autorun mechanisms.
- **Metamorfo Deployment:** The execution of Metamorfo (Casbaneiro) DLLs marks the final stage, enabling the malware's data theft and banking credential harvesting capabilities.

TTP Analysis



https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/

This incident analysis report delves into a sophisticated Nokoyawa ransomware campaign that utilized HTML smuggling, IcedID malware, Cobalt Strike, and swift execution to compromise target organizations. The attack, which transpired in November 2022, showcases the threat actor's use of various tactics to achieve a domain-wide ransomware compromise within a remarkably short timeframe. The report offers insights into the attack's lifecycle, techniques employed, and recommendations for enhancing cybersecurity practices.

Attack Lifecycle:

Initial Compromise: The attack initiated with the delivery of an HTML file, potentially via email, using HTML smuggling to evade security measures. The HTML file led to the download of a password-protected ZIP file containing an ISO file.

Payload Delivery: Inside the ZIP file, the ISO file held the IcedID malware payload. A LNK file disguised as a document was visible to the user, who interacted with it.

Payload Execution: Clicking the LNK file triggered the execution of malicious commands, copying rundll32 and a malicious DLL from the ISO to the host. The DLL established a connection to IcedID command and control servers.

Lateral Movement: A series of commands led to IcedID establishing persistence on the host via a scheduled task. The malware collected system information using utilities like net, ipconfig, systeminfo, and nltest.

Cobalt Strike Engagement: After a few hours, IcedID spawned a cmd process that connected to a Cobalt Strike server, accessing LSASS and checking domain admins.

Domain Controller Access: The threat actor, using Cobalt Strike, identified domain administrators through net utility and initiated an RDP session to a domain controller. A Cobalt Strike beacon was placed on the domain controller.

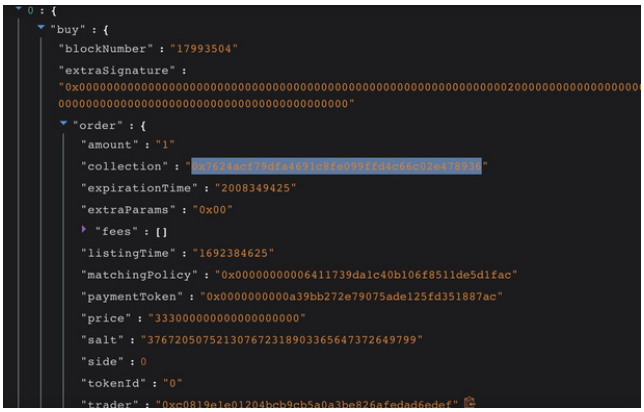
Discovery and Lateral Movement: The threat actor conducted Active Directory discovery using AdFind, archived results, and performed nslookup across the network.

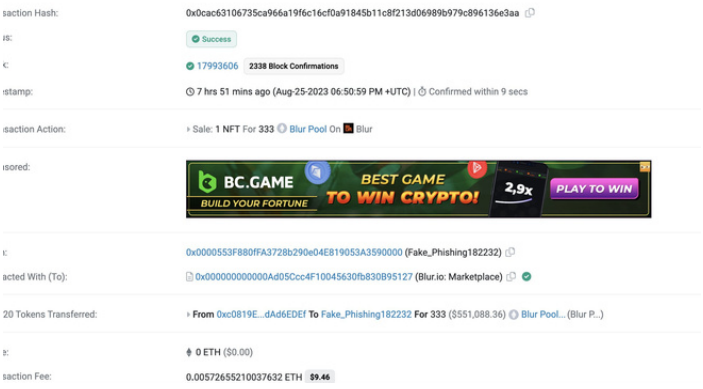
SessionGopher Usage: The threat actor employed encoded PowerShell (SessionGopher) on the domain controller to decrypt saved session information. Access to backup servers and file shares ensued.

Network Scan and File Movement: After a network scan, PsExec and WMIC facilitated file movement across systems. Key files included the ransomware binary and an executing batch script.

Ransomware Execution: Nokoyawa ransomware was executed on a domain controller using PsExec to initiate the process on other hosts in the domain. The ransomware attack commenced just over 12 hours after the initial infection.

Scam Contract



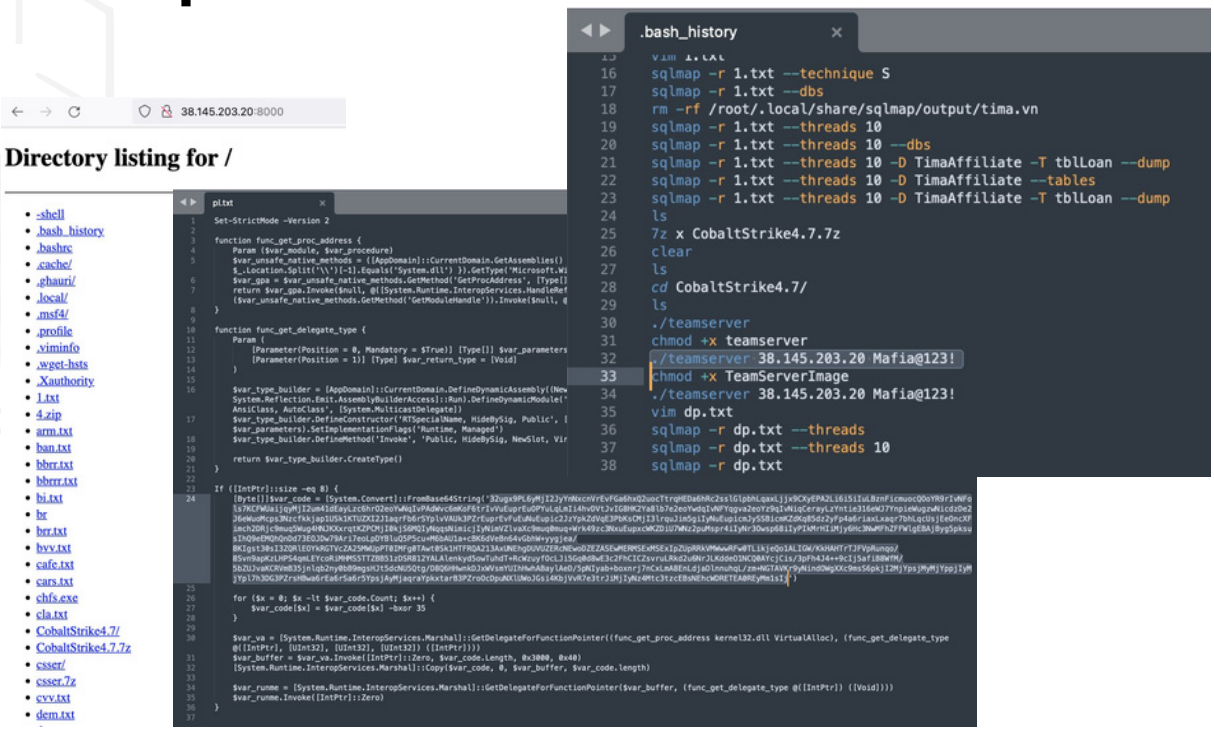


https://twitter.com/realScamSniffer/status/1695267174859100252

This advisory report highlights a significant financial loss incurred by a victim who fell victim to a malicious Blur bid in a Non-Fungible Token (NFT) auction. The victim lost 333 ETH as a result of signing the malicious bid. This report provides an overview of the incident, describes the impact, and offers recommendations to prevent similar incidents in the future.

The victim participated in an NFT auction and encountered a malicious bid associated with a Blur token. This malicious bid offered 333 ETH to a suspicious NFT address, 0x7624acf79dfa4691c8fe099ffd4c66c02e478936. As a result, the victim lost the equivalent of 333 ETH due to the interaction with the malicious bid.

Opendir



https://twitter.com/sicehice/status/1694542540563755127

This advisory report provides an overview of recent threat activity involving OpenDir hosting, the deployment of CobaltStrike, the use of malicious PowerShell, and the targeting of Indian and Spanish websites with SQLMap. The identified IP address, 38.145.203.20, has been associated with these malicious activities, indicating a potential cyber threat that requires immediate attention and mitigation efforts.

Threat Overview:

1. **OpenDir Hosting:** OpenDir hosting refers to the practice of hosting web directories with open permissions, often allowing unauthorized users to access and upload content. Threat actors can exploit such vulnerabilities to distribute malicious files or payloads.
2. **CobaltStrike:** CobaltStrike is a popular post-exploitation tool used by threat actors for advanced persistent threat (APT) campaigns. It provides capabilities for command and control (C2) communication, lateral movement, and data exfiltration.
3. **Malicious PowerShell:** PowerShell is a scripting language commonly used by administrators for automation. Threat actors abuse PowerShell to execute malicious code, bypass security measures, and achieve unauthorized access to systems.
4. **SQLMap:** SQLMap is an open-source penetration testing tool that automates the detection and exploitation of SQL injection vulnerabilities in web applications. It can be used by threat actors to compromise vulnerable websites and gain unauthorized access to databases.

Threat Details:

- **IP Address:** 38.145.203.20
- **Port Usage:** Port 8000 (OpenDir Hosting), Port 80 (CobaltStrike C2)
- **Affected Regions:** India, Spain

Threat Activity:

1. **OpenDir Hosting:** The IP address 38.145.203.20 is hosting directories with open permissions, potentially facilitating the distribution of malicious files. Organizations are advised to investigate and secure these directories to prevent unauthorized access.
2. **CobaltStrike C2:** The IP address is also operating a CobaltStrike command and control server on port 80. CobaltStrike is known for its use in APT campaigns and can indicate the presence of advanced threat actors within an organization's network.
3. **Malicious PowerShell:** Threat actors may leverage PowerShell to execute malicious scripts and achieve various malicious objectives, such as privilege escalation, lateral movement, and data exfiltration.
4. **SQLMap Targeting:** The threat actor is targeting websites in India and Spain using SQLMap, suggesting an attempt to exploit SQL injection vulnerabilities for unauthorized access and data compromise.

1Day

This advisory report highlights critical vulnerabilities associated with Juniper Junos OS, specifically CVE-2023-3684, CVE-2023-3685, CVE-2023-3686, and CVE-2023-3687. These vulnerabilities have the potential to lead to remote code execution (RCE) attacks. This report provides details about the vulnerabilities, affected systems, potential risks, and recommended mitigation steps.

A Proof of Concept for chaining the CVEs [CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, CVE-2023-36847] developed by @watchTowr to achieve Remote Code Execution in Juniper JunOS within SRX and EX Series products.

Networking hardware company Juniper Networks recently issued an "out-of-cycle" security update to address multiple vulnerabilities present in the J-Web component of Junos OS. These vulnerabilities have the potential to be exploited together, allowing attackers to achieve remote code execution on vulnerable installations.

The combined vulnerabilities have earned a cumulative Common Vulnerability Scoring System (CVSS) rating of 9.8, indicating their critical severity. These flaws impact all versions of Junos OS on SRX and EX Series.

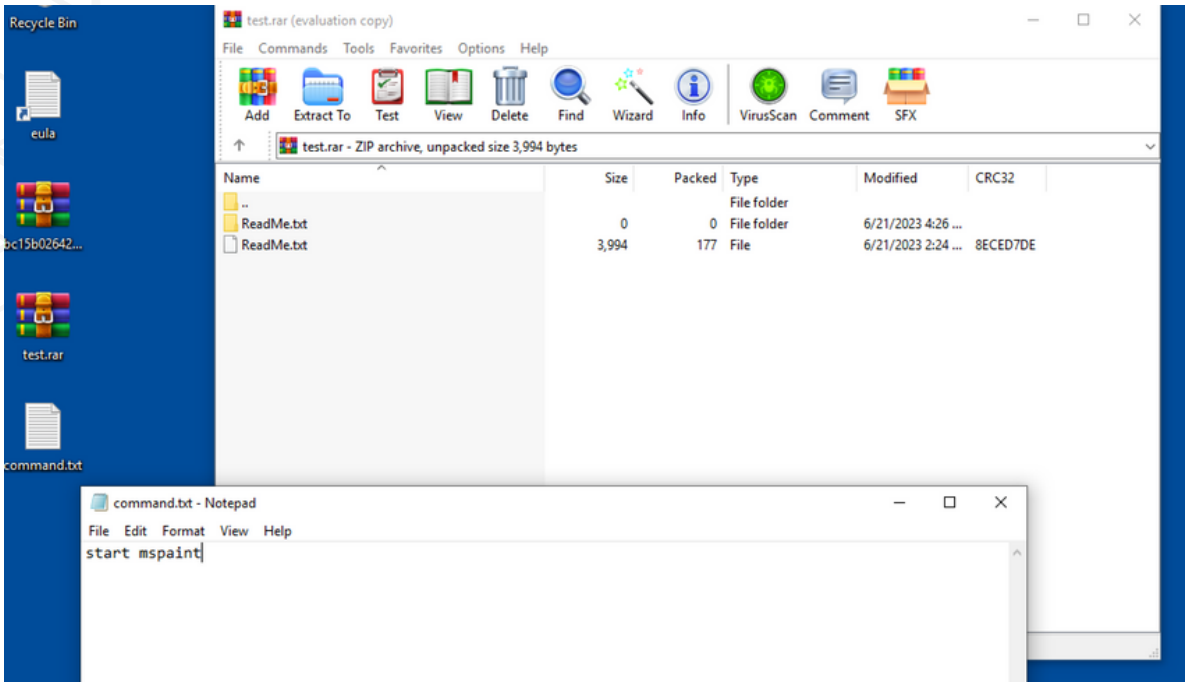
According to the advisory released on August 17, 2023, Juniper Networks warned that "an unauthenticated, network-based attacker may be able to remotely execute code on the devices" by chaining the exploitation of these vulnerabilities.

The J-Web interface is utilized for configuring, managing, and monitoring Junos OS devices. The vulnerabilities are outlined as follows:

1. CVE-2023-36844 and CVE-2023-36845 (CVSS scores: 5.3): Two vulnerabilities related to PHP external variable modification within J-Web of Juniper Networks Junos OS on EX Series and SRX Series. These allow an unauthenticated attacker on the network to control specific essential environment variables.
2. CVE-2023-36846 and CVE-2023-36847 (CVSS scores: 5.3): Two vulnerabilities involve missing authentications for critical functions in Juniper Networks Junos OS on EX Series and SRX Series. An unauthenticated network-based attacker could potentially cause limited impact on the integrity of the file system.

The potential exploit involves an attacker sending a carefully crafted request to modify certain PHP environment variables or upload arbitrary files via the J-Web interface, all without requiring any form of authentication.
The vulnerabilities have been addressed in various versions of Junos OS for both the EX Series and SRX Series. Users are highly recommended to apply the necessary updates to mitigate potential threats of remote code execution. Additionally, Juniper Networks suggests two mitigation approaches: users can either disable J-Web altogether or restrict access to the interface only from trusted hosts.

🌶️ Trending Exploit



https://github.com/BoredHackerBlog/winrar_CVE-2023-38831_lazy_poc

The repository's title is "winrar_CVE-2023-38831_lazy_poc." It's hosted on GitHub, a platform used for version control and collaboration on software development projects. The repository appears to contain resources related to the CVE-2023-38831 vulnerability in WinRAR.

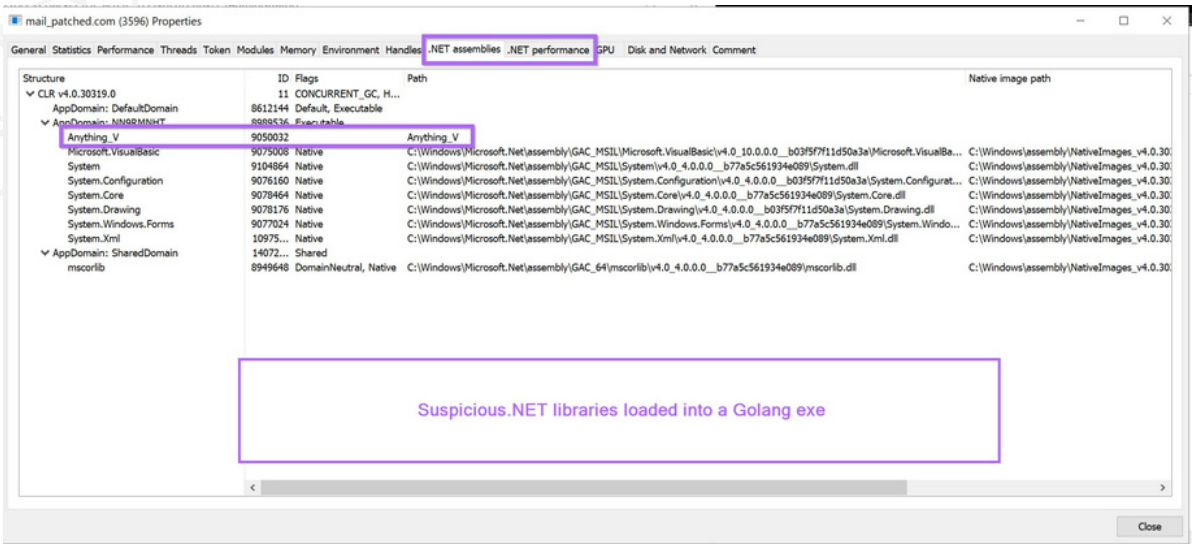
Purpose: The main purpose of this repository seems to be to showcase a "lazy" way to create a malicious WinRAR file that exploits the CVE-2023-38831 vulnerability. The repository provides instructions and resources for replicating this PoC.

Contents: The repository contains a set of files and folders, including a README.md file that provides detailed information about the vulnerability, the PoC, and how to use it for testing purposes. It also contains a compressed RAR file named "test.rar" that can be used to test the PoC. The README file likely guides users on how to use and understand these resources.

Motivation: The motivation behind creating and sharing such a PoC could vary. Some security researchers create PoCs to demonstrate the importance of addressing specific vulnerabilities and to encourage prompt patching by software vendors. However, the term "lazy" in the repository's description suggests that the approach might not be comprehensive or optimized for ethical purposes.

Other exploit:
https://github.com/b1tg/CVE-2023-38831-winrar-exploit

The Topic of the Week :)



https://twitter.com/embee_research/status/1694635899903152619

This report provides an in-depth analysis of a complex malware sample and demonstrates the dynamic extraction of an Xworm payload from a bloated Golang file. The analysis was conducted in collaboration with Huntress Labs, utilizing tools such as Procmon, Process Hacker, Entropy Analysis, Debloating, and debuggers. The objective was to uncover the payload, analyze its capabilities, and provide insights into the malware's behavior.

Analysis Steps and Findings:

1. File Download: The initial executable file is a massive 1.5GB in size and written in Golang. While Detect-it-easy recognized it as an executable, a string search hinted at its Golang origin.
2. Entropy Analysis: Entropy Analysis revealed that the file contained significant low-entropy junk. Hexdumping confirmed a large block of null bytes.
3. Debloating: The null bytes were manually removed with a hex editor, which is time-consuming for such a large file. Alternatively, the "pe-debloat" tool by @SquiblydooBlog was employed, reducing the file size to 960KB.
4. Dynamic Analysis: Due to the complexity of Golang files, a dynamic analysis approach was chosen. The file was executed and monitored using Procmon.
5. Persistence and Suspicious Libraries: Procmon unveiled the creation of a scheduled task for persistence, along with the loading of libraries related to .NET and CLR.
6. NET Assemblies: Process Hacker confirmed that the running Golang file loaded .NET assemblies into memory, one of which raised suspicions.
7. Dnspy and Source Code Inspection: Dnspy was attached to the Golang file, allowing inspection of the source code of the loaded .NET modules. By listing the .NET modules, "anything_v" stood out.
8. Keylogging and Enumeration: The "anything_v" module contained code suggesting keylogging and enumeration capabilities of the target computer.
9. Configuration Decryption: By jumping to the entry point of "anything_v," an encrypted configuration was revealed. It also showed the capability to create Windows Defender exclusions.
10. Dynamically Decoding Configuration: By setting a breakpoint on the decryption function and using a watch window, the decrypted configuration content was obtained from memory.
11. Xworm Malware: The decrypted configuration strongly indicated that the initial bloated file served as a loader for the Xworm Malware.
12. Creating New Detections: The extracted information, including schtasks, config folders, executed commands, and C2 info, can be leveraged to create new detections. Suggestions include identifying .com files in scheduled tasks, detecting bloated .com files (>200MB), and monitoring .com files running from %appdata%.

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.