Threat Intel Roundup: QakBot, Ignition, RICHIESTA DI PAGAMENTO

Week in Overview(28 Aug-5 Sep)

Technical Summary

Apache Ignition Unauthenticated Remote Code Execution Vulnerability

- **CVE Identifier:** Not Authorized
- **Vulnerability Type:** Unauthenticated Remote Code Execution (RCE)
- **Description:** This unauthenticated RCE vulnerability impacts Apache Ignition, allowing attackers to execute arbitrary code without prior authorization. Specific version details and mitigation measures are unavailable due to the lack of authorized information.
- **Mitigation:** Organizations are advised to keep Apache Ignition up to date, enforce access controls, segment networks, monitor for suspicious activity, and educate users.

CVE-2023-37895 Apache Jackrabbit RMI #RCE

- **CVE Identifier:** CVE-2023-37895
- **Vulnerability Type:** Remote Code Execution (RCE)
- **Description:** CVE-2023-37895 is an RCE vulnerability affecting Apache Jackrabbit RMI. Attackers can execute arbitrary code remotely due to improper handling of objects during deserialization. A fix is available in authorized versions.
- **Mitigation:** Users are advised to upgrade to an authorized version of Apache Jackrabbit RMI to eliminate this vulnerability.

Exploitation of MinIO Storage System Vulnerabilities

- **Description:** Unauthorized actors are actively exploiting vulnerabilities in the MinIO storage system. These vulnerabilities may allow attackers to gain unauthorized access to sensitive data or disrupt operations. Organizations should apply authorized patches and secure their MinIO installations.

Phishing Campaign Targeting Italian Audience - RICHIESTA DI PAGAMENTO 04/09/2023

- **Description:** A phishing campaign, labeled "RICHIESTA DI PAGAMENTO 04/09/2023," is actively targeting an Italian audience. It employs deceptive tactics to trick recipients into revealing sensitive information or making payments. Users are cautioned to verify the authenticity of such emails before taking any action.

QakBot Takedown - Bot Connections to Active C2s

- **Description:** A recent takedown operation targeted the QakBot botnet by disrupting its command-and-control (C2) infrastructure. Law enforcement and cybersecurity experts collaborated to sever bot connections to active C2 servers, which could mitigate the threat posed by QakBot. Users are encouraged to stay vigilant for signs of QakBot infections and apply security measures.

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:

- QakBot Takedown
- Apache Ignition
- MinIO Mass Exploit
- Apache Jackrabbit

Cyber Threat Map

🚨 Vulnerability of the Week

Ignition

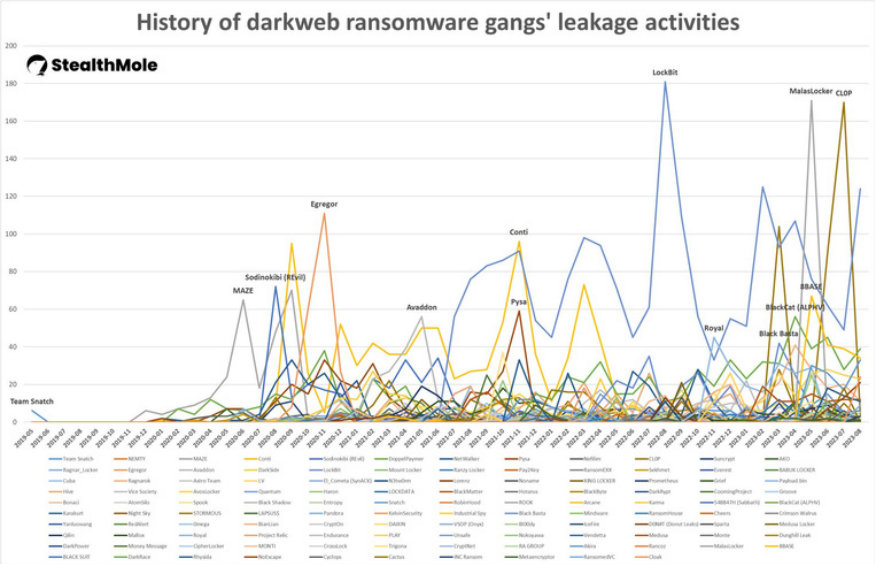
CVE-2023-39476

The exploit for this unauthenticated RCE vulnerability involves manipulating the Apache Ignition system through a complex series of steps. The attacker leverages an unauthorized deserialization point, potentially within JavaSerializationCodec. The exact mechanism and impact of the vulnerability depend on the unverified version of Apache Ignition in use.

https://xz.aliyun.com/t/12813

Due to the lack of authorized information about this vulnerability, it is challenging to provide specific mitigation steps. However, organizations using Apache Ignition should consider the following general security practices:

⛳ Leakage Insight



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

In the past, ransomware attacks primarily involved encrypting victims' data and demanding a ransom in exchange for decryption keys. However, in 2019, a notable change occurred in the tactics employed by ransomware gangs. These groups began stealing sensitive data from their victims before encrypting it and then threatening to leak this data on the dark web if a ransom was not paid. This shift represented a significant escalation in the capabilities and intentions of ransomware actors.

The Trend of Data Theft and Leakage:

1. **2019 - The Catalyst:**
   - In 2019, the first known instances of data-stealing ransomware attacks were reported. These attacks involved exfiltrating sensitive data before encrypting it.
   - The attackers typically demanded a ransom for the decryption key and threatened to publicly release the stolen data if the ransom was not paid.
2. **Growing Number of Victims:**
   - As the initial perpetrators continued their activities, other ransomware gangs adopted similar tactics.
   - The threat of data exposure added immense pressure on victims to comply with ransom demands.
3. Emergence of New Ransomware Gangs:
   - Over time, new ransomware gangs specializing in data theft and leakage emerged.
   - These groups refined their techniques and targeted a wide range of organizations, including healthcare, finance, and critical infrastructure.
4. Evolving Tactics:
   - Ransomware gangs evolved their methods, employing advanced social engineering, spear-phishing, and supply chain attacks to gain access to victims' networks.
   - They often targeted vulnerabilities in remote desktop protocols (RDP) and exploited weaknesses in network security.

Malware Distribution Sites

Bundled Files (2) ⓘ

	Scanned	Detections	File type	Name
^	2023-09-04	13 / 54	Windows shortcut	screens013923.zip/wdocx.lnk
	SHA-256	0c319f2f8753d469fcc5e731ad525e6bc2af89cc41135b2185ccbd180afe3b96		
	Date Bundled	2023-09-02 20:32:32		
	File Size	2.02 KB		
^	?	?	PNG	screens013923.zip/Screenshot_3.png
	SHA-256	d4a3ece77ec42a480fa5fd5c40f0be4c9124420a07d95458ca581c765797adbf		
	Date Bundled	2023-09-02 23:22:36		
	File Size	27.41 KB		

Decoded Text

{"BeaconType": ["HTTP"], "Port": 80, "SleepTime": 45000, "MaxGetSize": 2801745, "Jitter": 37, "C2Server": "185.225.75.63,/bootstrap.min.js", "HttpPostUri": "/bootstraped.pws", "Malleable_C2_Instructions": ["Remove 1522 bytes from the end", "Remove 84 bytes from the beginning", "Remove 3931 bytes from the beginning", "Base64 URL-safe decode", "XOR mask w/ random key"], "HttpGet_Verb": "GET", "HttpPost_Verb": "POST", "HttpPostChunk": 0, "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe", "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe", "CryptoScheme": 0, "Proxy_Behavior": "Use IE settings", "Watermark": 987654321, "bStageCleanup": "True", "bCFGCaution": "False", "KillDate": 0, "bProcInject_StartRWX": "False", "bProcInject_UseRWX": "False", "bProcInject_MinAllocSize": 17500, "ProcInject_PrependAppend_x86": ["kJA=", "Empty"], "ProcInject_PrependAppend_x64": ["kJA=", "Empty"], "ProcInject_Execute": ["ntdll:RtlUserThreadStart", "CreateThread", "NtQueueApcThread-s", "CreateRemoteThread", "RtlCreateUserThread"], "ProcInject_AllocationMethod": "NtMapViewOfSection", "bUsesCookies": "True", "HostHeader": ""}

https://twitter.com/malwrhunterteam/status/1698752629558432231

This advisory report outlines several suspicious files, namely "screens013923.zip," "wdocx.lnk," "screenshot_1.lnk," and a potentially malicious IP address "185.225.75[.]63." These elements have been identified as potential security concerns, warranting immediate attention and investigation.

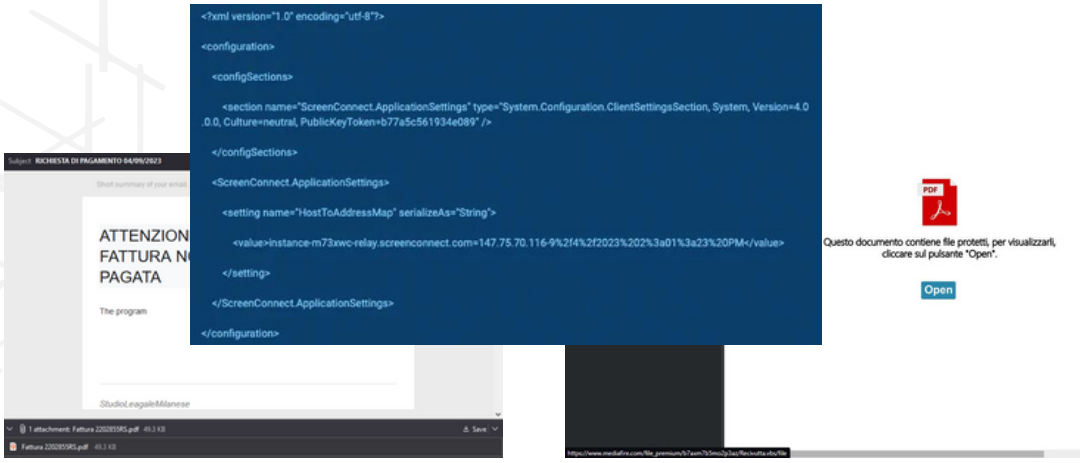
Incident Details:

1. **"screens013923.zip" File:**
   - **File Hash:** 3592100c259832c5fa236b03b96039cc44a558f5958b3ce449e6b217adb09f7c
2. The file "screens013923.zip" is flagged as suspicious due to its file hash. ZIP files can be used to conceal malware, and their contents should be carefully analyzed before extraction.
3. **"wdocx.lnk" / "screenshot_1.lnk" Files:**
   - **File Hash:** 0c319f2f8753d469fcc5e731ad525e6bc2af89cc41135b2185ccbd180afe3b96
4. The files "wdocx.lnk" and "screenshot_1.lnk" are also marked as suspicious based on their file hash. LNK files can be used to launch malicious scripts or executables and should be investigated further.
5. **IP Address:**
   - **IP Address:** 185.225.75[.]63

5. The IP address "185.225.75[.]63" is identified as potentially malicious. It may be associated with a command and control (C2) server, a source of malicious traffic, or other malicious activities. Investigating the purpose and origin of this IP address is crucial.

- **"/bootstraped.pws" File:**
- The file "/bootstraped.pws" is mentioned without additional context. Further investigation is needed to determine the nature and purpose of this file.

Proxylife



https://twitter.com/0xToxin/status/1698972467555889532

This advisory report highlights a phishing campaign that specifically targets the Italian audience, masquerading as "RICHIESTA DI PAGAMENTO 04/09/2023." The campaign involves malicious registry activity, malicious URLs, and an intricate execution chain leading to the delivery of malware. The report aims to raise awareness and provide recommendations for mitigating this threat.

Campaign Overview:

The phishing campaign titled "RICHIESTA DI PAGAMENTO 04/09/2023" is designed to deceive recipients into downloading and executing malicious files, ultimately compromising their systems. This campaign poses a significant threat to Italian users.

Registry Activity:

Malicious registry modifications have been observed as part of this campaign, including the addition and deletion of registry keys. These actions are indicative of attempts to maintain persistence and execute malicious code.

Malicious URLs:

Several malicious URLs have been identified as part of this campaign:

1. **https://www.mediafire[.]com/file_premium/b7axm7b5mo2p3az/Recivutta.vbs/file**
2. **https://247info[.]click/ofertaprezi.pdf**
3. **https://247info[.]click/hgsuhfs.jbb**
4. **https://t[.]ly/IddaZ (https://www.dropbox[.]com/scl/fi/q7koxcyug90zcutj2dwsh/simple.ghf?rlkey=1qi40k7ozkrev1govodhdxv8i&dl=1)**
5. **https://247info[.]click/DocRecevutta.exe**

MalwareBazaar and AnyRun:

MalwareBazaar and AnyRun provide additional information and analysis of this campaign's artifacts, including execution chains and associated behaviors:

- MalwareBazaar Analysis
- AnyRun Analysis 1
- AnyRun Analysis 2

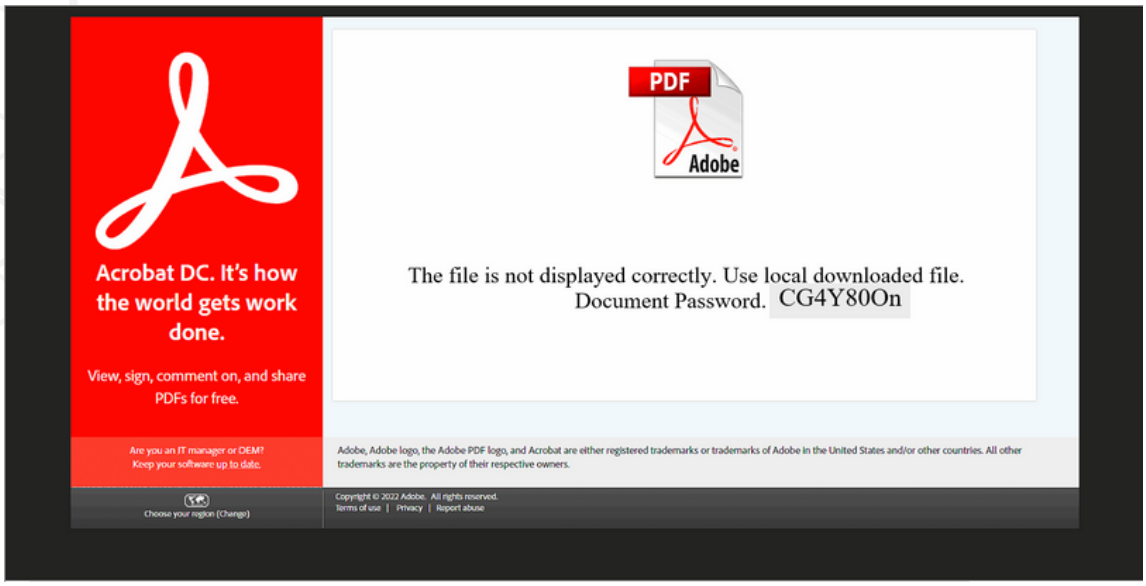
Execution Chain:

The execution chain involves a series of file types, including .eml, .pdf, .vbs, .exe, .msi, and a potential UAC bypass using **fodhelper.exe**. This complex chain is designed to evade detection and compromise the victim's system.

Command and Control (C2):

The identified C2 server, **instance-m73xwc-relay.screenconnect[.]com**, is used for command and control purposes. C2 servers are often instrumental in the execution of malicious activities.

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.

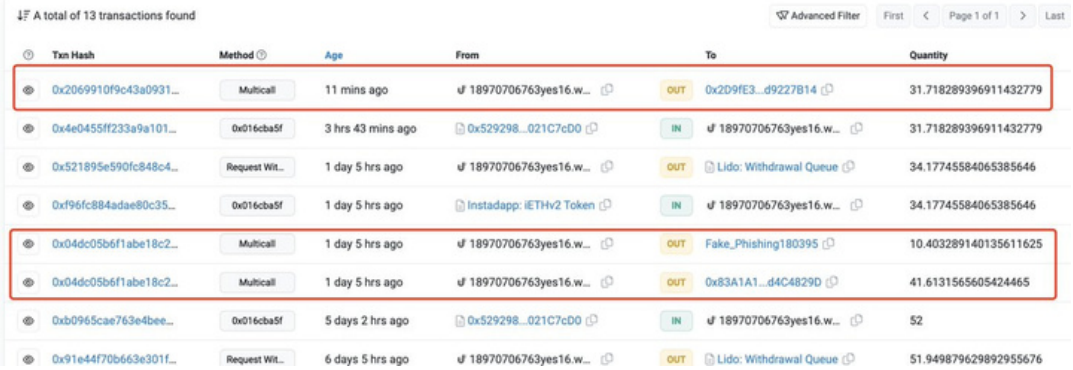
Discovery and Lateral Movement: The threat actor conducted Active Directory discovery using AdFind, archived results, and performed nslookup across the network.

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



A total of 13 transactions found

Advanced Filter | First | Page 1 of 1 | Last

Txn Hash	Method	Age	From		To	Quantity
0x2069910f9c43a0931...	Multicall	11 mins ago	18970706763yes16.w...	OUT	0x2D9fE3...d9227B14	31.718289396911432779
0x4e0455ff233a9a101...	0x016cba5f	3 hrs 43 mins ago	0x529298...021C7cD0	IN	18970706763yes16.w...	31.718289396911432779
0x521895e590fc848c4...	Request Wit...	1 day 5 hrs ago	18970706763yes16.w...	OUT	Lido: Withdrawal Queue	34.17745584065385646
0xf96fc884adae80c35...	0x016cba5f	1 day 5 hrs ago	Instadapp: iETHv2 Token	IN	18970706763yes16.w...	34.17745584065385646
0x04dc05b6f1abe18c2...	Multicall	1 day 5 hrs ago	18970706763yes16.w...	OUT	Fake_Phishing180395	10.403289140135611625
0x04dc05b6f1abe18c2...	Multicall	1 day 5 hrs ago	18970706763yes16.w...	OUT	0x83A1A1...d4C4829D	41.6131565605424465
0xb0965cae763e4bee...	0x016cba5f	5 days 2 hrs ago	0x529298...021C7cD0	IN	18970706763yes16.w...	52
0x91e44f70b663e301f...	Request Wit...	6 days 5 hrs ago	18970706763yes16.w...	OUT	Lido: Withdrawal Queue	51.949879629892955676

https://twitter.com/realScamSniffer/status/1698373110473589164

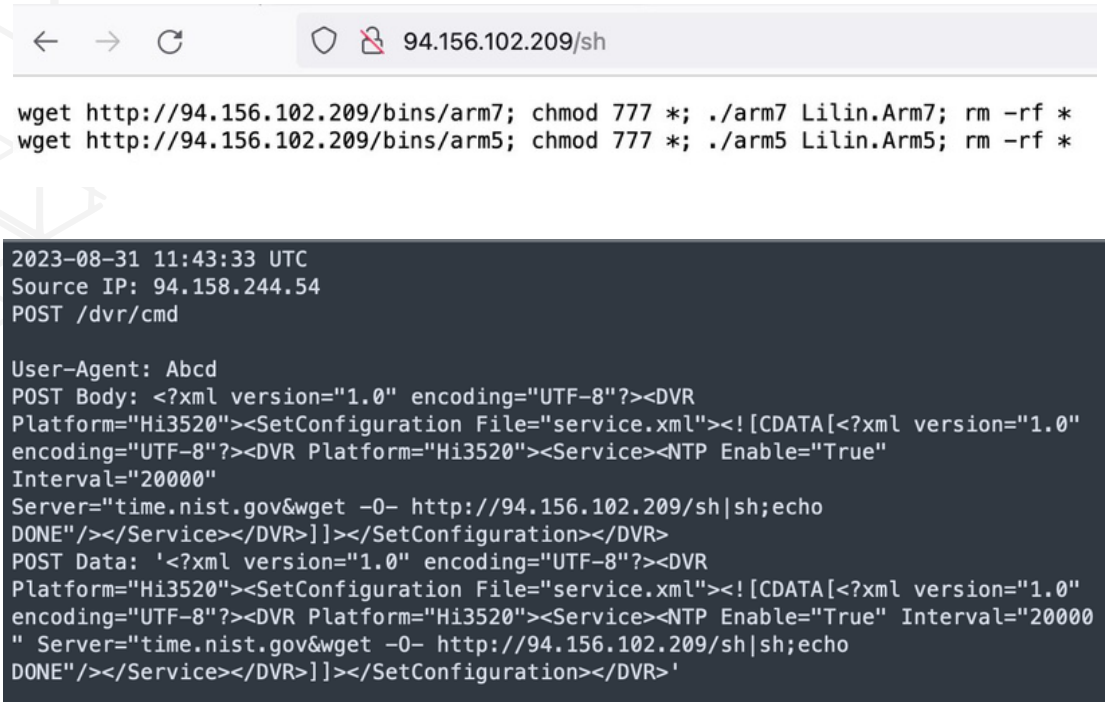
it was observed that a user fell victim to a phishing attack and subsequently lost a total of 83 $stETH (staked ETH) tokens. The user initially lost 52 $stETH and, inexplicably, transferred an additional 31 $stETH to the same wallet three hours later. Furthermore, the victim had also signed an "increaseAllowance" transaction, suggesting potential vulnerability to further exploitation.

Incident Details:

1. **Initial Loss of 52 $stETH:**
   a. The victim reported a loss of 52 $stETH tokens, indicating that they had fallen victim to a phishing attack. The exact circumstances surrounding the attack are currently under investigation.
2. **Subsequent Transfer of 31 $stETH:**
   a. Surprisingly, three hours after the initial loss, the victim transferred an additional 31 $stETH tokens to the same wallet. This raises concerns about the user's awareness of the ongoing threat and the security of their wallet.

3. **"increaseAllowance" Transaction:**
   - The victim's wallet records indicate that they signed an "increaseAllowance" transaction. This transaction is often used to increase the spending limit of a smart contract or wallet. The presence of such a transaction may indicate a compromised wallet or a lack of awareness about the transaction's implications.

📝 Opendir



https://twitter.com/sicehice/status/1697455299383247091

On August 31, 2023, a Remote Code Execution (RCE) attempt was detected targeting Lilin DVR (Digital Video Recorder) devices. The attack also involved the spreading of the Mirai malware. This advisory report provides an overview of the incident, including relevant Indicators of Compromise (IOCs) and hashes.

Incident Details:

1. **Attack Vector:**
2. The attackers initiated the attack by sending a POST request to **/dvr/cmd** from the source IP address 94.158.244.54. This indicates an attempt to execute a command on the targeted DVR devices.
3. **Command and Control (C2) Server:**
4. After compromising the DVR devices, the attackers established connections from ARM5 and ARM7 devices to the C2 server with the IP address 94.156.102.209 on port 7645. This C2 server was used to maintain control over the compromised devices.
5. **Indicators of Compromise (IOCs):**
   - **C2 Server:** hxxp://94.156.102.209/sh
   - **C2 Server IP:** 94.156.102.209
   - **Source IP:** 94.158.244.54
6. **Hashes:**
7. The following hashes were associated with the incident and may be used to identify malicious files or processes:
   - **36c31d4ea8879149964e7e5e595d10c6**
   - **9b9f5b128cbb472d98d18e8d34f4ceca**
   - **f26a6aec2c4565da7744b6d80f77f262**

1Day

CVE-2023-37895 is a severe security vulnerability discovered in the Apache Jackrabbit RMI service. The vulnerability allows remote attackers to execute arbitrary code on affected systems, potentially leading to unauthorized access, data exfiltration, or complete compromise of the targeted system.

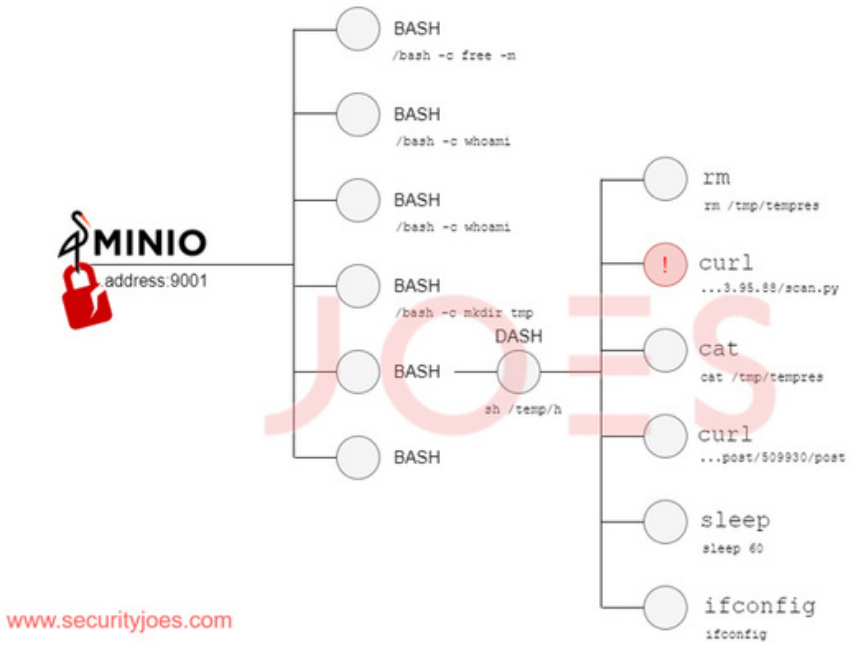
Exploitation Details:
The exploit for CVE-2023-37895 involves leveraging RMI over HTTP. The attacker targets the **org.apache.jackrabbit.servlet.remote.RemoteBindingServlet** component.

To exploit this vulnerability, the attacker follows a specific sequence of steps:

1. Utilizes **JcrUtils** to obtain a **Repository** object.
2. Specifies an HTTP URL, which results in obtaining a **URLRemoteRepository**.
3. Utilizes the **Repository** interface, which includes the **login** function, requiring **javax.jcr.Credentials** as a parameter.
4. Exploits two implementations of the **javax.jcr.Credentials** interface, particularly **SimpleCredentials**, which accepts a **<string, object>** type hashmap.
5. Serializes a payload and places it within the hashmap.
6. Constructs and sends the payload to exploit the vulnerability.

https://y4er.com/posts/cve-2023-37895-apache-jackrabbit-rmi-rce/

🌶️ Trending Exploit



https://thehackernews.com/2023/09/hackers-exploit-minio-storage-system.html

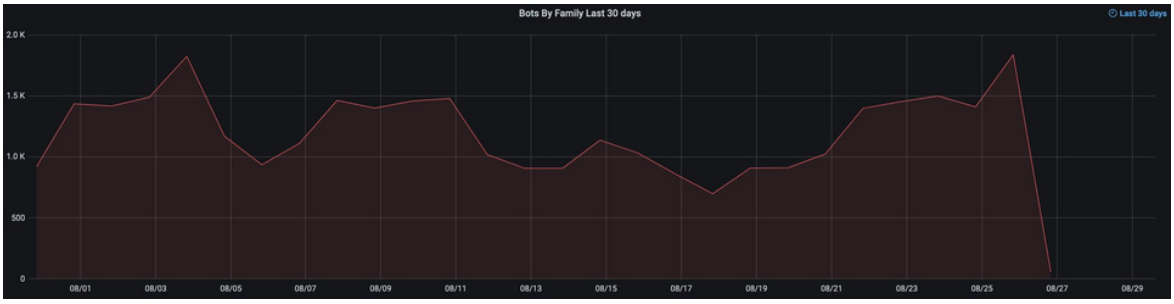
An unidentified threat actor has exploited vulnerabilities (CVE-2023-28432 and CVE-2023-28434) in the MinIO high-performance object storage system. These vulnerabilities pose a high risk and have been leveraged for unauthorized code execution on compromised servers. The incident has been reported by Security Joes, a cybersecurity and incident response firm.

Attack Details:
In the attack chain investigated by Security Joes, the threat actor used these vulnerabilities to gain admin credentials, followed by abuse of the compromised system's foothold. Specifically, the attacker replaced the legitimate MinIO binary with a malicious version through an update command specifying a MIRROR_URL. This malicious modification to the binary exposed an endpoint capable of receiving and executing commands via HTTP requests, effectively serving as a backdoor. These commands inherit the system permissions of the user initiating the application.

Furthermore, the altered binary closely resembles an exploit named "Evil MinIO," published on GitHub in early April 2023. However, there is currently no evidence linking the exploit's author to the threat actors behind this incident.

Threat Actor Proficiency:
The threat actor involved in this incident demonstrated proficiency in bash scripts and Python. Additionally, they utilized the backdoor access to deliver supplementary payloads from a remote server for post-exploitation via a downloader script. This script can target both Windows and Linux environments and assesses compromised hosts to determine whether execution should be terminated.

The Topic of the Week :)



https://twitter.com/teamcymru_S2/status/1696645523527123412

This report provides an overview of the Operation Duck Hunt takedown of the QakBot botnet, focusing on the perspective of bot (victim) connections to recently-polled active Command and Control servers (C2s). The operation commenced around 20:30 UTC on Friday evening, August 25. The report draws attention to significant developments and provides relevant resources for further analysis.

Background:
Operation Duck Hunt, targeting the QakBot botnet, represents a significant cybersecurity operation aimed at disrupting a well-known banking trojan and information-stealing malware. This operation involved the takedown of C2 infrastructure, thereby crippling the botnet's ability to communicate with its infected endpoints.

Incident Timeline:
- **Date and Time:** August 25, around 20:30 UTC.
- Operation Duck Hunt was initiated, leading to the disruption of the QakBot botnet's C2 infrastructure.

Key Observations:
- **Botnet Disruption:**
  - Operation Duck Hunt successfully disrupted the QakBot botnet's ability to communicate with its infected endpoints.
  - The takedown operation led to a significant reduction in malicious activities and potential harm to victims.
- **Protection for Victims:**
  - By targeting the C2 infrastructure, the operation aimed to protect the interests and sensitive data of victims affected by the QakBot botnet.
- **Resource for Analysis:**
  - Additional information and detailed analysis regarding Operation Duck Hunt and the QakBot botnet takedown can be found at the provided URL: Team Cymru - Malware and Botnet Analysis and Detection.
- **#BARS:**
  - The hashtag #BARS is included in the report, suggesting that it may be relevant to the incident. Further investigation or context may be required to understand its significance.

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.