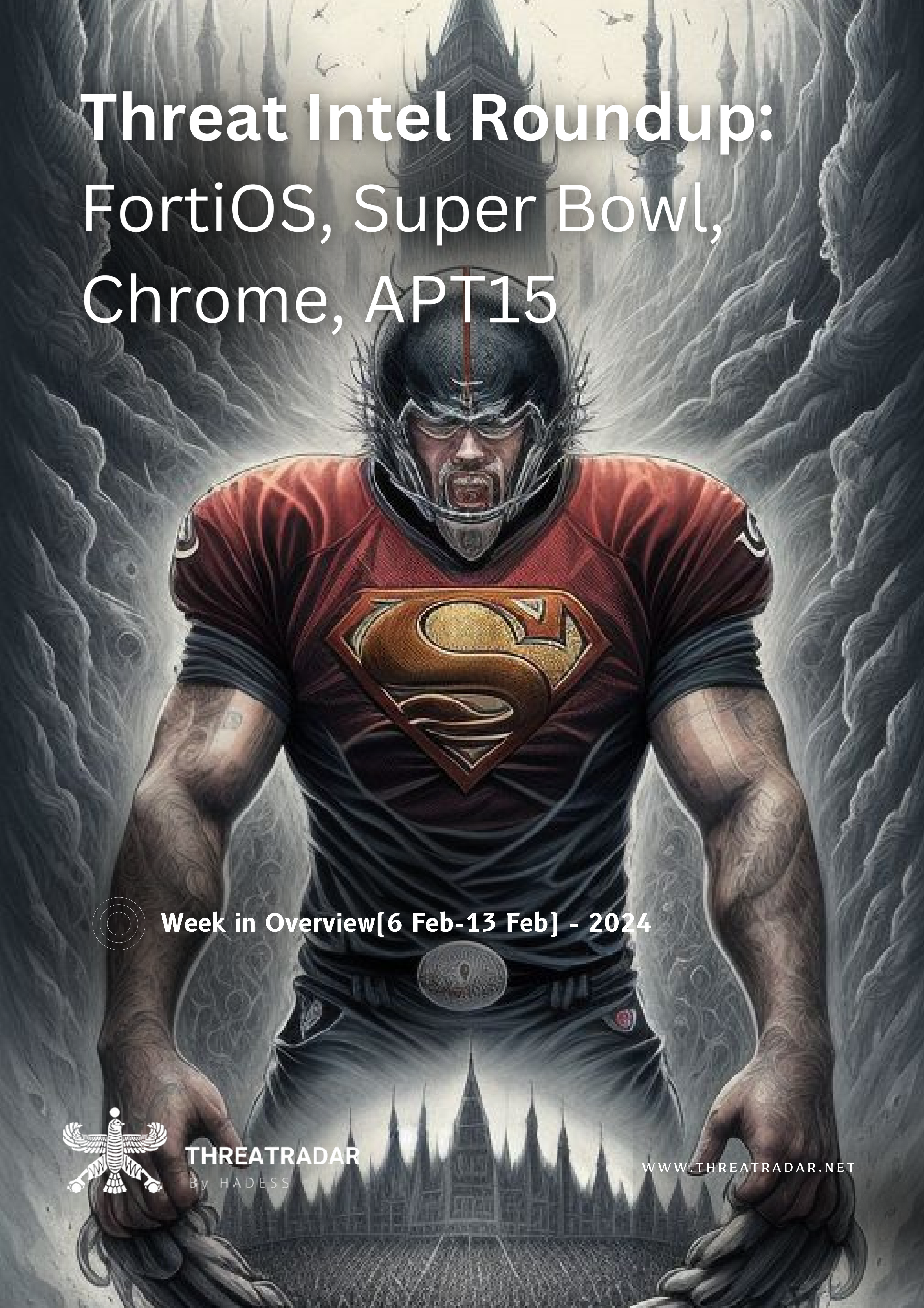
Threat Intel Roundup: FortiOS, Super Bowl, Chrome, APT15



Week in Overview[6 Feb-13 Feb] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

Technical Summary: Chinese APT Groups Exploiting SOHO Facilities for Cyberespionage
Chinese Advanced Persistent Threat (APT) groups, particularly APT15 (Vixen Panda, Ke3chang) and APT31 (Zirconium, Judgment Panda), have been identified as exploiting Small Office/Home Office (SOHO) facilities for cyberespionage operations, primarily targeting government and political institutions. These groups leverage compromised SOHO devices, such as routers, to create sophisticated obfuscation networks, making detection of their activities challenging. Recent incidents, including the compromise of the Federal Agency for Cartography and Geodesy (BKG) in Germany, highlight the severity of these attacks. Preventive measures, such as updating and replacing outdated devices, are recommended to mitigate the risks associated with these Chinese cyber actors.

Technical Summary: CrowdStrike Super Bowl Ad Campaign: "Riding with CrowdStrike"
CrowdStrike launched a high-impact ad campaign during the Super Bowl, titled "Riding with CrowdStrike," to raise awareness about modern cybersecurity threats. The campaign emphasizes CrowdStrike's commitment to securing the future against relentless adversaries. Through dynamic visuals and a powerful narrative, the ad showcases CrowdStrike's proactive approach to cybersecurity and its role as a trusted ally in safeguarding organizations and individuals from cyberattacks.

Technical Summary: Exploring Malware Obfuscation Techniques
Malware authors employ various obfuscation techniques to evade detection and analysis by cybersecurity researchers. This series explores modern methods used by malware obfuscators, such as .NET Reactor and SmartAssembly, to modify malware code and hinder analysis. Techniques include proxy functions, character breakdown, numeric conversion, heavy math operations, and Control Flow Graph (CFG) obfuscation. The series aims to demystify deobfuscation techniques and provide insights for both beginners and experienced malware analysts.

Technical Summary: Raspberry Robin Malware Advances with New Exploits
The Raspberry Robin malware has evolved with two new one-day exploits, CVE-2023-36802 and CVE-2023-29360, to escalate privileges on compromised devices. This Windows worm, discovered by security experts, infects networks via infected USB drives and gains access through msiexec.exe, installing malicious DLL files. The malware employs sophisticated techniques, including utilizing Discord for distribution and leveraging exploits targeting CVE vulnerabilities, to evade detection and elevate privileges on compromised devices.

Technical Summary: CVE-2024-22024 Exploitation Attempts
CVE-2024-22024 is a vulnerability exploited by threat actors, primarily targeting the '/dana-na/auth/saml-sso.cgi' endpoint in Ivanti Connect Secure. Exploitation attempts have been observed, indicating a potential threat to organizations using Ivanti products. The vulnerability allows remote attackers to execute arbitrary code or commands, highlighting the importance of applying security patches and implementing mitigations to prevent exploitation.

Technical Summary: CVE-2023-5996
CVE-2023-5996 is a use-after-free vulnerability discovered in Chrome's WebAudio component, exploited by threat actors to execute arbitrary code. The vulnerability allows attackers to trigger audio rendering threads in closed AudioContext instances, leading to unauthorized code execution. Users are advised to update their Chrome browsers to patched versions to mitigate the risk of exploitation.

Technical Summary: CVE-2024-21762
CVE-2024-21762 is an out-of-bounds write vulnerability identified in FortiOS, potentially allowing remote unauthenticated attackers to execute arbitrary code or commands. The vulnerability affects multiple versions of FortiOS, and users are advised to upgrade to patched versions to address the issue and mitigate the risk of exploitation.

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:

- Chinese APT Groups Exploiting SOHO Facilities for Cyberespionage
- CrowdStrike Super Bowl Ad Campaign: "Riding with CrowdStrike"
- Exploring Malware Obfuscation Techniques
- Raspberry Robin Malware Advances with New Exploits
- CVE-2024-22024 Exploitation Attempts
- CVE-2023-5996
- CVE-2024-21762

🚨 Vulnerability of the Week

FortiOS CVE-2024-21762

Advisory ID: FG-IR-24-015
Date: February 8, 2024
Severity: Critical
CVE ID: CVE-2024-21762
CVSSv3 Score: 9.6
IR Number: FG-IR-24-015

Summary: A critical vulnerability has been discovered in FortiOS, specifically in the sslvpnd component, which could allow remote attackers to execute arbitrary code or commands via specially crafted HTTP requests. This vulnerability stems from an out-of-bounds write issue [CWE-787]. It is crucial to address this vulnerability promptly to prevent potential exploitation by malicious actors. It has been noted that this vulnerability is potentially being exploited in the wild.
Impact: Successful exploitation of this vulnerability could result in unauthorized execution of arbitrary code or commands on affected systems, leading to potential compromise of confidentiality, integrity, and availability of data and services.

Affected Versions and Solutions:

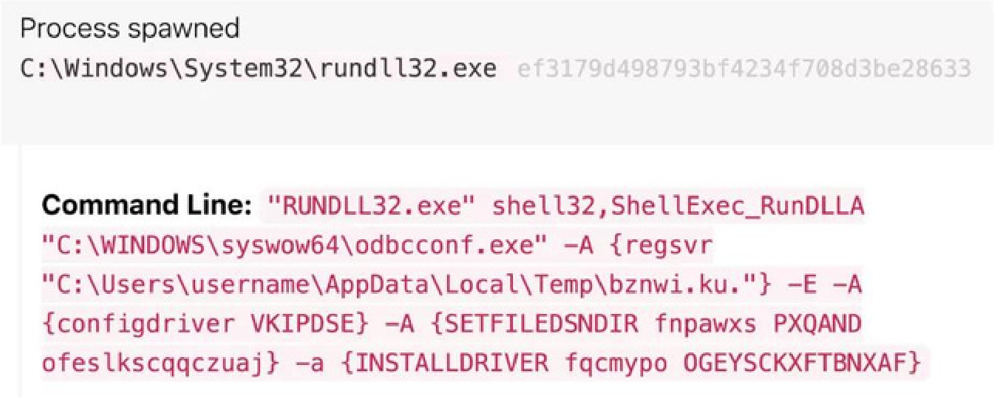
- FortiOS 7.6: Not affected (Not Applicable)
- FortiOS 7.4: Upgrade affected versions (7.4.0 through 7.4.2) to version 7.4.3 or above.
- FortiOS 7.2: Upgrade affected versions (7.2.0 through 7.2.6) to version 7.2.7 or above.
- FortiOS 7.0: Upgrade affected versions (7.0.0 through 7.0.13) to version 7.0.14 or above.
- FortiOS 6.4: Upgrade affected versions (6.4.0 through 6.4.14) to version 6.4.15 or above.
- FortiOS 6.2: Upgrade affected versions (6.2.0 through 6.2.15) to version 6.2.16 or above.
- FortiOS 6.0: Migrate to a fixed release. All versions are affected.
- FortiProxy 7.4: Upgrade affected versions (7.4.0 through 7.4.2) to version 7.4.3 or above.
- FortiProxy 7.2: Upgrade affected versions (7.2.0 through 7.2.8) to version 7.2.9 or above.
- FortiProxy 7.0: Upgrade affected versions (7.0.0 through 7.0.14) to version 7.0.15 or above.
- FortiProxy 2.0: Upgrade affected versions (2.0.0 through 2.0.13) to version 2.0.14 or above.
- FortiProxy 1.2: Migrate to a fixed release. All versions are affected.
- FortiProxy 1.1: Migrate to a fixed release. All versions are affected.
- FortiProxy 1.0: Migrate to a fixed release. All versions are affected.

Workaround: Disabling SSL VPN is advised as a temporary workaround. Note that disabling webmode is not considered a valid workaround.

Recommendation: It is strongly recommended that all affected users apply the respective patches or upgrades as soon as possible to mitigate the risk associated with this vulnerability. Additionally, organizations should monitor their networks for any signs of unauthorized access or unusual activity.

https://twitter.com/Kostastsale/status/1755820455108182280

🥵 Malware or Ransomware



```
Process spawned
C:\Windows\System32\rundll32.exe  ef3179d498793bf4234f708d3be28633
```

Command Line:
```
"RUNDLL32.exe" shell32,ShellExec_RunDLLA
"C:\WINDOWS\syswow64\odbcconf.exe" -A {regsvr
"C:\Users\username\AppData\Local\Temp\bznwi.ku."} -E -A
{configdriver VKIPDSE} -A {SETFILEDSNDIR fnpawxs PXQAND
ofeslkscqqczuaj} -a {INSTALLDRIVER fqcmypo OGEYSCKXFTBNXAF}
```

https://twitter.com/socradar/status/1757070881833029799

Raspberry Robin, a Windows worm malware first discovered in 2021, has evolved with increased sophistication and now incorporates two new one-day exploits: CVE-2023-36802 and CVE-2023-29360. These exploits enable the malware to escalate privileges on compromised devices, posing significant risks to affected networks.

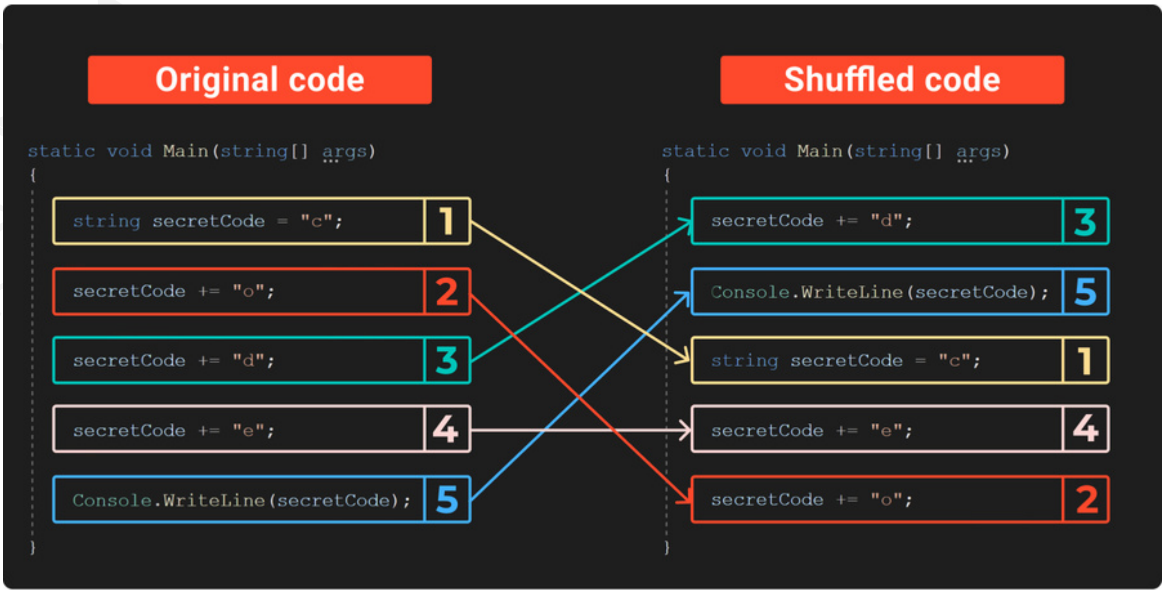
Recent Developments:

- Hundreds of businesses' networks have already fallen victim to Raspberry Robin, indicating widespread impact.
- Raspberry Robin infiltrates systems through infected USB drives containing malicious .LNK files.
- Upon execution, the malware launches a msiexec.exe process to install malicious DLL files, subsequently establishing communication with command and control (C2) servers via short URLs.
- The malware leverages legitimate Windows utilities like fodhelper.exe and odbcconf.exe to execute and configure the malicious DLLs, enabling it to gain persistence and evade detection.
- Recent observations reveal that Raspberry Robin utilizes Discord to distribute malicious archive files, disguising them as legitimate Windows components.
- The malware now incorporates two new one-day exploits targeting CVE-2023-36802 and CVE-2023-29360, both Local Privilege Escalation (LPE) vulnerabilities in Microsoft Streaming Service Proxy.

Significance:

- The inclusion of new exploits signifies a significant advancement in Raspberry Robin's capabilities, potentially indicating collaboration with exploit sellers or direct involvement of malware authors in exploit development.
- Raspberry Robin continues to refine its features, enhance evasion techniques, and adapt communication methods to evade detection by security measures.

Art of Detection



Original code

```
static void Main(string[] args)
{
    string secretCode = "c";
    secretCode += "o";
    secretCode += "d";
    secretCode += "e";
    Console.WriteLine(secretCode);
}
```

Shuffled code

```
static void Main(string[] args)
{
    secretCode += "d";
    Console.WriteLine(secretCode);
    string secretCode = "c";
    secretCode += "e";
    secretCode += "o";
}
```

https://twitter.com/anyrun_app/status/1756975909402194428

A new series has commenced, delving into the complex realm of malware obfuscation. This series aims to dissect tools like .NET Reactor and SmartAssembly, shedding light on how they modify .NET code to impede analysis, specifically targeting .NET's Intermediate Language (IL). The exploration of obfuscation techniques is geared towards providing insights for both beginners and seasoned individuals in malware analysis.

Understanding Obfuscators: Obfuscators are software designed to modify code, hindering analysis and making it challenging for researchers to decompile. While some obfuscators mutate machine code, targeting malware developed using languages like C, Assembly, or Rust, others focus on modifying IL code generated by .NET compilers.

Series Objectives: This series of articles aims to unravel modern techniques employed by obfuscators like .NET Reactor and SmartAssembly, preferred choices of malware creators. The articles will delve into deobfuscation methods, explore tools designed to counter obfuscation, and potentially develop or adapt deobfuscators.

Scope and Audience: The content is designed to be accessible to individuals with a basic understanding of .NET, while also catering to those with some experience in malware analysis. A foundational knowledge of malware analysis tools and concepts is expected, with prior experience in analyzing obfuscated code considered advantageous.

Sample Obfuscation Strategies: The series initiates by presenting a simple obfuscator and exploring various strategies to enhance protection, including:

- Proxy Functions: Moving string assignments into separate functions to complicate analysis.
- Character Breakdown: Splitting strings into individual characters to obscure their meaning.
- Numeric Conversion: Replacing characters with their numerical representations to obfuscate the code.
- Heavy Math: Using complex mathematical operations with randomly generated expressions to deter analysis.
- CFG Obfuscation: Making the control flow complex and challenging to follow.

Future Outlook: The series promises to continue dissecting obfuscation techniques, aiming to provide readers with a deeper understanding of malware evasion tactics. Each article will build upon the previous, gradually unraveling the intricate layers of obfuscation employed by malware creators.

🥷 TTP Analysis

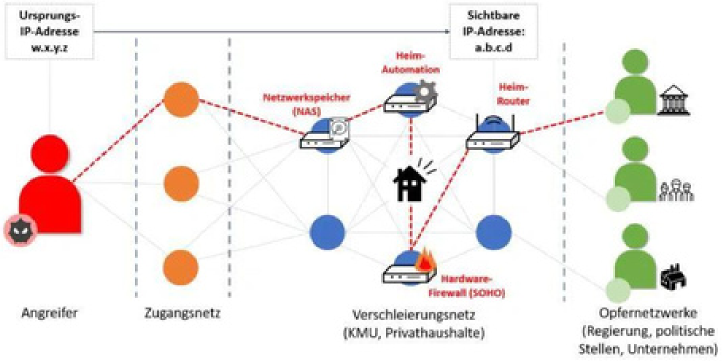

Ursprungs-IP-Adresse w.x.y.z
Sichtbare IP-Adresse: a.b.c.d
Heim-Automation
Netzwerkspeicher (NAS)
Heim-Router
Hardware-Firewall (SOHO)
Angreifer
Zugangsnetz
Verschleierungsnetz (KMU, Privathaushalte)
Opfernetzwerke (Regierung, politische Stellen, Unternehmen)

Abbildung: Schematische Darstellung eines Anonymisierungsnetzwerks

The German intelligence service BfV (Bundesamt für Verfassungsschutz) has issued a Cyber Brief detailing the activities of Chinese cyber espionage groups APT15 (Vixen Panda, Ke3chang) and APT31 (Zirconium, Judgment Panda). These groups have been identified as exploiting Small Office/Home Office (SOHO) facilities for state-sponsored cyber operations, primarily targeting government and political institutions.

In this campaign, APT15 and APT31 have utilized SOHO devices, commonly used to create small home networks, for their cyber operations. These devices, if not adequately updated or supported by manufacturers, are particularly vulnerable to exploitation.

The attackers leverage compromised SOHO devices to create sophisticated obfuscation networks, resembling commercial VPN networks. This infrastructure enables them to penetrate victim networks with multiple intermediate steps, making it challenging to detect their activities.

While the BfV has not reported any casualties, German news sources indicate that APT15 compromised the Federal Agency for Cartography and Geodesy (BKG) using a network of compromised routers. This incident, confirmed by forensic network analysis, occurred in December 2021, resulting in the reconstruction of the affected network.

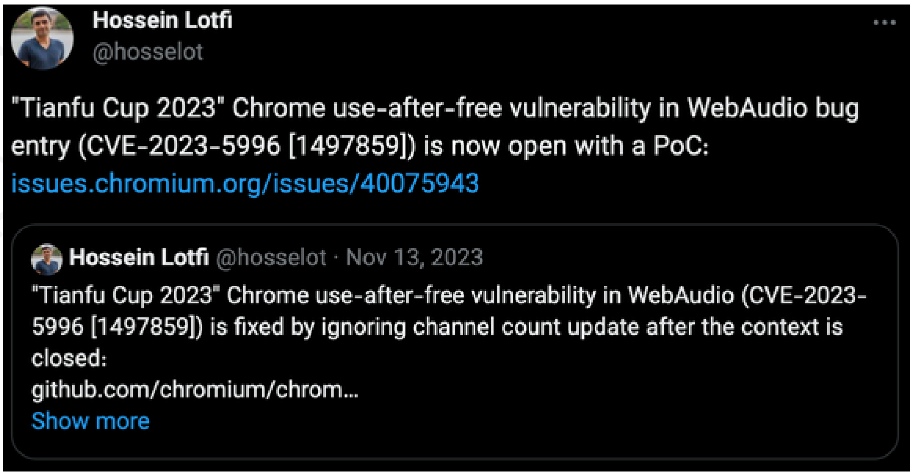
The severity of the incident prompted international cooperation, leading to the creation of a joint classified report on APT15, involving at least 12 countries sharing their knowledge.

Additionally, APT31's campaign targeting SOHO devices, particularly routers, was previously attributed by the French ANSSI in April 2021.

The Cyber Brief offers preventive measures to mitigate risks associated with Chinese cyber actors, emphasizing the importance of installing updates and replacing outdated devices no longer supported by manufacturers.

https://twitter.com/_cybule/status/1699741309479563512

1Day



Hossein Lotfi
@hosselot

"Tianfu Cup 2023" Chrome use-after-free vulnerability in WebAudio bug entry (CVE-2023-5996 [1497859]) is now open with a PoC: issues.chromium.org/issues/40075943

Hossein Lotfi @hosselot · Nov 13, 2023
"Tianfu Cup 2023" Chrome use-after-free vulnerability in WebAudio (CVE-2023-5996 [1497859]) is fixed by ignoring channel count update after the context is closed:
github.com/chromium/chrom...
Show more

Advisory ID: CVE-2023-5996
Date: October 31, 2023
Severity: High
CVE ID: CVE-2023-5996
Vulnerability Type: Use-after-free
Affected Software: Google Chrome
Impact: Remote Code Execution (RCE)

Summary: A critical vulnerability has been discovered in Google Chrome's WebAudio component, indexed as CVE-2023-5996. The vulnerability allows remote attackers to execute arbitrary code within the context of the renderer process. The issue was first brought to light by Hossein Lotfi during the Tianfu Cup 2023 event.

Vulnerability Details: The vulnerability stems from improper handling of AudioContext in certain scenarios, allowing the forced initiation of audio rendering processes even without user interaction. Specifically, the vulnerability occurs within the RealtimeAudioDestinationHandler class. By manipulating the channel count parameter, attackers can trigger the StartPlatformDestination function, consequently initiating audio rendering threads. This can be further exploited to reinstate audio rendering threads in closed AudioContext objects, leading to a use-after-free vulnerability.

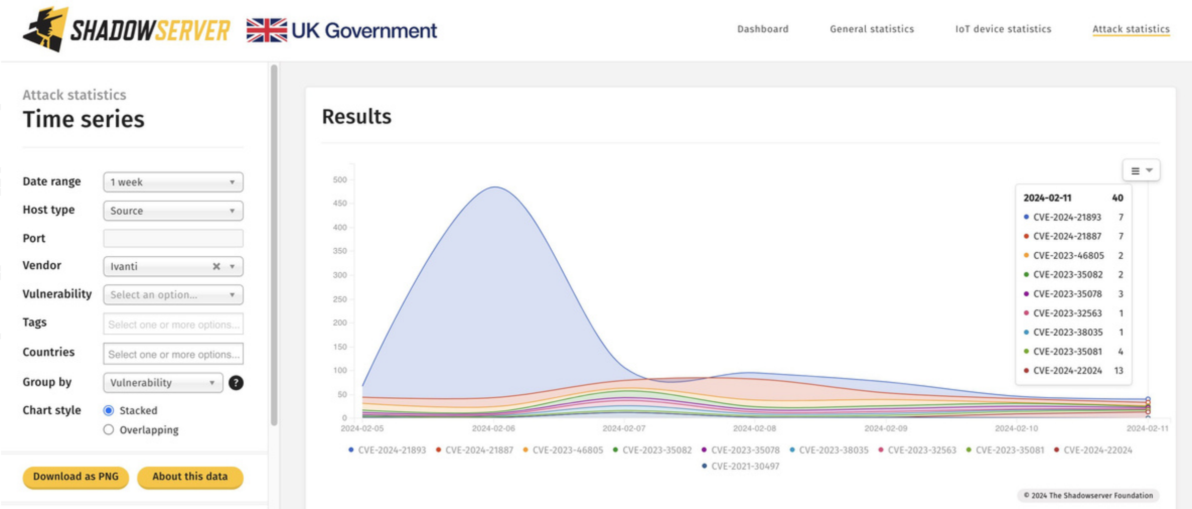
Exploitation: Exploiting this vulnerability enables attackers to execute arbitrary code within the context of the affected renderer process. By carefully crafting an exploit, attackers can trigger a use-after-free condition, allowing them to manipulate memory layout and execute arbitrary code. This could lead to potential compromise of confidentiality, integrity, and availability of user data and system resources.

Recommendation: To mitigate the risk associated with CVE-2023-5996, it is strongly recommended that all users update their Google Chrome installations to the latest available version as soon as possible. Additionally, users are advised to exercise caution when visiting unfamiliar websites or downloading files from untrusted sources to minimize the risk of exploitation.

References:

- Google Chrome Issue Tracker - CVE-2023-5996
- https://twitter.com/hosselot/status/1757049551888719973

🌶 Trending Exploit



Attack statistics

Time series

Date range	1 week
Host type	Source
Port	
Vendor	Ivanti
Vulnerability	Select an option...
Tags	Select one or more options...
Countries	Select one or more options...
Group by	Vulnerability
Chart style	● Stacked ○ Overlapping

Results

2024-02-11	40
● CVE-2024-21893	7
● CVE-2024-21887	7
● CVE-2023-46805	2
● CVE-2023-35082	2
● CVE-2023-35078	3
● CVE-2023-32563	1
● CVE-2023-38035	1
● CVE-2023-35081	4
● CVE-2024-22024	13

https://twitter.com/Shadowserver/status/1757063290746790184

Since February 9th, 2024, around 8:00 UTC, there has been a notable increase in exploitation attempts targeting Ivanti Connect Secure systems. These attempts primarily focus on exploiting the '/dana-na/auth/saml-sso.cgi' endpoint. Analysis reveals that these are primarily callback tests, suggesting reconnaissance or vulnerability verification activities. As of the latest observation, a total of 47 unique IP addresses have been identified engaging in exploitation attempts.

Advisory and Further Information: For detailed information regarding CVE-2024-22024 and mitigation strategies, refer to the official Ivanti advisory available at Ivanti Advisory.

For ongoing monitoring of CVE-2024-22024 exploitation attempts and other targeted attacks against Ivanti products, access the Shadowserver dashboard at Shadowserver Dashboard. Note that the tag for CVE-2024-22024 was added on February 10th, 2024, and thus the dashboard does not display attack statistics for February 9th, 2024.

Recommendations:

- Ivanti Connect Secure administrators are strongly advised to review the provided advisory and apply recommended patches or updates promptly.
- Implement additional security measures such as firewall rules, intrusion detection systems, and web application firewalls to detect and mitigate exploitation attempts.
- Monitor network traffic and system logs for any suspicious activities or unauthorized access attempts.
- Regularly update and patch Ivanti products to ensure resilience against known vulnerabilities and emerging threats.

🕯️ The Topic of the Week

https://www.youtube.com/watch?v=BEkziTXz9Js

CrowdStrike, a leading cybersecurity company, launched an impactful ad campaign during the Super Bowl, tapping into the massive audience of one of the most-watched events globally. The campaign, titled "Riding with CrowdStrike," aimed to raise awareness about modern cybersecurity threats and highlight CrowdStrike's commitment to securing the future against relentless adversaries.

The ad opens with a powerful message: "Modern adversaries are relentless." This sets the tone for the narrative, emphasizing the ever-evolving nature of cyber threats in an increasingly advanced technological landscape. As the scene unfolds, viewers are introduced to "Charlotte," portrayed as CrowdStrike's secret weapon, ready to take on these adversaries.

With pulsating music and dynamic visuals, the ad captures the urgency and importance of cybersecurity in today's digital age. CrowdStrike positions itself as the ally against these threats, offering protection not just for today but also for the future.

The tagline "CrowdStrike stops breaches. Today. Tomorrow. And beyond." encapsulates the company's dedication to continuous innovation and proactive defense against cyber breaches. It reinforces CrowdStrike's reputation as a trusted partner in safeguarding organizations and individuals from cyberattacks.

The ad effectively communicates CrowdStrike's message of resilience, highlighting the company's proactive approach to cybersecurity and its commitment to staying ahead of emerging threats. By showcasing their capabilities in a high-profile setting like the Super Bowl, CrowdStrike aims to reach a broad audience and reinforce its position as a leader in the cybersecurity industry.

To experience the full impact of the CrowdStrike Super Bowl ad campaign, viewers can watch the captivating video on YouTube: CrowdStrike Super Bowl Ad.

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.