Threat Intel Roundup: FortiCVE, SSL-VPN, Trap, DarkGate

Week in Overview[12 Mar-19 Mar] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **Uncovering the DarkGate Campaign: Exploiting Microsoft Windows Zero-Day** Summary: This technical report delves into the discovery of the DarkGate campaign, which exploited a zero-day vulnerability in Microsoft Windows. Researchers detail the modus operandi of the campaign, the vulnerability exploited (CVE-2024-21412), and the propagation of the DarkGate malware through fake software installers masquerading as legitimate applications. The report highlights the significance of promptly addressing such vulnerabilities and staying vigilant against sophisticated cyber threats.
2. **Microsoft AITM Honeytoken: Protecting Users from Phishing Attacks** Summary: This technical overview introduces the Microsoft AITM Honeytoken system designed to safeguard users from phishing attacks targeting Microsoft 365 tenants. The report explains how the system utilizes custom CSS injected into the Microsoft login page to detect and warn users about potential phishing attempts. By modifying the login page's appearance based on the origin of the request, the system aims to prevent successful phishing attacks and enhance overall security.
3. **Exploring Windows Hyper-V Secure Kernel Debugging with WinDbg and EXDI: Part 4** Summary: This technical article is the fourth installment in a series exploring Windows Hyper-V Secure Kernel Debugging using WinDbg and the Extended Debugging Interface (EXDI). The report delves into the analysis of various fields within the Virtual Machine Control Structure (VMCS) to combat mitigations against instruction trace within Windows. It provides insights into the operations of the Windows hypervisor and early boot processes, offering practical guidance for debugging secure kernel environments.

4. **Unveiling the Trap Stealer: A GO-based Data Theft Tool** Summary: This technical summary unveils the Trap Stealer, a data theft tool rewritten in GO (Golang), designed to exfiltrate sensitive information. The report describes the functionality of the tool, its origins as a Python-based application, and its method of uploading stolen data to a designated file-sharing service. By shedding light on this evolving cyber threat, the report aims to raise awareness and promote proactive measures against data theft attacks.
5. **Investigating and Exploiting a Pre-auth Remote Code Execution Vulnerability in FortiGate SSL VPN** Summary: This technical investigation focuses on a pre-auth remote code execution vulnerability discovered in FortiGate SSL VPN appliances. The report outlines the vulnerability's impact, exploitation techniques, and potential consequences for affected systems. By providing detailed insights into the vulnerability's exploitation, the report aims to assist security professionals in mitigating the risks posed by such critical security flaws.
6. **Vulnerability Alert: FortiOS and FortiProxy Authorization Bypass (CVE-2024-23112)** Summary: This technical alert highlights a critical authorization bypass vulnerability (CVE-2024-23112) affecting FortiOS and FortiProxy products. The report details the nature of the vulnerability, its potential impact on affected systems, and recommended mitigation strategies. By promptly addressing this vulnerability and implementing necessary security measures, organizations can mitigate the risk of unauthorized access and data breaches.

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:

- Uncovering the DarkGate Campaign: Exploiting Microsoft Windows Zero-Day
- Microsoft AITM Honeytoken: Protecting Users from Phishing Attacks
- Exploring Windows Hyper-V Secure Kernel Debugging with WinDbg and EXDI: Part 4
- Unveiling the Trap Stealer: A GO-based Data Theft Tool
- Investigating and Exploiting a Pre-auth Remote Code Execution Vulnerability in FortiGate SSL VPN
- Vulnerability Alert: FortiOS and FortiProxy Authorization Bypass (CVE-2024-23112)

🚨 Vulnerability of the Week

FortiOS CVE-2024-23112

A critical vulnerability, identified as CVE-2024-23112, has been discovered in FortiOS and FortiProxy, exposing a significant security flaw that could lead to unauthorized access to user bookmarks. Tracked under Common Weakness Enumeration (CWE-639), this vulnerability allows authenticated malicious users to bypass authorization controls through manipulation of user-controlled keys. This could potentially compromise sensitive information and undermine the security posture of affected systems.

Details: The vulnerability affects several versions of FortiOS and FortiProxy, including:

- FortiOS versions 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, and 7.0.1 through 7.0.13.
- FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, and 7.0.0 through 7.0.14 SSL-VPN.

Exploitation of this vulnerability occurs through URL manipulation, enabling an authenticated malicious user to gain unauthorized access to another user's bookmarks. By leveraging this vulnerability, attackers can bypass the intended authorization mechanisms and potentially access sensitive resources or perform unauthorized actions within the system.

ZoomEye Dork Findings: The widespread impact of this vulnerability is evident from ZoomEye Dork findings, with approximately 573,674 results identified mainly in the United States, Mexico, and various other countries. The dork query "app:"Fortinet httpd"" reveals a significant number of potentially vulnerable systems, highlighting the urgent need for mitigation measures and patch deployment.

Art of Detection

Table 33-52. VMX Controls For Intel Processor Trace

Type of VMX Control	Bit Position[1]	Value	Behavior
Secondary processor-based VM-execution control	19	0	Each PIP generated in VM non-root operation will set the NR bit. PSB+ in VMX non-root operation will include the VMCS packet, to ensure that the decoder knows which guest is currently in use.
		1	Each PIP generated in VMX non-root operation will clear the NR bit. PSB+ in VMX non-root operation will not include the VMCS packet.
VM-exit control	24	0	Each VM exit generates a PIP in which the NR bit is clear, and a CFE/EVD if Event Trace is enabled. In addition, SMM VM exits generate VMCS packets.
		1	VM exits do not generate PIPs, CFEs, or EVDs, and no VMCS packets are generated on SMM VM exits.
VM-entry control	17	0	Each VM entry generates a PIP in which the NR bit is set (except VM entries that return from SMM to VMX root operation), and a CFE if Event Trace is enabled. In addition, VM entries that return from SMM generate VMCS packets.
		1	VM entries do not generate PIPs or CFEs, and no VMCS packets are generated on VM entries that return from SMM.

https://twitter.com/AlanSguigna/status/1769695353970823294

In this installment of our series, we delve deeper into the fields within the Virtual Machine Control Structure (VMCS) to understand and modify them, specifically targeting some of the mitigations against instruction tracing within Windows. Before proceeding, it's recommended to review the preceding articles for context:

1. **Part 1:** An introduction to debugging Windows with Hyper-V and Virtualization-based Security (VBS) enabled, covering VM Launch and VM Exit breakpoints, along with a brief overview of Intel Processor Trace.
2. **Part 2:** Intel Processor Trace for tracing transitions from a Guest (securekernel) to Host (hvix64) environment.
3. **Part 3:** Debugging the securekernel with symbols.

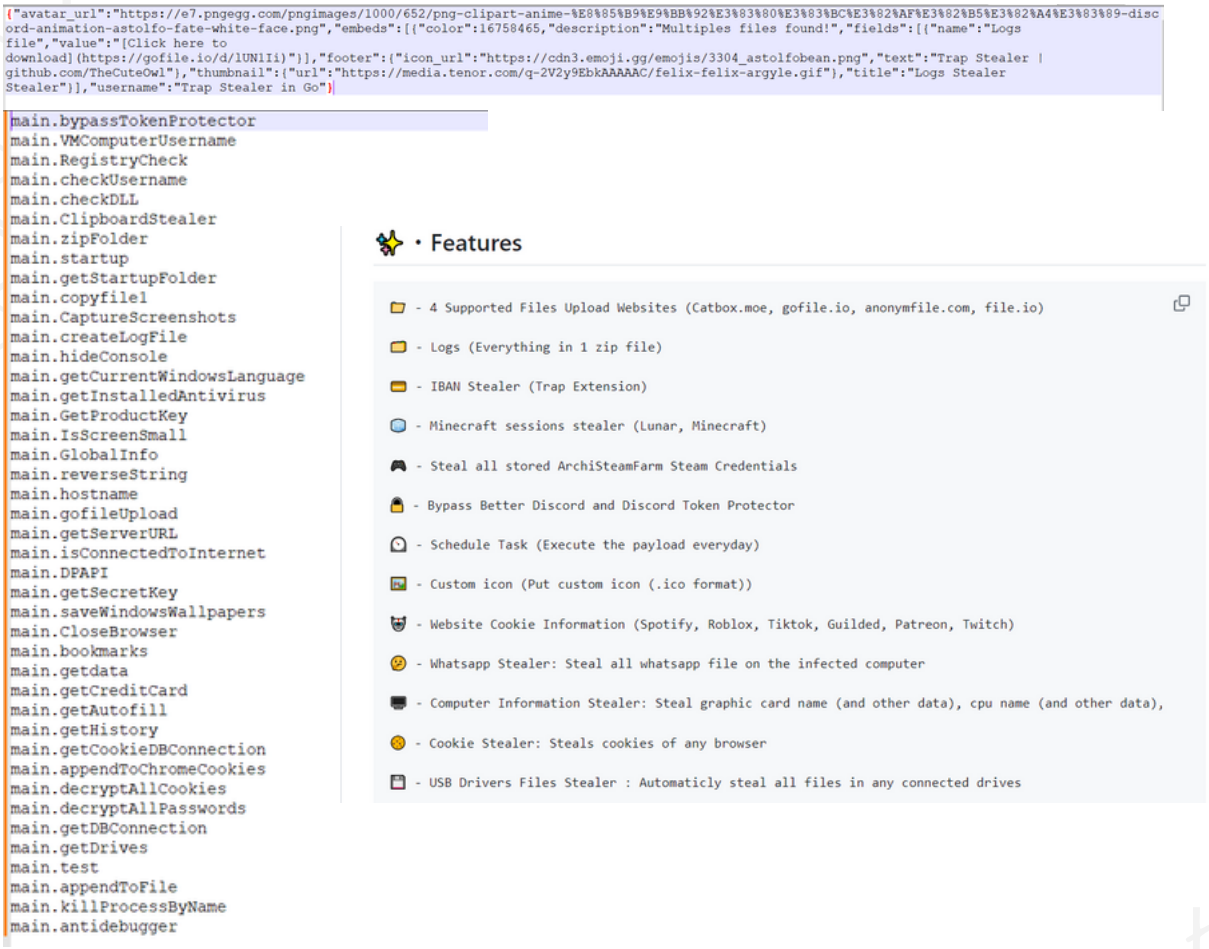
In my pursuit of technical exploration and knowledge dissemination, I often find inspiration in Satoshi Tanda's words from his article "How I found Microsoft Hypervisor bugs as a by-product of learning." He aptly states, "Simply learning security features yielded two vulnerabilities in Windows core components (and 3000 USD) as by-product." This ethos drives my commitment to sharing insights and discoveries for the benefit of others.

To enhance our understanding of the Windows hypervisor and early boot processes, we've developed a SourcePoint macro capable of extracting and modifying key fields within the VMCS. This macro, inspired by Satoshi's hvext.js application, leverages inline assembly to interact with the VMCS. Here's a glimpse into some of the functions within our macro:

- **vmread:** Reads a VMCS field based on the provided encoding.
- **vmwrite:** Writes a value to a VMCS field specified by the encoding.
- **dump:** Displays important VMCS fields for analysis.
- **reason:** Indicates the reason for VM exit.
- **ipt:** Enables Intel Processor Trace for uninterrupted tracing.

By executing the "dump" function, we gain insights into various VMCS fields across guest-state, host-state, VM-execution, VM-entry, and VM-exit categories. These insights are instrumental in understanding the hypervisor's behavior and customizing it to our needs.

😈 Malware or Ransomware



https://twitter.com/suyog41/status/1769631653536972984

A new iteration of the data theft tool known as Trap Stealer has emerged, now rewritten in GO. This tool, identified by the hash e4f61a7237508a71efed50b0a4b0df7d, marks a significant evolution from its previous Python-based version. The Trap Stealer GO variant poses a heightened threat to cybersecurity, facilitating the unauthorized exfiltration of sensitive information.

Trap Stealer Origins: The original version of Trap Stealer, coded in Python, gained notoriety for its capabilities in clandestinely harvesting data from compromised systems. Hosted on GitHub, the Python-based Trap Stealer repository provided malicious actors with a toolset for covertly extracting sensitive information from victim machines.

Transition to GO: The transition to GO represents a strategic move by threat actors to enhance the efficiency and stealthiness of data theft operations. The utilization of GO, known for its speed and versatility, empowers Trap Stealer with improved evasion techniques and advanced functionality.

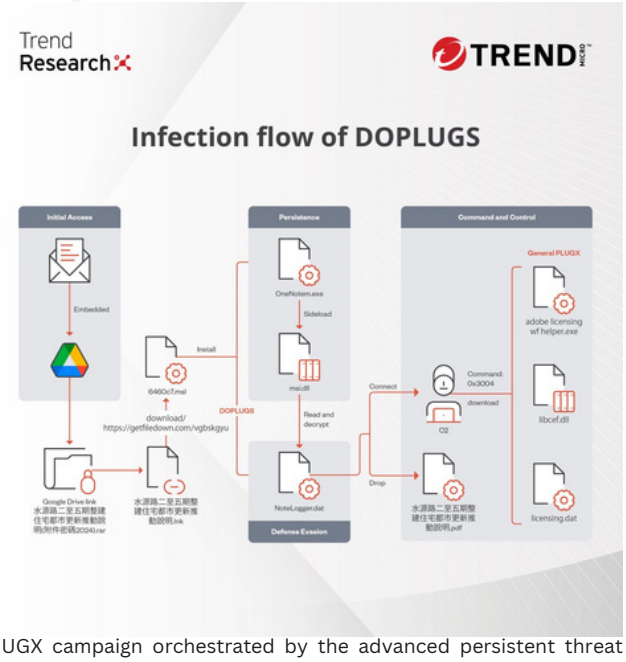
Key Features: Trap Stealer in its GO incarnation retains the core functionality of its predecessor while introducing enhancements tailored to the GO programming language. Key features include:

- **Stealthy Execution:** Leveraging the capabilities of GO, Trap Stealer executes stealthily on compromised systems, minimizing detection by security solutions.
- **Efficient Data Theft:** The tool efficiently harvests a wide range of sensitive information from victim machines, including credentials, financial data, and personal information.
- **Upload to gofile.io:** Stolen data is securely uploaded to gofile.io, a file-sharing platform, enabling threat actors to access and exploit the pilfered information remotely.

Indicators of Compromise (IOCs):

- Hash: e4f61a7237508a71efed50b0a4b0df7d
- GitHub Repository (Old Python Version): https://github.com/TheCuteOwl/Trap-Stealer
- Data Upload Platform: gofile.io

TTP Analysis



The SMUGX campaign orchestrated by the advanced persistent threat (APT) group Earth Preta, also known as Mustang Panda and Bronze President, has extended its reach beyond Europe into Asia, particularly targeting countries like Taiwan and Vietnam. The campaign employs customized variants of PlugX malware, dubbed DOPLUGS, indicating the evolving cyberthreat landscape in the region.

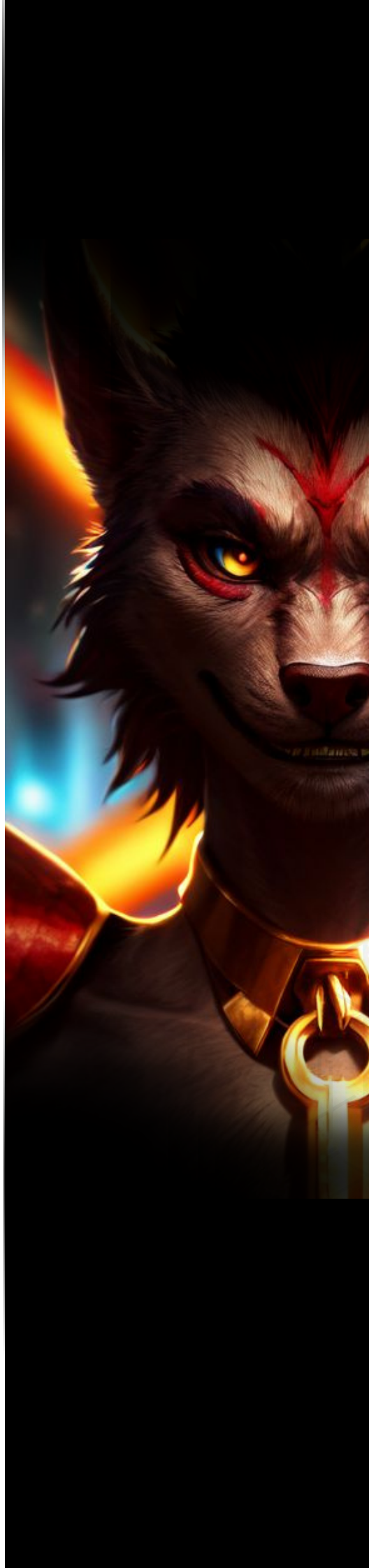
Campaign Overview: Initially disclosed by Check Point in July 2023, the SMUGX campaign primarily targeted European countries. However, our investigation unearthed its presence in Asia, with phishing emails containing customized PlugX malware observed in Taiwan, Vietnam, Malaysia, and other Asian nations throughout 2022 and 2023. This variant of PlugX, referred to as DOPLUGS, has been active since 2022 and exhibits distinct functionalities compared to its predecessors.

Decoys and Victims: Analysis of noteworthy DOPLUGS files since July 2023 reveals victims predominantly from Taiwan and Mongolia. Decoy files related to social engineering, such as documents referencing the Taiwanese presidential election of January 2024, were used to lure victims into executing the malware. Notably, the malware campaign appears tailored to exploit ongoing events and interests in the targeted regions.

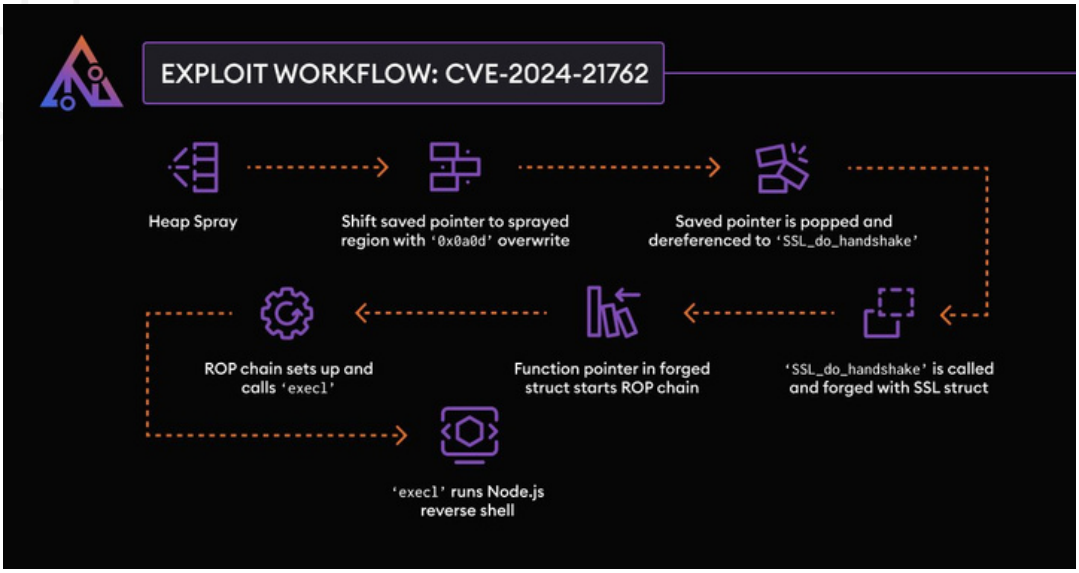
Spear-phishing Emails as Initial Access: Victims are targeted through spear-phishing emails embedded with Google Drive links hosting password-protected archive files. Upon interaction, malicious Windows shortcut files (LNK) disguised as documents are executed, triggering the download and execution of the DOPLUGS malware. The malware payload, concealed within legitimate executables and DLL files, is downloaded from remote servers controlled by the attackers.

Analysis of the Tools Used: Our analysis delves into the intricacies of DOPLUGS, highlighting its role as a downloader with backdoor capabilities. The infection flow involves the execution of multiple files, including LNK files and MSI executables, ultimately leading to the deployment of DOPLUGS on the victim's system. Noteworthy files associated with the infection flow include the LNK file "水源路二至五期整建住宅都市更新推動說明" (Explanation of Urban Renewal Initiative for Residential Development in Phases Two to Five of Shuiyuan Road), and associated MSI, executable, DLL, and encrypted payload files.

https://twitter.com/TrendMicroRSRCH/status/1769982141658431700



1Day



https://twitter.com/infosec_au/status/1768743977564393950

In February, Fortinet issued an advisory regarding an "out-of-bounds write vulnerability" affecting the SSL VPN component of their FortiGate network appliance. This vulnerability could potentially lead to remote code execution and was deemed critical due to the widespread deployment of FortiGate appliances. Our security research team immediately initiated an investigation to identify and exploit this vulnerability, aiming to provide valuable insights for defenders and enhance our exposure engine.

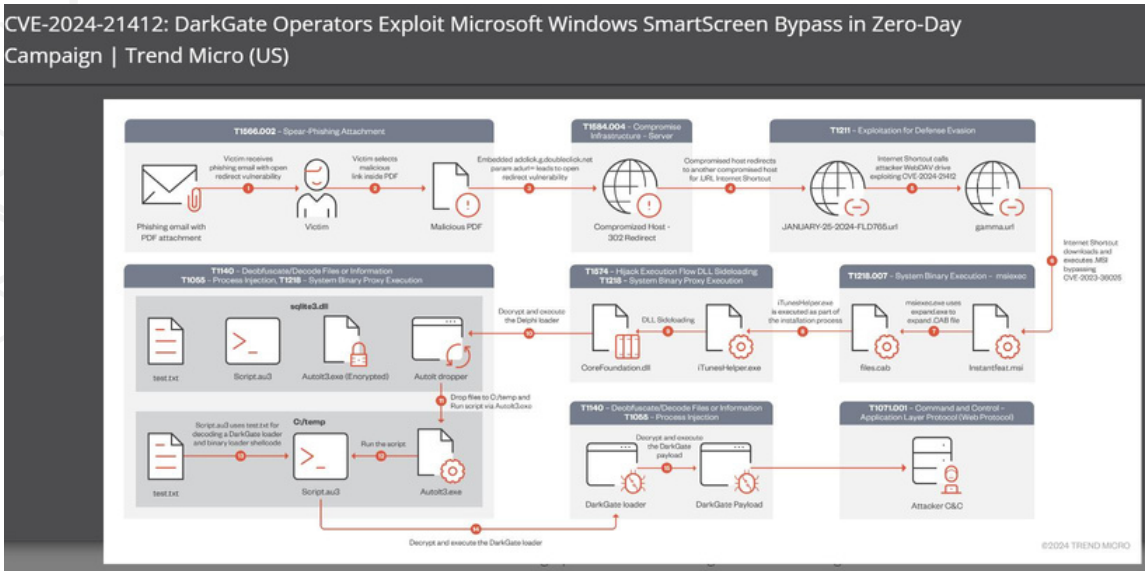
Extracting the Binary: We obtained two versions of the FortiGate appliance, version 7.2.5 and the latest at the time, version 7.2.7. These versions were mounted as VMs, and we extracted the binaries from them to compare changes. The FortiGate appliances bundle most applications into a single binary, "/bin/init." By decompressing and extracting the root filesystem, we obtained the necessary binaries for analysis.

Patch Diffing: We utilized Ghidra and BinDiff to compare the patched and unpatched binaries. However, due to significant version differences, manual inspection became necessary. We focused on the HTTP parsing functionality, particularly areas prone to memory corruption issues. Through careful analysis of function calls and log messages, we identified modifications in functions handling HTTP request parsing, notably adding length checks and error messages.

Finding an Endpoint: To determine exploitability, we activated debug logging and sent chunked requests to known endpoints. We identified the function responsible for logging errors related to chunked transfer encoding. Surprisingly, triggering this error was only possible when the function received a specific argument. By tracing back from calling functions, we identified a key function, "default_handler," which led us to potential exploitation avenues.

Triggering a Crash: We crafted Python scripts to test various chunked requests, focusing on triggering the added length checks. Despite the resilience of the parsing, we eventually achieved a crash with a carefully crafted payload. Interestingly, the crash occurred with a zero-length chunk followed by 89 chunk trailers, seemingly bypassing the new checks.

🌶️ Trending Exploit



https://twitter.com/TheCyberSecHub/status/1768395955802652795

In a recent discovery, researchers have unveiled a DarkGate campaign that emerged in mid-January 2024, leveraging a zero-day vulnerability within Microsoft Windows. The Zero Day Initiative (ZDI) brought to light this alarming exploit, marked by the utilization of fake software installers to propagate malware.

The vulnerability in question, designated as CVE-2024-21412 with a CVSS score of 8.1, pertains to an Internet Shortcut Files Security Feature Bypass Vulnerability. Exploiting this flaw allows unauthenticated attackers to circumvent displayed security checks by enticing victims to click on a specially crafted file link.
The modus operandi of the DarkGate campaign involved the deployment of PDF documents as lures, incorporating Google DoubleClick Digital Marketing (DDM) open redirects. These redirects steered unsuspecting victims towards compromised websites harboring the exploit for CVE-2024-21412, ultimately leading to the dissemination of malicious Microsoft (.MSI) installers.

Trend Micro's analysis revealed that the phishing campaign deployed open redirect URLs from Google Ad technologies to distribute counterfeit Microsoft software installers masquerading as legitimate applications such as Apple iTunes, Notion, and NVIDIA drivers. Disguised within these fake installers was a sideloaded DLL file, facilitating the decryption and infiltration of users' systems with the DarkGate malware payload.
Microsoft promptly addressed this vulnerability with Patch Tuesday security updates released in February 2024. Subsequently, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) included the flaw in its Known Exploited Vulnerabilities catalog.

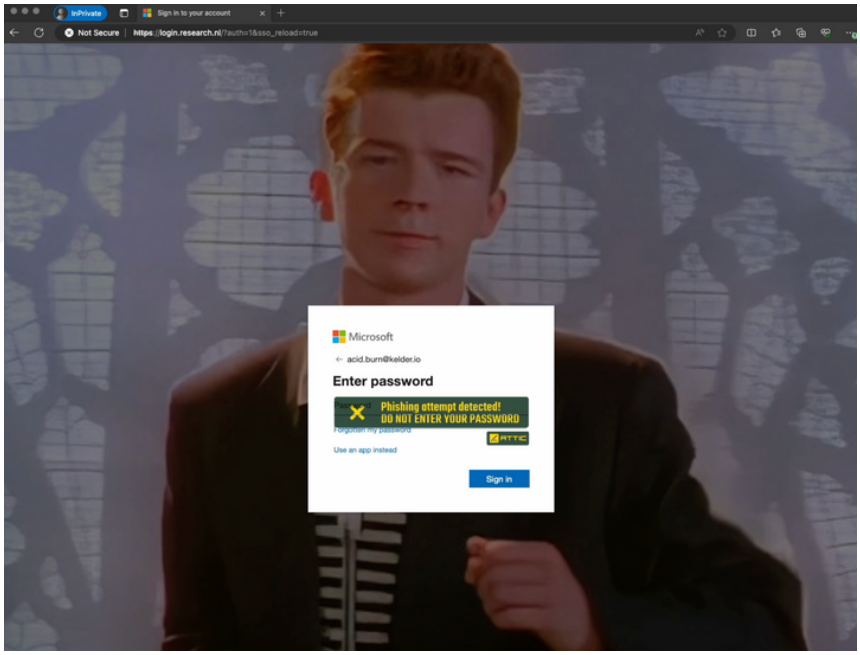
Furthermore, Trend Micro researchers identified the APT group Water Hydra as the perpetrators behind the exploitation of CVE-2024-21412 in a zero-day attack chain.

The DarkGate Remote Access Trojan (RAT), coded in Borland Delphi, operates within the cybercrime ecosystem as a malware-as-a-service (MaaS) model. Renowned for its sophistication, DarkGate boasts a plethora of features including process injection, file download and execution, information exfiltration, shell command execution, and keylogging capabilities. The malware is continuously evolving and poses a significant threat to organizations worldwide.

The attack chain analyzed by ZDI commences with a phishing message containing a PDF attachment housing a specially crafted link. Upon interaction, the victim is redirected to a compromised web server hosting an .URL internet shortcut file that exploits CVE-2024-21412.

The report underscores the importance of vigilance and caution among users, advising against trusting software installers received from unofficial channels. By remaining vigilant and educating users about potential threats, organizations can mitigate the risks posed by sophisticated cyberattacks like the DarkGate campaign.

The Topic of the Week



https://twitter.com/wesleyneelen/status/1769695254897140011

In January, we introduced a groundbreaking feature to Attic designed to detect AiTM (Account in the Middle) attacks targeting Microsoft 365 tenants of our customers. Leveraging the platform of didsomeoneclone.me and employing custom CSS in the Microsoft login page, we pioneered a method to identify and mitigate these sophisticated threats. Since its inception, our approach has gained traction among industry peers, including EYE, CIPP, and the esteemed honey-heroes at Thinkst. This collaborative effort has amplified our impact, fortifying the cybersecurity landscape against evolving threats.

Building upon our initial innovation, EYE and CIPP have enhanced our solution by incorporating a crucial improvement. They ingeniously modified the CSS to provide users with a warning whenever they encounter a potential AITM phishing website. This proactive approach not only detects phishing attempts but also empowers users to preemptively thwart such attacks. Inspired by their innovation, we have opted to integrate this technique (optionally) into our own products, recognizing the paramount importance of prevention alongside detection.

How Does It Work?
Our existing detection mechanism relies on injecting CSS code into the Microsoft tenant, allowing it to interact with our backend. Upon receiving a request, the backend analyzes its origin. If the request is traced back to a known phishing website, a notification is promptly dispatched.

However, CSS offers capabilities beyond backend interaction. It enables us to modify the appearance of the Microsoft login page dynamically. Our novel approach involves setting a background-image for the Microsoft sign-in box, hosted on our backend. Depending on the request's legitimacy, the backend either returns an image alerting the user to potential malicious activity or provides an empty response, concealing any warning. The updated CSS snippet illustrates this concept:

```
.ext-sign-in-box {
    background: white url('https://dscm.li/-250987757') center no-repeat;
}
```

By leveraging CSS manipulation, we enhance user awareness and empower them to make informed decisions when navigating potentially hazardous online environments. This layered defense strategy not only identifies threats but also actively engages users in the fight against cybercrime, fostering a safer digital ecosystem for all.

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.