Threat Intel Roundup: Aria, Anonymous Sudan, Qakbot, AI, UMBR

VMware Aria Flaw, Anonymous Sudan's Microsoft Breach, Qakbot Threat, AI Advancements, and UMBR Token Turmoil

Week in Overview[25 Jun- 2 July]

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

VMware Aria Operations for Logs Vulnerability (CVE-2023-20864): A critical vulnerability has been found in VMware Aria Operations for Logs, which could lead to remote code execution. Users are strongly advised to update their installations with the released security patches to protect their systems.

Remote Code Execution in Spring Cloud Function: Certain versions of Spring Cloud Function, including 3.1.6 and 3.2.2, are vulnerable to remote code execution when using routing functionality. Attackers can exploit this issue by providing a specially crafted SpEL as a routing-expression, potentially gaining access to local resources.

Qakbot "**obama270**" Variant Detection: A YARA rule has been created to identify the presence of specific strings related to the Qakbot variant known as "obama270." This rule checks for specific filenames, DLLs, directory creation, and a malicious URL associated with this variant.

ERC20 Approval Phishing Attack Leads to **$UMBR** Token Loss: An investor has suffered a significant loss of $1.08 million worth of $UMBR tokens due to falling victim to an ERC20 Approval phishing attack. This incident highlights the risks associated with phishing scams in the cryptocurrency domain.

Detection of **QuasarRAT** and RDP Brute Force Tools: An "opendir" hosting server has been found to contain QuasarRAT, a remote administration tool, and RDPbruteforcer, a tool used for brute-forcing Remote Desktop Protocol (RDP) credentials.

ManageEngine ADSelfService Plus Zero-Day Vulnerability: A critical zero-day vulnerability (CVE-2023-35719, CWE-288) has been discovered in ManageEngine ADSelfService Plus. Physical attackers can bypass authentication and execute arbitrary code. Immediate action, especially within a zero trust architecture, is crucial to mitigate the risk.

PowerShell Backend Remote Code Execution in Microsoft Exchange: A critical remote code execution vulnerability (CVE-2023-32031) has been identified in the PowerShell backend of Microsoft Exchange. Organizations using affected versions should take immediate steps to mitigate the potential impact.

Government Intelligence Agencies Exploit AI Facial Recognition: Intelligence agencies are utilizing AI-based facial recognition technology to track a suspected Russian individual. This application aims to identify faces from various sources, aiding in estimating origins and tracking criminal activities.

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:

- **VMware Aria Operations for Logs Vulnerability**
- **Addressing QuasarRAT and RDP Brute Force Tools**
- **Securing PowerShell Backend in Microsoft Exchange**
- **Mitigating ERC20 Approval Phishing Attacks**
- **Qakbot "obama270" Variant Detection**

Vulnerabilities by Activity

CVE-2023-20864

A critical vulnerability (CVE-2023-20864) has been identified in VMware Aria Operations for Logs, potentially leading to remote code execution. This vulnerability could be exploited by attackers to compromise the integrity and confidentiality of affected systems. VMware has released security patches to address this issue, and it is strongly recommended that all users of VMware Aria Operations for Logs update their installations immediately to ensure the security of their systems.

The vulnerability, identified as CVE-2023-20864, allows an attacker to execute arbitrary code remotely in VMware Aria Operations for Logs. By exploiting this vulnerability, an attacker can gain unauthorized access to the affected systems, compromising their security and potentially leading to data theft, unauthorized system modifications, or other malicious activities.

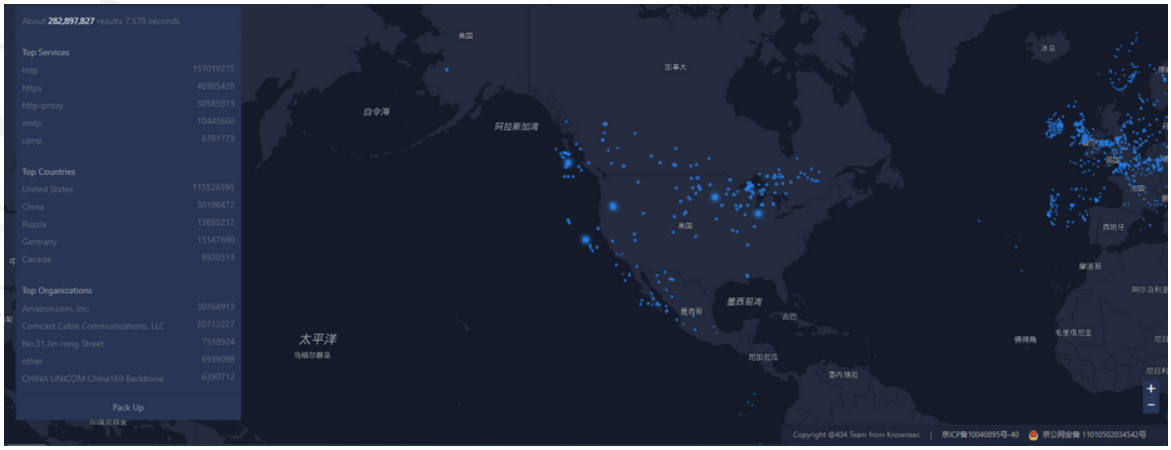
Risk Level: Critical

Recommended Actions:

- Update VMware Aria Operations for Logs: Immediately apply the latest security patches provided by VMware to address the vulnerability. These patches contain fixes for the vulnerability and will help protect your system from potential attacks.
- Disable Remote Access: If remote access is not required for the proper functioning of VMware Aria Operations for Logs, it is advisable to disable it to reduce the attack surface and mitigate the risk of exploitation.
- Implement Network Segmentation: Implement network segmentation to isolate critical systems from potential threats. This can help contain the impact of a potential attack and limit the spread of malicious activities within your network.
- Monitor for Indicators of Compromise (IoCs): Stay vigilant and monitor your systems for any signs of suspicious activities or potential exploitation attempts. Regularly review logs, network traffic, and system behavior to identify any anomalies that could indicate a compromise.
- Keep Software and Systems Updated: Ensure that all software, including operating systems and applications, are regularly updated with the latest security patches. This practice helps protect against known vulnerabilities and reduces the risk of exploitation.
- Educate Users: Raise awareness among your employees or users about the importance of cybersecurity best practices. Encourage them to exercise caution when opening email attachments, visiting unfamiliar websites, or clicking on suspicious links.

Ref.VMware Aria Operations for

CVE-2022-22963



Security Eye Query Result

In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.

To address the CVE-2017-12629 vulnerability, which involves remote code execution in Apache Solr, the following remediation and mitigation steps can be taken:

Update to a Patched Version: Upgrade your Spring Cloud Function to a version that includes the patch for CVE-2022-22963. Versions 3.1.7 and 3.2.3, or any subsequent releases, should contain the fix for this vulnerability.

Disable Routing Functionality (If Not Required): If your application does not require the routing functionality provided by Spring Cloud Function, consider disabling it altogether. By doing so, you can eliminate the risk associated with this specific vulnerability.

Validate and Sanitize User Input: If your application allows users to provide SpEL expressions for routing, ensure that all user-supplied input is thoroughly validated and sanitized. Implement strict input validation checks to prevent any malicious code from being executed.

Use Whitelisting Approach: If possible, use a whitelist approach to restrict the allowed SpEL expressions to a predefined set of safe expressions. This way, you can limit the potential impact of any malicious inputs.

With the continuous migration of business to the cloud, the number of network security incidents and threats on public cloud platforms remains high. Domestic key industries, including but not limited to my country's scientific research institutions, large enterprises, governments and institutions, have become the key targets of attackers: a total of 156 attack sources.

✅ Here's a YARA rule for detecting the mentioned scenario:

```
rule CloudPlatformThreat {
  strings:
    $url1 = "http://51.81.133.90/qweasd"
    $url2 = "http://51.81.133.90/NWWW.6"
    $url3 = "http://14.1.98.226:8880/ff.elf"
    $url4 = "http://14.1.98.226:8880/7z"
    $ipv4 = "51.81.133.90"
    $file_hash1 = "b9bcb150c1449dcc6a69ff1916a115ce"
    $file_hash2 = "8c47779d3ad0e925461b4fbf7d3a139d"
    $file_hash3 = "392f13b090f54438b3212005226e5d52"
    $hostname1 = "oracle.zzhreceive.top"
    $hostname2 = "bbq.zzhreceive.top"

  condition:
    any of ($url1, $url2, $url3, $url4, $ipv4, $file_hash1, $file_hash2, $file_hash3, $hostname1, $hostname2) or
    (any of them for 3 or more)
}
```

CVE-2022-29144

This vulnerability has been identified in Microsoft Edge which could allow a malicious user to potentially enable the escalation of privileges via remote access. How it can be Exploited The privilege escalation vulnerability exists in Microsoft Edge (Chromium-based) because the vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed, up to and including the entire Internet.

Remediation and Mitigation for CVE-2022-29144:
Apply Security Update: Check for and apply the latest security update provided by Microsoft for Microsoft Edge (Chromium-based). Ensure that you have installed the patch or update that addresses the vulnerability associated with CVE-2022-29144.

Keep Software Up to Date: Regularly update Microsoft Edge (Chromium-based) to the latest version available. This helps ensure that you have the latest security enhancements and patches implemented.

Enable Automatic Updates: Enable automatic updates for Microsoft Edge (Chromium-based) to receive security updates and patches as soon as they are released. This ensures that your browser stays protected against known vulnerabilities.

Use Secure Browsing Practices: Exercise caution when visiting unfamiliar or suspicious websites. Be wary of clicking on links or downloading files from untrusted sources, as they may exploit vulnerabilities in the browser.

Use Firewall and Antivirus Software: Install and regularly update reputable firewall and antivirus software on your system. These security solutions can help detect and block potential threats targeting Microsoft Edge and other applications.

CVE-2023-2008

A flaw was found in the Linux kernel's udmabuf device driver. The specific flaw exists within a fault handler. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an array. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel.

Remediation and Mitigation for CVE-2023-2008:
Apply the patch: Check for official patches or updates provided by the Linux distribution or vendor. Apply the latest kernel updates that address the vulnerability. These patches usually include fixes for known security vulnerabilities, including CVE-2023-2008.

Implement least privilege: Configure your systems to run with the least privileges necessary. Restrict root access and limit access permissions for users and processes to minimize the potential impact of an attacker escalating privileges.

Enable kernel hardening features: Take advantage of kernel hardening features such as Address Space Layout Randomization (ASLR), Stack Protector (SSP), and Kernel Address Space Layout Randomization (KASLR). These features can make it more difficult for attackers to exploit vulnerabilities and execute arbitrary code.

Enable SELinux or AppArmor: Enable and properly configure security modules like SELinux (Security-Enhanced Linux) or AppArmor to enforce strict access control policies. These security frameworks can restrict the actions and permissions of processes, including the kernel, and help mitigate the impact of an exploitation attempt.

CVE-2023-3447

The Active Directory Integration / LDAP Integration plugin for WordPress is vulnerable to LDAP Injection in versions up to, and including, 4.1.5. This is due to insufficient escaping on the supplied username value. This makes it possible for unauthenticated malicious users to extract potentially sensitive information from the LDAP directory.

Remediation and Mitigation for CVE-2023-3447:
Update the plugin: If you are using the Active Directory Integration / LDAP Integration plugin for WordPress, upgrade to version 4.1.6 or newer. The plugin vendor may have released a patch or fix to address the vulnerability. Applying the latest update will help mitigate the risk.

Disable or remove the vulnerable plugin: If upgrading to a patched version is not possible or feasible, consider disabling or removing the plugin from your WordPress installation. This will eliminate the risk of exploitation through the vulnerable plugin altogether.

Implement input validation and sanitization: Review the plugin's code and ensure that the supplied username value is properly escaped and sanitized before being used in LDAP queries. Implement input validation to prevent the injection of malicious LDAP queries.

Apply principle of least privilege: Restrict the permissions and access levels for LDAP queries to only what is necessary for the plugin to function correctly. Limit the privileges of the LDAP account used by the plugin to minimize the potential impact of an attack.

Leakage Insight

AnonymousSudan Official Channel

We would like to bring to your attention an announcement made by an entity claiming to have successfully hacked Microsoft and obtained unauthorized access to a significant database containing more than 30 million Microsoft accounts, including email addresses and passwords. The entity is offering to sell this alleged database for a price of 50,000 USD. We strongly advise caution and skepticism regarding these claims, as unauthorized access and selling of personal data are illegal activities.

An announcement has been made by an entity named "#AnonymousSudan," claiming to have hacked Microsoft and obtained unauthorized access to a substantial database containing millions of Microsoft accounts, email addresses, and passwords. They are promoting the sale of this database for a price of 50,000 USD. It is crucial to note that these claims have not been verified, and Microsoft has denied any breach or compromise of their systems.

Action Required:

- Do Not Engage: It is strongly recommended that individuals and organizations refrain from engaging with or contacting the provided bot (@AnonymousSudan_Bot) to negotiate or inquire about the alleged database. Participating in or supporting illegal activities such as unauthorized access and data breaches can have severe legal and ethical consequences.
- Maintain Strong Security Practices: Regardless of the validity of the claims, it is essential to ensure the security of your systems and data. Follow best practices for cybersecurity, including using strong, unique passwords, enabling multi-factor authentication, regularly updating software, and monitoring for any signs of unauthorized access or suspicious activity.
- Report Suspicious Activity: If you come across any information or evidence related to this alleged breach or any unauthorized access to Microsoft accounts, promptly report it to Microsoft's security team or the appropriate law enforcement agencies in your jurisdiction. Provide detailed information, including any communication or evidence related to the claims.
- Educate and Raise Awareness: Increase awareness among employees and users about the importance of maintaining strong security practices, recognizing phishing attempts, and protecting sensitive information. Encourage them to report any suspicious activity or potential security incidents promptly.

DDos Insight

It has come to our attention that there is a recommendation to block all traffic originating from the IP range 109.205.213.0/24. Although there is some discrepancy in geolocation data, it is advised to exercise caution and consider blocking traffic from this IP range due to potential security concerns. While the physical location of hosts associated with this netblock is reported to be in the United States, it is essential to note that geolocation vendors may have varying data. Implementing this block can help mitigate potential risks and protect your network infrastructure.

The IP range 109.205.213.0/24 has been associated with security concerns, and it is advisable to drop all traffic originating from this range. While there are discrepancies in geolocation data, with some vendors indicating locations such as Azerbaijan ( ) or the United Kingdom ( ), it is reported that hosts within this netblock are physically located in the United States ( ). Due to the potential security implications, it is recommended to block traffic from this IP range to minimize the risk of potential attacks or unauthorized access attempts.

Affected IP Range: 109.205.213.0/24

Risk Level: Moderate to High

Recommended Actions:

- Implement Network Firewall Rules: Configure your network firewall to drop all traffic originating from the IP range 109.205.213.0/24. Consult your network administrator or IT team to ensure proper implementation and adherence to your organization's security policies.
- Monitor Network Traffic: Continuously monitor your network traffic for any signs of suspicious activity or attempts to access your systems from the specified IP range. Implement appropriate intrusion detection and prevention systems to enhance your network's security posture.
- Stay Informed: Keep up to date with the latest information regarding this IP range and any associated security concerns. Monitor security advisories from trusted sources to ensure that you have the most accurate and up-to-date information about potential risks.
- Report Suspicious Activity: If you observe any unusual or suspicious activity originating from the IP range 109.205.213.0/24, promptly report it to your organization's IT security team or the appropriate authorities. Provide detailed information about the activity and any relevant logs to assist in the investigation.
- Verify Geolocation Data: While there are discrepancies in geolocation data associated with this IP range, consider verifying the physical location of hosts within your own network or with reliable geolocation providers. This can provide additional insight into the potential risks associated with traffic from this range.

https://twitter.com/bad_packets/status/1673867561715355651

Proxylife

We want to alert you to a potential security threat related to the distribution of malware known as Qakbot. The threat actors behind this campaign are utilizing an obfuscation technique involving the use of various file formats and scripting commands to deliver and execute malicious code. It is important to be aware of these techniques and take necessary precautions to protect your systems and data.

The malicious activity associated with Qakbot involves a multi-stage process, as described below:

- File Manipulation: A file named "obama270.pdf" is being manipulated by converting it into a .zip file, then further obfuscated into a .js file, and finally transformed into a .dll file.
- Execution of JavaScript: The "RrwuR.js" script is executed using the Windows Script Host (wscript). This script likely contains malicious instructions or code to facilitate further malicious activities.
- Powershell Command: A powershell command is used to download a file from the URL "https://viltare.]com/Pll6qXoN.dat" and store it locally.
- Creation of Directory: A new directory named "C:\ProgramData\SNWSPinna" is created on the affected system.
- File Download: The downloaded file from the previous step is saved as "Pinna.dll" in the newly created directory.
- Execution of Malicious DLL: The rundll32 command is used to execute the malicious "Pinna.dll" file from the newly created directory.

Detection Rule:

```
rule Qakbot_Obama270 {
meta:
description = "Detects Qakbot variant obfuscated as obama270"
author = "OpenAI"
reference = "https://raw.githubusercontent.com/pr0xylife/Qakbot/main/Qakbot_obama270_21.06.2023.txt"
strings:
$pdf = "obama270.pdf"
$js = "RrwuR.js"
$dll = "Pinna.dll"
$directory = "C:\ProgramData\SNWSPinna\"
$url = "https://viltare.]com/Pll6qXoN.dat"
condition:
all of ($pdf, $js, $dll, $directory, $url)
}
```

https://github.com/pr0xylife/Qakbot/blob/main/Qakbot_obama270_21.06.2023.txt

This YARA rule checks for the presence of specific strings related to the Qakbot variant described as "obama270". It looks for the filenames "obama270.pdf" (the initial file), "RrwuR.js" (the JavaScript script), "Pinna.dll" (the malicious DLL), the creation of the directory "C:\ProgramData\SNWSPinna", and the URL "https://viltare.]com/Pll6qXoN.dat" from which a file is downloaded.

We would like to bring to your attention the existence of a server at IP address 78.47.123.155, which appears to host a collection of potentially malicious tools and utilities. The presence of these tools, including those related to password recovery, remote access, and network scanning, raises concerns regarding the intentions and activities of the server's operator. It is crucial to exercise caution and refrain from engaging with or accessing any content originating from this server.

The server located at IP address 78.47.123.155 is reported to contain a variety of tools and utilities that may have malicious intent. The following notable items have been identified:

1. shell.ps1: This script claims to recover passwords used by Veeam to connect to remote hosts (such as vSphere, Hyper-V, etc.), but its usage for "academic purposes" raises suspicion.
2. 000.msi: This file appears to install an Atera RMM agent, with the IntegratorLogin set as "juliuslbrch@hotmail.com". The true purpose and implications of this agent remain unclear.
3. anydesk.bat: This batch file creates a user named "Defender-Update" with the password "defen2!AWlW@1". It enables RDP (Remote Desktop Protocol), downloads and installs another Atera agent, and assigns the password "Anym4gSxbBaL". These actions indicate potential unauthorized access attempts.
4. klink24.bat: This batch file downloads klink.exe (plink), a tool commonly used for SSH connections, and uses it to establish RDP through a reverse SSH tunnel. Such techniques can be indicative of unauthorized or stealthy network access.

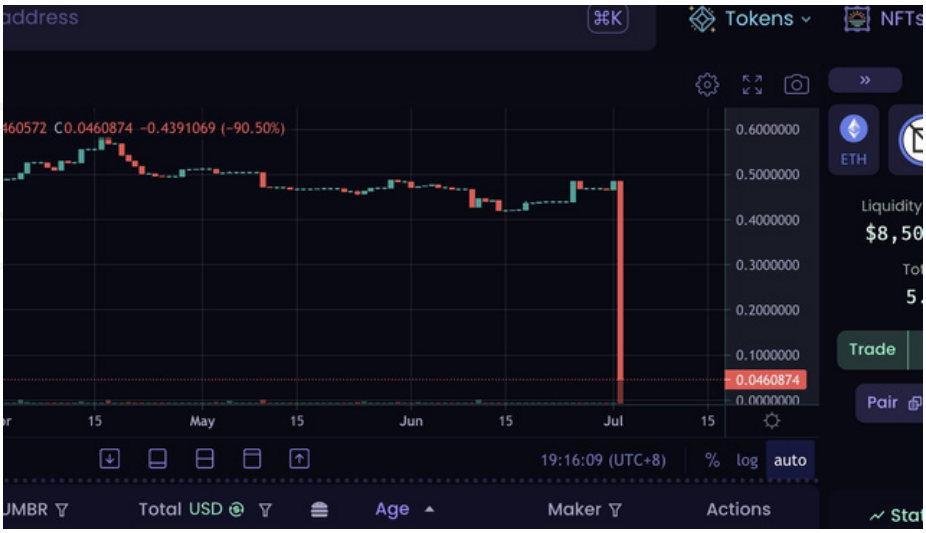
Additionally, it has been reported that the server contains utilities such as WinRAR, Mimikatz, Lazagne, and previously hosted "netscanold.exe" (SoftPerfect Network Scanner). These tools raise concerns about potential unauthorized network reconnaissance and data extraction.
https://twitter.com/1ZRR4H/status/1674672356013268993

_ APT Analysis

Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

https://www.trellix.com/en-us/advanced-research-center/threat-reports/jun-2023.html

Scam Contract



ERC20 Approval

In a shocking incident, an unsuspecting investor fell victim to an ERC20 Approval phishing attack, resulting in the loss of a staggering $1.08 million worth of $UMBR tokens. The attack highlights the risks associated with phishing scams and the importance of staying vigilant in the cryptocurrency ecosystem.

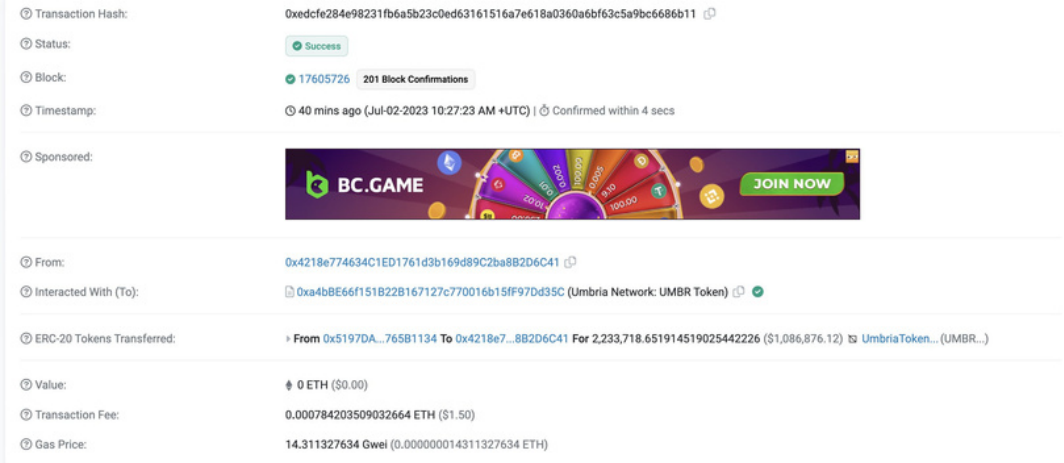
The victim, whose identity remains undisclosed, reportedly received a seemingly legitimate email urging them to approve an ERC20 token contract called $UMBR. Falling prey to the sophisticated phishing attempt, the investor unknowingly authorized the transfer of a substantial amount of $UMBR tokens to the attacker's address.

As news of the incident broke, the market reacted swiftly, causing a significant drop in the value of $UMBR tokens. Within minutes, the price plummeted by a staggering 90%, leaving investors in disbelief and exacerbating the financial impact of the attack.

Authorities are actively investigating the incident, and cybersecurity experts are urging crypto enthusiasts to exercise caution when receiving unsolicited emails or approving token contracts. It serves as a stark reminder that vigilance and adherence to best security practices are paramount when engaging in the ever-evolving world of digital assets.

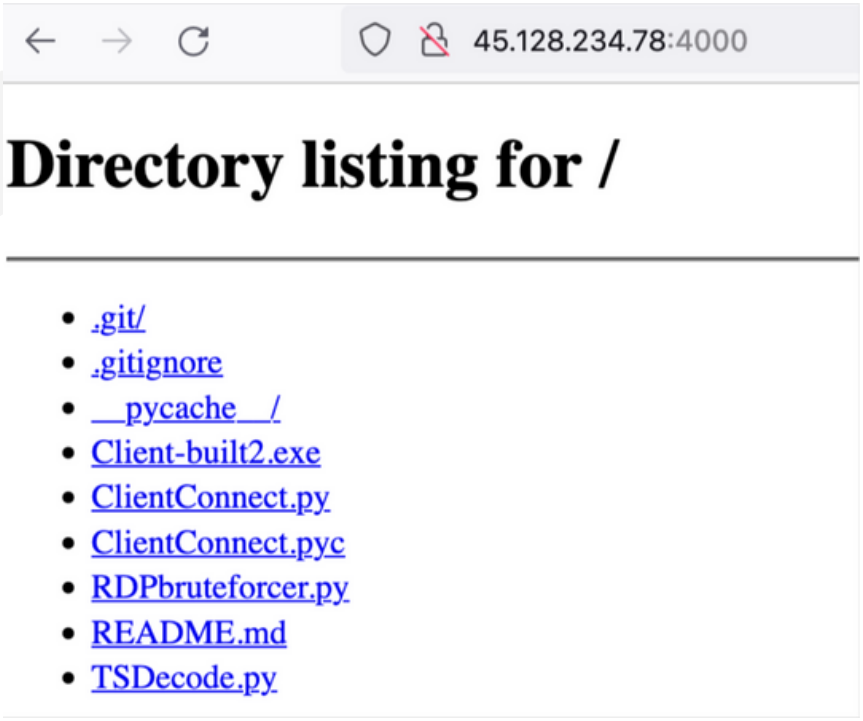
The incident serves as a stark wake-up call for the entire cryptocurrency community, highlighting the urgent need for increased security measures, improved user education, and more robust authentication protocols to combat phishing attacks and protect investors' funds.

https://twitter.com/realScamSniffer/status/1675464090343583746



Transaction Detail

Opendir



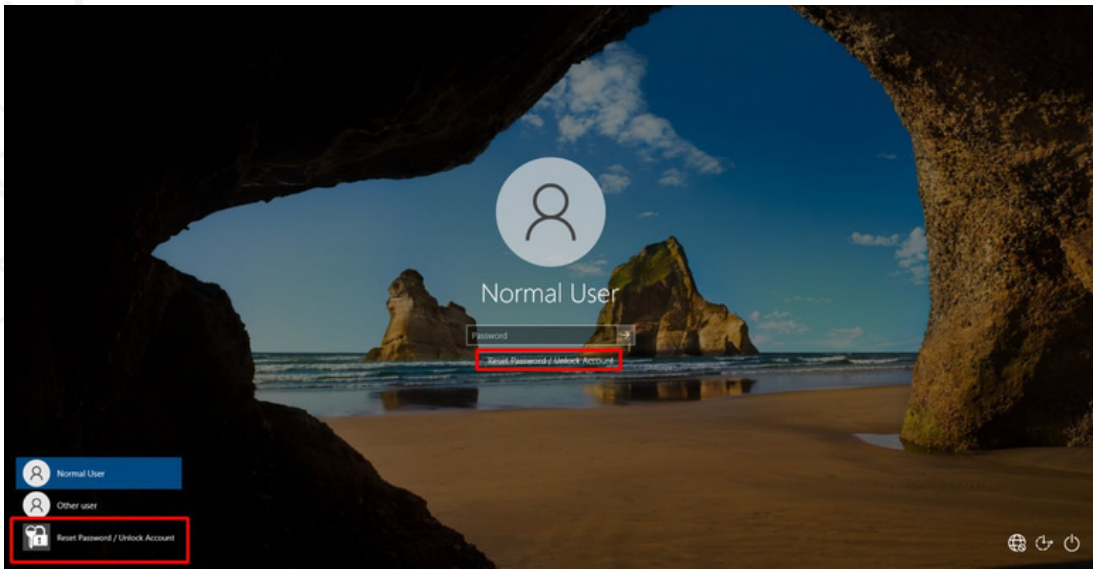
Directory Listing of 45.128.234.78:4000

opendir hosting QuasarRAT and RDP bruteforce tools
RDPbruteforcer

45.128.234[.]78:4000
C2: 213.181.206[.]70:4782

```
rule detect_opendir_quasarrat {
strings:
$opendir = "opendir"
$quasarrat = "QuasarRAT"
$rdp_bruteforce = "RDPbruteforcer"
$ip1 = "45.128.234.78"
$ip2 = "213.181.206.70"
condition:
any of ($opendir, $quasarrat, $rdp_bruteforce) and
any of ($ip1, $ip2)
}
```

0Day



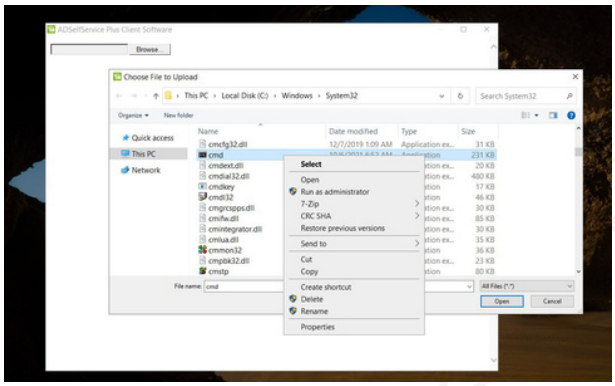
Logon Reset Password

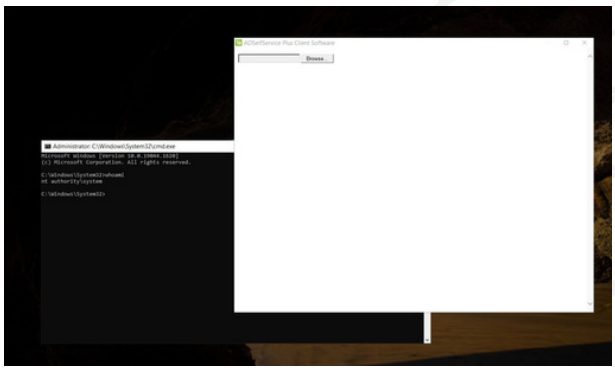
We have discovered a critical zero-day vulnerability (CVE-2023-35719, CWE-288) in ManageEngine ADSelfService Plus, an enterprise password management and self-service reset solution. This vulnerability allows physically present attackers to bypass authentication and execute arbitrary code on affected installations. It is important to take immediate action to mitigate the risk posed by this vulnerability, especially when utilizing a zero trust architecture.

Vulnerability Details: The vulnerability (CVE-2023-35719) resides in the Password Reset Portal used by the GINA (Graphical Identification and Authentication) client. It stems from the inadequate verification of data authenticity received via HTTP, enabling attackers to bypass authentication and execute code within the privileged SYSTEM context.

Exploitation of this vulnerability does not require any prior authentication, allowing physically present attackers to gain unauthorized access to the affected systems. The vulnerability has been confirmed to exist in ManageEngine ADSelfService Plus versions as early as 4.2.9, released in 2012, up to the latest version 6.3 Build 6301 at the time of writing (2023-06-23).

Risk Implications: Successful exploitation of this vulnerability can lead to unauthorized access, arbitrary code execution, and potential compromise of sensitive data within the affected ManageEngine ADSelfService Plus installations. The potential impact can be severe, and immediate action is necessary to mitigate the risk.





Exec cmd

Old school method for run cmd from logon

Recommended Actions:

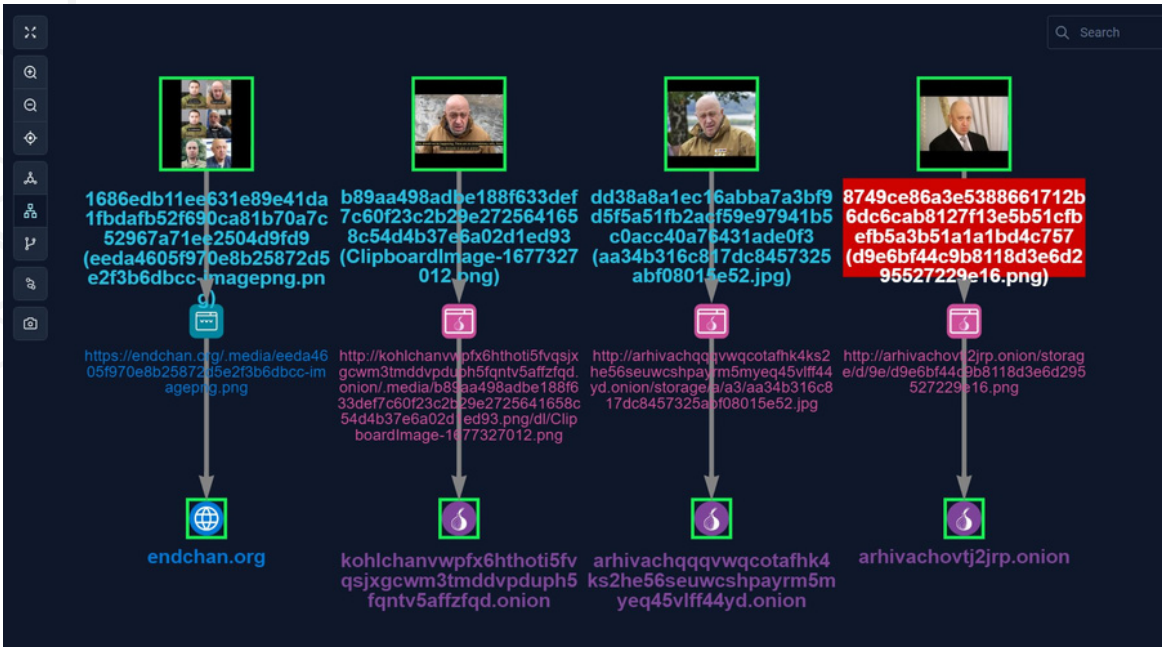
1. Apply Vendor Patch: It is crucial to promptly apply the official patch provided by ManageEngine to address the identified vulnerability. Keep track of security advisories and updates from the vendor and follow their recommended mitigation steps.
2. Zero Trust Architecture: In a zero trust architecture, assume that all network resources are untrusted and continuously verify and authenticate all users, devices, and data interactions. Implement strict access controls, network segmentation, and multi-factor authentication (MFA) to minimize the potential impact of any vulnerabilities.
3. Network Segmentation and Isolation: Separate critical systems from the rest of the network through proper network segmentation. Implement strict firewall rules to restrict unnecessary network traffic and isolate sensitive systems from potential attackers.
4. Threat Monitoring and Detection: Deploy robust security monitoring solutions that can detect and alert on any unauthorized access attempts or suspicious activities related to ManageEngine ADSelfService Plus. Continuously monitor network traffic, log files, and system activities for any signs of compromise.
5. Employee Awareness: Educate employees about the potential risks associated with this vulnerability and the importance of adhering to security best practices. Advise them to report any unusual or suspicious activities to the IT security team promptly.

Trending Exploit

A critical remote code execution vulnerability has been discovered in the PowerShell backend of Microsoft Exchange (CVE-2023-32031). This vulnerability poses a significant risk to organizations utilizing affected versions of Microsoft Exchange. It is crucial to take immediate action to mitigate the potential impact.

https://github.com/testanull/ProxyNotShell-PoC/tree/main

The Topic of the Week



Fusion Intelligence Center Prigozhin

Government Intelligence Agencies Exploit AI Facial Recognition for Tracking Suspected Russian Individual

In a startling revelation, it has come to light that multiple government intelligence agencies are utilizing advanced AI-based facial recognition technology to track the movements and whereabouts of a Russian individual. This cutting-edge technology is being employed in the ongoing efforts to combat international crime and enhance global security.

The undisclosed Russian individual, believed to be involved in illicit activities, has caught the attention of intelligence agencies worldwide. Leveraging the power of AI, these agencies are actively mining various sources, including the dark web, deep web, Telegram, and other hidden platforms, to extract images that may provide valuable leads.

By employing sophisticated algorithms and machine learning, the facial recognition technology is capable of analyzing vast amounts of data and identifying matches or similarities among faces. This enables intelligence agencies to narrow down potential locations and estimate the origins of individuals connected to the targeted Russian figure.

The application of AI-based facial recognition in law enforcement and intelligence operations has gained traction in recent years. Its ability to rapidly process massive datasets and identify patterns has proven instrumental in tracking and apprehending criminals across borders.

However, the utilization of such technology also raises concerns related to privacy and potential misuse. Critics argue that the widespread use of facial recognition systems by government agencies could infringe upon individual rights and lead to unwarranted surveillance.
As the debate surrounding the ethics and regulation of facial recognition technology continues, it remains imperative for authorities to strike a balance between public safety and protecting individual privacy rights. Transparency and accountability in the use of these technologies are crucial to maintain public trust and mitigate potential abuses.

While the specific details of the ongoing operation remain undisclosed, it is clear that governments are increasingly harnessing the power of AI and machine learning to strengthen their intelligence capabilities. As technology continues to advance, the impact of these efforts on global security and the protection of individual freedoms will undoubtedly be a topic of ongoing discussion and scrutiny.

https://twitter.com/stealthmole_int/status/1674675793119825921

cat /etc/HADESS

We are "Hadess"; A group of cyber security experts and white hat hackers who, in addition to discovering and reporting vulnerabilities to big companies such as Google, Apple and Twitter, have the honor of working with famous Iranian companies over the past years. Ayman Burhan Rehiaft Azarakhsh Cyber Security Company provides its customers with integrated solutions in the field of cyber security, with a deep insight and understanding of the software development process as well as the development infrastructure.

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.