

Threat Intel Roundup: DeadGlyph, T-Mobile, Juniper SRX, JetBrains TeamCity



Week in Overview[19 Sep-26 Sep]



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. Malware Distribution from zzlsteel[.]cc and Associated C2 Domains

- **Concern:** Distribution of OriginBotnet and XKeyBot malware.
- **C2 Servers:** nitrosoftwares[.]shop, ltm-canada[.]com/login/, turinapparrels[.]com/login/.

2. "Passport and KYC Documents[.]zip" Malware

- **Concern:** Sophisticated multi-stage malware delivered via a zip file.
- **Execution Chain:** LNK -> PowerShell -> Dropbox -> Delphi RunPE -> UPX -> unknown C++ malware.

3. Stealth Falcon Preying on Middle Eastern Skies with DeadGlyph

- **Concern:** Cyber-espionage group targeting entities in the Middle East using DeadGlyph malware.
- **Tactics:** Spear-phishing, custom malware, and persistent operations.

4. T-Mobile Employee PII Breach and Sony Data Breach

- **Concern:** Employee PII leaked in T-Mobile breach; alleged Sony data breach.
- **Impact:** Exposure of sensitive employee information, potential for identity theft and fraud.

5. CVE-2023-41892 Craft CMS Remote Code Execution Vulnerability

- **Concern:** RCE vulnerability in Craft CMS.
- **Exploitation:** Attackers can execute arbitrary code remotely.
- **Mitigation:** Update Craft CMS to the latest version, monitor for unauthorized access.

6. From ScreenConnect to Hive Ransomware in 61 Hours

- **Concern:** Rapid progression from ScreenConnect exploitation to Hive Ransomware deployment.
- **Impact:** Encryption of files, ransom demands, potential data loss.

7. Critical Authentication Bypass in JetBrains TeamCity CI/CD Servers (CVE-2023-42793)

- **Concern:** Authentication bypass vulnerability in JetBrains TeamCity CI/CD servers.
- **Impact:** Unauthorized administrative control, potential supply chain attack vector.

8. Critical Vulnerability in Juniper Devices

- **Concern:** Unauthenticated RCE flaw in Juniper SRX firewalls and EX switches.
- **Impact:** Remote code execution, unauthorized access, potential data breach.

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:

- Critical Vulnerability in Juniper Devices
- Critical Authentication Bypass in JetBrains TeamCity CI/CD Servers (CVE-2023-42793)
- From ScreenConnect to Hive Ransomware in 61 Hours
- CVE-2023-41892 Craft CMS Remote Code Execution Vulnerability
- T-Mobile Employee PII Breach and Sony Data Breach
- Malware Distribution from zzlsteel[.]cc and Associated C2 Domains
- "Passport and KYC Documents[.]zip" Malware
- Stealth Falcon Preying on Middle Eastern Skies with DeadGlyph



Vulnerability of the Week

Craft CMS

CVE-2023-41892

A significant security vulnerability, CVE-2023-41892, has been identified in Craft CMS, a widely used content management system. This vulnerability allows for Remote Code Execution (RCE), enabling attackers to execute arbitrary code remotely and potentially compromise the security and integrity of the affected application. The Proof-of-Concept (POC) provided demonstrates the exploitation process, underscoring the urgency for immediate mitigation actions to prevent unauthorized access and control over the vulnerable systems.

Technical Details

The POC outlines the exploitation process, beginning with the use of specific headers and data payloads sent via HTTP requests to the vulnerable Craft CMS server. The exploit involves writing a malicious payload to a temporary file on the server, triggering Imagick to write a shell, and then executing arbitrary commands on the server. The exploit uses the `conditions/render` action and manipulates the `configObject[class]` parameter to execute the arbitrary code, leading to the compromise of the server. The POC code provided is executed with Python, and it automates the entire exploitation process, making it easy for an attacker to compromise a vulnerable Craft CMS server.

Mitigation and Recommendations

To mitigate the risks associated with CVE-2023-41892, it is crucial for organizations using Craft CMS to update their systems to a version that patches this vulnerability. If an update is not immediately available, organizations should consider disabling the affected functionality or increasing monitoring and access controls to detect and prevent exploitation attempts. It is also essential to conduct a thorough security assessment to identify and remediate any unauthorized changes or access to the affected systems. Organizations are advised to follow best practices for security hygiene, including regular patch management, monitoring, and employee awareness training to prevent exploitation of vulnerabilities.



Leakage Insight

```
... "Name": "T-Mobile", "Phone": "1-800-950-5888", "Address": "16000 W. 16th Ave, Denver, CO 80202", "Website": "https://www.t-mobile.com", "Employees": 100000, "Revenue": 10000000000, "Data Breach": true, "Breach Date": "2023-09-21", "Breach Type": "PII", "Breach Description": "A significant data breach involving the leak of T-Mobile employee Personally Identifiable Information (PII). The breach occurred in April 2023 and was not disclosed until September 21, 2023. The leaked information includes names, phone numbers, and addresses of employees. The breach was allegedly executed by 'Doubl' and the leaked information was disseminated by 'Emo'."}
```

```
... "Name": "Sony Group Corporation", "Phone": "+81 3 6858 2100", "Address": "1-1-1, Hatchobashi, Minato-ku, Tokyo 105-8505, Japan", "Website": "https://www.sony.com", "Employees": 100000, "Revenue": 100000000000, "Data Breach": true, "Breach Date": "2023-09-21", "Breach Type": "PII", "Breach Description": "A significant data breach involving the leak of Sony employee Personally Identifiable Information (PII). The breach occurred in April 2023 and was not disclosed until September 21, 2023. The leaked information includes names, phone numbers, and addresses of employees. The breach was allegedly executed by 'Doubl' and the leaked information was disseminated by 'Emo'."}
```

Yesterday, 07:18 PM #1

Hello. Sony has been breached by ransomedvc: details from the group:
Sony Group Corporation, formerly Tokyo Telecommunications Engineering Corporation, and Sony Corporation, is a Japanese multinational conglomerate corporation headquartered in Minato, Tokyo, Japan. We have successfully compromised all of sony systems. We are strictly going to follow them to pay the digital tax, or else the data will simply be sold. We are sharing a minimalist sample so we can make sure both parties are ok.

File tree: link
Sample Of Data: link
link to post:

RANSOMEDVC

We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!

News: SONY.com data and access for sale

NOTICE: Downtime has been resolved, very sorry! PS: We need affiliates :))

[Join Our Affiliate Program](#)

SONY.COM / Post Date: 28.9.2023

Revenue: \$88,000,000,000 (\$88b)

- Sony Group Corporation, formerly Tokyo Telecommunications Engineering Corporation, and Sony Corporation, is a Japanese multinational conglomerate corporation headquartered in Minato, Tokyo, Japan

We have successfully compromised all of sony systems. We won't ransom them! we will sell the data, due to sony not wanting to

<https://twitter.com/troyhunt/status/1706286479100817847>
<https://twitter.com/vxunderground/status/1705042920137425171>

A significant data breach has been reported involving the leak of T-Mobile employee Personally Identifiable Information (PII), marking the second such incident this year. The breach, which occurred in April 2023, was not disclosed until September 21, 2023. The individuals allegedly responsible for the breach and the subsequent leak are known as "Doubl" and "Emo," respectively. The leaked information, now publicly available on BreachForum, is being disseminated widely across various platforms, including Telegram and Discord. This incident underscores the critical importance of robust data security measures and timely breach disclosure to protect sensitive employee information.

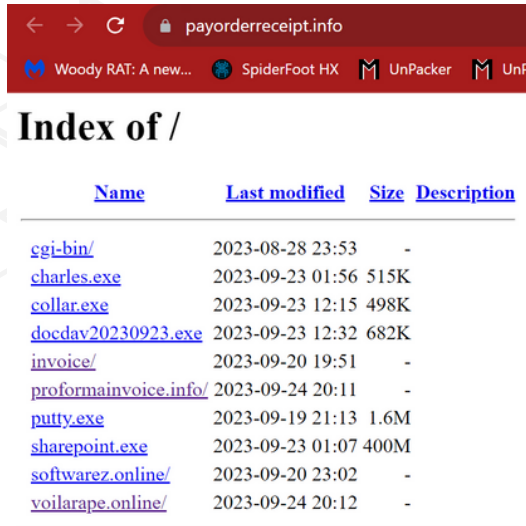
Detailed Information

The breach was executed by "Doubl" and the leaked information was disseminated by "Emo." The exact details of the breach methodology are not known, but the delay in the leak suggests a possible period of data exploitation or sale in underground markets before public release. The leaked data is extensive, encompassing multiple databases, and the exact extent of the information leaked is still being ascertained. Preliminary reports suggest that the data is substantial and sensitive, warranting immediate attention and mitigation efforts to protect the affected individuals.

In light of the T-Mobile breach, organizations must prioritize the security of both customer and employee data. The alleged data breach at Sony further emphasizes the growing cybersecurity threats facing corporations. While details about the Sony breach are still emerging, it is crucial for Sony to conduct a swift and thorough investigation, notify affected parties, and take appropriate measures to mitigate the impact. Continuous monitoring, robust cybersecurity infrastructure, and adherence to best security practices are paramount in protecting organizational and personal data from breaches and leaks.



Malware Distribution Sites



payorderreceipt.info

Woody RAT: A new... SpiderFoot HX UnPacker UnP

Index of /

Name	Last modified	Size	Description
cgi-bin/	2023-08-28 23:53	-	
charles.exe	2023-09-23 01:56	515K	
collar.exe	2023-09-23 12:15	498K	
docdav20230923.exe	2023-09-23 12:32	682K	
invoice/	2023-09-20 19:51	-	
proformainvoice.info/	2023-09-24 20:11	-	
putty.exe	2023-09-19 21:13	1.6M	
sharepoint.exe	2023-09-23 01:07	400M	
softwarez.online/	2023-09-20 23:02	-	
voilarape.online/	2023-09-24 20:12	-	



product-secured.com

Woody RAT: A new... SpiderFoot HX UnPacker UnP

Index of /

Name	Last modified	Size	Description
agimoney/	2023-09-19 21:08	-	
blackorangeweb/	2023-09-19 21:09	-	
cgi-bin/	2023-07-12 12:31	-	
chibaike/	2023-09-19 21:10	-	
dadsrosats/	2023-09-19 21:09	-	
davidnew/	2023-09-24 22:16	-	
dcross/	2023-09-19 21:07	-	
freededen/	2023-09-22 01:54	-	
guruf40/	2023-09-19 21:05	-	
head/	2023-09-19 16:40	-	
huslandflow/	2023-09-24 22:16	-	
javalux/	2023-09-19 21:11	-	
john/	2023-09-19 21:08	-	
josig/	2023-09-20 21:31	-	
menase/	2023-09-19 21:07	-	
numtrade/	2023-09-19 21:00	-	
nax/	2023-09-19 21:06	-	
oyas/	2023-09-19 21:06	-	
paulwhite01/	2023-09-19 21:10	-	
stargaz247/	2023-09-19 21:11	-	
trusplus/	2023-09-19 21:12	-	
unknownp/	2023-09-19 21:11	-	
youngkid/	2023-09-19 21:12	-	
yayoben85/	2023-09-19 21:05	-	
zoth.comway/	2023-09-19 21:04	-	

<https://twitter.com/Gi7wOrm/status/1706061724099457411>

A malicious infrastructure has been identified, hosting XWorm and SnakeKeylogger malware. The staging server and command and control servers (C2s) associated with XWorm, as well as an FTP server associated with SnakeKeylogger, have been spotted. The pattern aligns with the known cybercriminal group, DDGroup. Organizations are advised to take immediate action to block access to the identified malicious domains and servers and scan their networks for indicators of compromise.

Details of the Malware Infrastructure

- **Staging Server:** payorderreceipt[.]info
- **Malware Types:** XWorm and SnakeKeylogger
- **XWorm C2s:**
 - xwormfresh[.]duckdns[.]org:7002
 - homesafe1000[.]duckdns[.]org:7000
- **SnakeKeylogger FTP Server:** ftp://ftp.product-secured[.]com/
- **Associated Group:** DDGroup

Impact

- **XWorm:** Can allow unauthorized access and control over infected systems.
- **SnakeKeylogger:** Can record and transmit sensitive information, including login credentials and personal information.

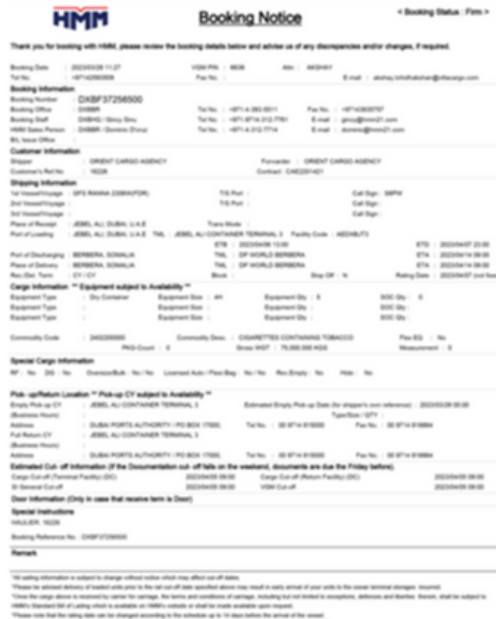
YARA Rule for Detection

Below is a basic YARA rule for detecting the presence of XWorm and SnakeKeylogger. This rule should be customized and enhanced for more effective detection.

```
rule XWorm_SnakeKeylogger_Detection {
  meta:
    description = "YARA Rule for XWorm and SnakeKeylogger Detection"
    author = "Your Organization"
    date = "2023-09-26"
  strings:
    $xworm1 = "xwormfresh[.]duckdns[.]org:7002"
    $xworm2 = "homesafe1000[.]duckdns[.]org:7000"
    $snakekeylogger = "ftp.product-secured[.]com"
  condition:
    any of them
}
```



ProxyLife



<https://twitter.com/jaydinbas/status/1706289240781308236>

This advisory report provides a comprehensive technical analysis of a malicious file named "Passport and KYC Documents[.zip]," identified by its hash on VirusTotal. The malware follows a sophisticated execution chain: LNK -> PowerShell -> Dropbox -> Delphi RunPE -> UPX -> unknown C++ malware, and is suspected to communicate with a Command and Control (C2) server at macores[.]com (192.71.249[.]198). The malware employs various evasion and obfuscation techniques, making detection and analysis challenging.

Technical Details

Malware Execution Chain:

1. **LNK File:** The attack begins with an LNK file contained within the zip archive, which, when executed, triggers a PowerShell script.
2. **PowerShell Script:** The PowerShell script fetches a malicious payload hosted on Dropbox.
3. **Delphi RunPE:** The downloaded payload is a Delphi RunPE executable that performs process hollowing to inject malicious code into legitimate processes.
4. **UPX Packed Payload:** The injected code is UPX packed, further obfuscating the final payload.
5. **Unknown C++ Malware:** The final payload is an unknown C++ malware, which is executed in the context of the hollowed process.

C2 Communication:

- **C2 Server:** The malware likely communicates with a C2 server hosted at macores[.]com (192.71.249[.]198).
- **Data Exfiltration:** The malware may exfiltrate sensitive data to the C2 server, further compromising the security of the infected system.

Evasion Techniques:

- **Decoy Website:** The malware uses a decoy website (<http://hmm21.com>) and a Lion King-esque picture to distract and mislead the victim, making it appear benign.
- **Obfuscation:** The use of UPX packing and process hollowing makes it difficult to analyze the malware and determine its true functionality.



TTP Analysis

The report from WeLiveSecurity provides an in-depth analysis of the cyber-espionage group, Stealth Falcon, and their latest campaign utilizing the DeadGlyph malware to target entities in the Middle East. Stealth Falcon, known for its sophisticated cyber-espionage tactics, has been actively deploying DeadGlyph, a custom backdoor, to compromise systems and exfiltrate sensitive information. The group's operations are characterized by meticulous planning, the use of previously unseen malware, and a clear focus on specific targets, making their activities a significant concern for cybersecurity in the Middle East.

Technical Details of DeadGlyph

Malware Delivery and Installation:

- **Initial Access:** Stealth Falcon primarily uses spear-phishing emails with malicious attachments or links to compromise their targets.
- **Exploitation:** The group exploits vulnerabilities in software to execute the malware on the victim's system.
- **Installation:** Once executed, DeadGlyph is installed on the system, establishing persistence and ensuring it remains operational even after system reboots.

Malware Capabilities:

- **Command and Control (C2) Communication:** DeadGlyph communicates with a C2 server controlled by Stealth Falcon, sending information and receiving commands.
- **Information Gathering:** The malware is capable of collecting and sending detailed information about the compromised system to the C2 server.
- **Additional Payloads:** DeadGlyph can download and execute additional malware or tools based on commands from the C2 server.
- **Data Exfiltration:** Sensitive data is exfiltrated from the victim's system to the C2 server for further exploitation by Stealth Falcon.

Evasion Techniques:

- **Obfuscation:** DeadGlyph employs obfuscation techniques to avoid detection by antivirus solutions.
- **Limited Footprint:** The malware operates with a minimal footprint, reducing the likelihood of detection by system monitoring tools.

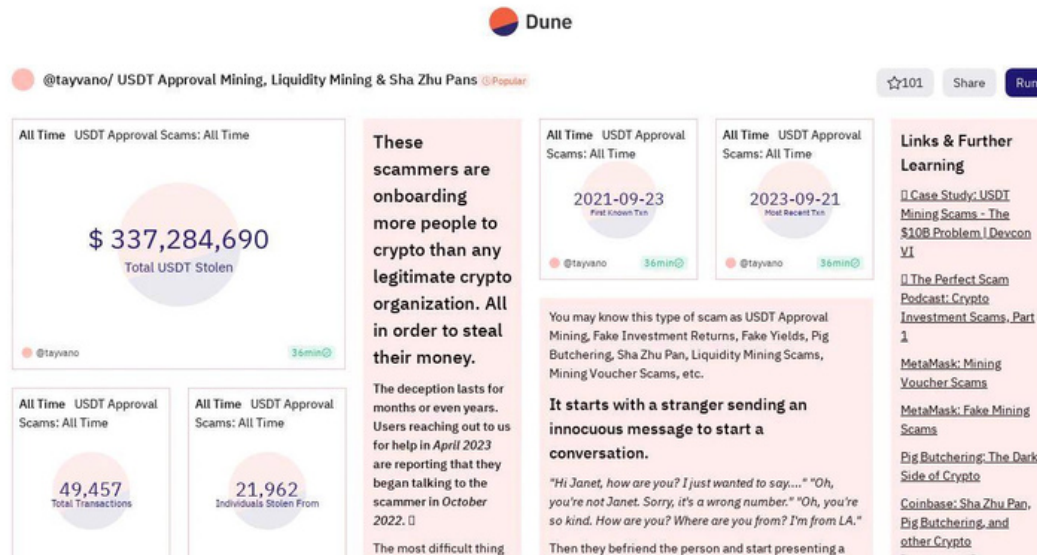
Stealth Falcon Tactics, Techniques, and Procedures (TTPs)

Stealth Falcon's operations demonstrate a high level of sophistication and coordination:

- **Targeted Attacks:** The group conducts highly targeted attacks, focusing on specific individuals or organizations in the Middle East.
- **Spear-Phishing:** Stealth Falcon utilizes spear-phishing as a primary attack vector, crafting convincing emails to lure victims into executing the malware.
- **Custom Malware:** The use of custom malware like DeadGlyph, which is not widely recognized by antivirus solutions, enhances the group's ability to compromise systems undetected.
- **Persistent Operations:** Stealth Falcon operates persistently, continuously evolving their tactics and tools to maintain access to compromised systems and networks.



Scam Contract



<https://dune.com/tayvano/sha-zhu-pan>

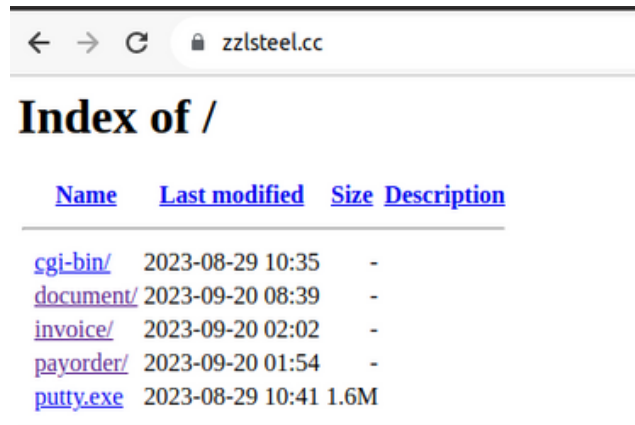
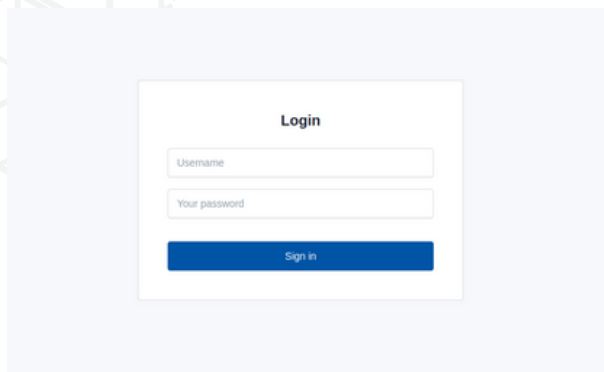
The dashboard on Dune, titled "sha-zhu-pan" by Tayvano, highlights a critical and growing issue in the cryptocurrency space: the proliferation of scams that are effectively onboarding more individuals to crypto than legitimate organizations, only to defraud them of their investments. The scammers operate by building trust with individuals over extended periods, sometimes months or even years, guiding them through the process of investing in cryptocurrency, and then exploiting this trust to steal their funds.

The Scam Operation

The scammers initiate contact with potential victims and gradually build a relationship of trust. Users who reached out for help in April 2023 reported that they had been in contact with the scammers since October 2022. This long con allows the scammers to guide the victims through the process of purchasing and investing in cryptocurrency, all the while setting the stage for the eventual fraud. The victims, believing they are making legitimate investments, willingly and happily follow the instructions of the scammers, visiting fraudulent websites, approving interactions, and sending transactions, unaware of the deception.



Opendir



← → ↻ 🔒 zzlsteel.cc

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
cgi-bin/	2023-08-29 10:35	-	
document/	2023-09-20 08:39	-	
invoice/	2023-09-20 02:02	-	
payorder/	2023-09-20 01:54	-	
putty.exe	2023-08-29 10:41	1.6M	

<https://twitter.com/ViriBack/status/1705735976478191712>

This advisory report outlines the critical information regarding a malware distribution site, zzlsteel[.]cc, which is notably serving the OriginBotnet and XKeyBot malware. These malicious software variants are known to communicate with a Command and Control (C2) server located at nitroso软wares[.]shop. Both domains, along with other C2 servers, are registered with Namecheap, highlighting a potential security concern related to the domain registration service. Immediate attention and action are required to mitigate the risks associated with this malware distribution and control infrastructure.

Malware Distribution:

- **Domain:** zzlsteel[.]cc
- **Malware Types:** OriginBotnet, XKeyBot
- **Delivery Method:** The exact delivery method is unknown, but users visiting the site may inadvertently download and execute the malware on their systems.

Command and Control Servers:

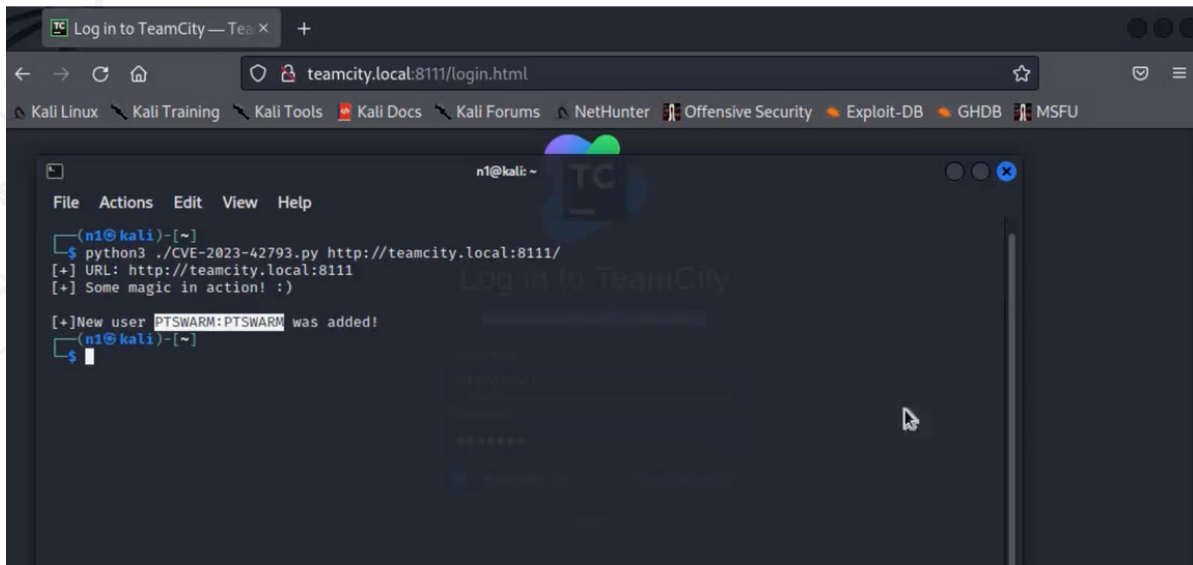
- **Primary C2:** nitroso软wares[.]shop
- **Additional C2 Servers:**
 - ltm-canada[.]com/login/
 - turinapparrels[.]com/login/
- **Registration:** All domains are registered via Namecheap.

Malware Functionality:

- **OriginBotnet / XKeyBot:** These malware types are botnets that can provide the attacker with unauthorized control over the infected systems.
- **Communication:** The malware communicates with the C2 servers, receiving instructions and potentially downloading additional payloads.



1Day



A critical authentication bypass vulnerability, CVE-2023-42793, has been disclosed in JetBrains TeamCity CI/CD servers. This vulnerability allows an unauthenticated attacker with HTTP(S) access to perform a remote code execution attack and gain administrative control of the server, posing a significant threat as a potential supply chain attack vector. Immediate action is required to mitigate this vulnerability.

Details of the Vulnerability

- Vulnerability: Authentication Bypass leading to Remote Code Execution
- CVE ID: CVE-2023-42793
- Severity: Critical
- Affected Product: On-premises instances of JetBrains TeamCity CI/CD server
- Impact: Unauthorized administrative control, potential for supply chain attacks

Exploitation

As of September 25, 2023, there is no known in-the-wild exploitation or public exploit code available for CVE-2023-42793. However, the potential impact of successful exploitation is significant, warranting urgent attention and mitigation.

Affected Versions

CVE-2023-42793 affects all on-prem versions of JetBrains TeamCity prior to 2023.05.4. TeamCity Cloud is not affected.

Mitigation Guidance

- **Upgrade to Fixed Version:** Upgrade to TeamCity version 2023.05.4 immediately to resolve the vulnerability.
- **Apply Security Patch Plugins:** If unable to upgrade, apply vulnerability-specific security patch plugins as a temporary workaround. These plugins are supported on TeamCity 8.0+ and will mitigate CVE-2023-42793 specifically.
 - TeamCity 2018.2 to 2023.05.3
 - TeamCity 8.0 to 2018.1
- **Server Restart:** For TeamCity versions older than 2019.2, a server restart is required after the plugin has been installed.
- **Consider Taking Server Offline:** If unable to upgrade or apply a patch, consider taking the server offline until the vulnerability can be mitigated.





Trending Exploit

A critical unauthenticated remote code execution (RCE) vulnerability has been discovered in Juniper SRX firewalls and EX switches, affecting an estimated 12,000 devices. Despite initially being rated as medium severity, the vulnerability (CVE-2023-36845) has been proven to allow remote code execution without authentication, posing a significant threat to affected systems. Immediate action is required to mitigate the risk.

Details of the Vulnerability

- Vulnerability: Fileless Remote Code Execution Flaw
- CVE IDs: CVE-2023-36844/CVE-2023-36845/CVE-2023-36846/CVE-2023-36847
- Severity: Critical (9.8)
- Affected Devices: Juniper SRX firewalls and EX switches
- Impact: Unauthorized remote code execution, potential unauthorized access to corporate networks

Exploitation

Researchers have released proof-of-concept (PoC) exploits demonstrating the vulnerability's exploitability. The exploit allows attackers to remotely execute arbitrary code without authentication by manipulating environment variables and utilizing PHP's features.

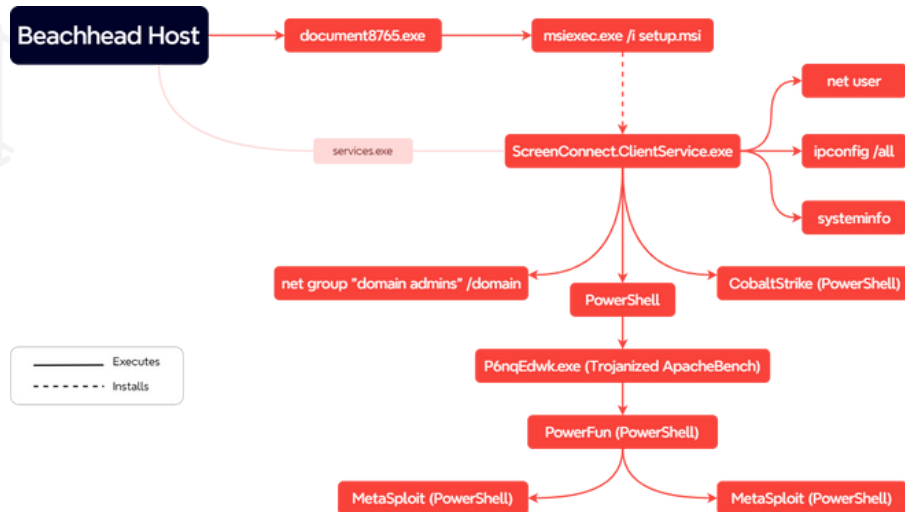
Affected Versions

The vulnerability impacts the following versions of Junos OS on EX Series and SRX Series:

- All versions before 20.4R3-S8
- 21.1 version 21.1R1 and later versions
- 21.2 versions before 21.2R3-S6
- 21.3 versions before 21.3R3-S5
- 21.4 versions before 21.4R3-S5
- 22.1 versions before 22.1R3-S3
- 22.2 versions before 22.2R3-S2
- 22.3 versions before 22.3R2-S2, 22.3R3
- 22.4 versions before 22.4R2-S1, 22.4R3



The Topic of the Week



<https://thedfirreport.com/2023/09/25/from-screenconnect-to-hive-ransomware-in-61-hours/>

The detailed report from The DFIR Report, published on September 25, 2023, offers an in-depth examination of a cyberattack that culminated in the deployment of Hive Ransomware within a mere 61 hours. The attackers exploited ScreenConnect, a widely used remote access tool, to infiltrate the victim's network. This case study highlights the speed and efficiency with which cybercriminals can operate, leveraging legitimate tools to bypass security measures and execute their attack swiftly and stealthily.

Attack Progression

Upon gaining access via ScreenConnect, the attackers quickly escalated their privileges, demonstrating a comprehensive understanding of the network's vulnerabilities. The use of Cobalt Strike, a legitimate penetration testing tool, further aided their malicious activities, allowing them to traverse the network undetected. The attackers' adeptness in utilizing these tools underscores the challenge organizations face in differentiating between legitimate and malicious activities within their networks. The rapid lateral movement and privilege escalation led to the successful deployment of Hive Ransomware, leaving the victim with encrypted files and a ransom demand.

Tactics and Techniques

The attackers exhibited a range of sophisticated tactics and techniques throughout the attack. Their initial exploitation of ScreenConnect, a tool typically used for legitimate remote access, highlights the trend of cybercriminals leveraging legitimate tools to avoid detection. The subsequent use of Cobalt Strike allowed them to further navigate the network, likely exploiting unpatched vulnerabilities and weak security configurations to escalate privileges and move laterally. The final deployment of Hive Ransomware encrypted the victim's files, rendering them inaccessible and culminating in a ransom demand for decryption keys.





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