

Threat Intel Roundup: WebKit, Akira, Kimsuky

Week in Overview(28 Nov-5 Dec)



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

WebKit Vulnerabilities CVE-2023-42916 and CVE-2023-42917

- **CVE-2023-42916:** An out-of-bounds read in WebKit, potentially leading to sensitive information disclosure. Addressed with improved input validation.
- **CVE-2023-42917:** A memory corruption issue in WebKit, potentially leading to arbitrary code execution. Addressed with improved locking.
- **Affected Products:** iOS, iPadOS, macOS, Safari.
- **Patch Availability:** Updates released in iOS 17.1.2, iPadOS 17.1.2, macOS 14.1.2, Safari 17.1.2.

2. APT Patchwork Cyber Attack Campaign

- **Attack Vector:** Utilizes a malicious PDF document link and a secondary payload hosted on a compromised CDN.
- **Key Components:** Involves a disguised shortcut file and executable payloads downloaded from a CDN.
- **C2 Server:** kungkao[.]online used for command and control.

3. D-Link D-View Coreservice_Action_Script RCE Vulnerability (CVE-2023-44414)

- **Vulnerability:** Remote Code Execution in D-Link D-View.
- **Impact:** Allows unauthenticated remote attackers to execute arbitrary code.
- **Severity:** CVSS score of 9.8 (Critical).

4. OwnCloud CVE-2023-49103

- **Vulnerability:** Affects OwnCloud software.
- **Impact:** Potential for remote, unauthenticated attackers to execute arbitrary code.
- **Severity Assessment:** While numerous IP addresses are exposed, the actual severity is limited to a smaller subset.

5. KQL Queries for Tracking CISA Known Exploited Vulnerabilities

- **Purpose:** Enhance tracking and management of vulnerabilities listed by CISA.
- **Queries Developed:** ListCISAEexploitedVulnerabilities(), New Active CISA Known Exploited Vulnerability Detected, Due Date Passed CISA Known Exploited Vulnerabilities.

6. Report on "State of Cloud Security" by Datadog

- **Focus:** Analysis of security posture of organizations using AWS, Azure, or Google Cloud.
- **Key Findings:** Issues with long-lived credentials, insufficient MFA enforcement, IMDSv2 adoption, and over-privileged workloads.
- **Mitigation Strategies:** Restrict interaction with the application, apply patches, and monitor network traffic.

7. "Your #Booking Admin Account #violates our partnership terms" Malware Campaign

- **Attack Method:** Phishing emails with malicious attachments and links.
- **Impact:** Targets users with a deceptive message leading to malware installation.
- **Mitigation:** Educate users, use endpoint protection, and monitor network traffic.

8. Report on Akira Ransomware Intrusion Set and CERT Intrinsec's Recommendations

- **Intrusion Set:** Analysis of Akira ransomware's tactics, techniques, and procedures.
- **Recommendations:** Include patch management, multi-factor authentication, and network monitoring.

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:

- WebKit Vulnerabilities CVE-2023-42916 and CVE-2023-42917
- APT Patchwork Cyber Attack Campaign
- D-Link D-View Coreservice_Action_Script Remote Code Execution Vulnerability (CVE-2023-44414)
- OwnCloud CVE-2023-49103
- KQL Queries for Tracking CISA Known Exploited Vulnerabilities
- Report on "State of Cloud Security" by Datadog
- "Your #Booking Admin Account #violates our partnership terms" Malware Campaign
- Report on Akira Ransomware Intrusion Set and CERT Intrinsec's Recommendations



Vulnerability of the Week

WebKit CVE-2023-42916

Two significant vulnerabilities were identified in WebKit, the browser engine used by Apple's Safari, affecting iOS, iPadOS, macOS, and Safari versions. These vulnerabilities are tracked as CVE-2023-42916 and CVE-2023-42917.

CVE-2023-42916: Sensitive Information Disclosure

- **Impact:** Processing web content may disclose sensitive information due to an out-of-bounds read.
- **Affected Products:** iOS 17.1.2, iPadOS 17.1.2, macOS 14.1.2, Safari 17.1.2.
- **Description:** This vulnerability was addressed with improved input validation. Apple acknowledged that this issue might have been exploited against versions of iOS before iOS 16.7.1.
- **Reporter:** Clément Lecigne of Google's Threat Analysis Group.
- **WebKit Bugzilla Link:** [265041](#)
- **Apple Support Links:** [iOS and iPadOS](#), [macOS](#), [Safari](#)

CVE-2023-42917: Arbitrary Code Execution

- **Impact:** Processing web content may lead to arbitrary code execution due to memory corruption.
- **Affected Products:** iOS 17.1.2, iPadOS 17.1.2, macOS 14.1.2, Safari 17.1.2.
- **Description:** This vulnerability was addressed with improved locking. Apple is aware of reports that this issue may have been exploited against versions of iOS before iOS 16.7.1.
- **Reporter:** Clément Lecigne of Google's Threat Analysis Group.
- **WebKit Bugzilla Link:** [265067](#)
- **Apple Support Links:** [iOS and iPadOS](#), [macOS](#), [Safari](#)

Mitigation and Updates

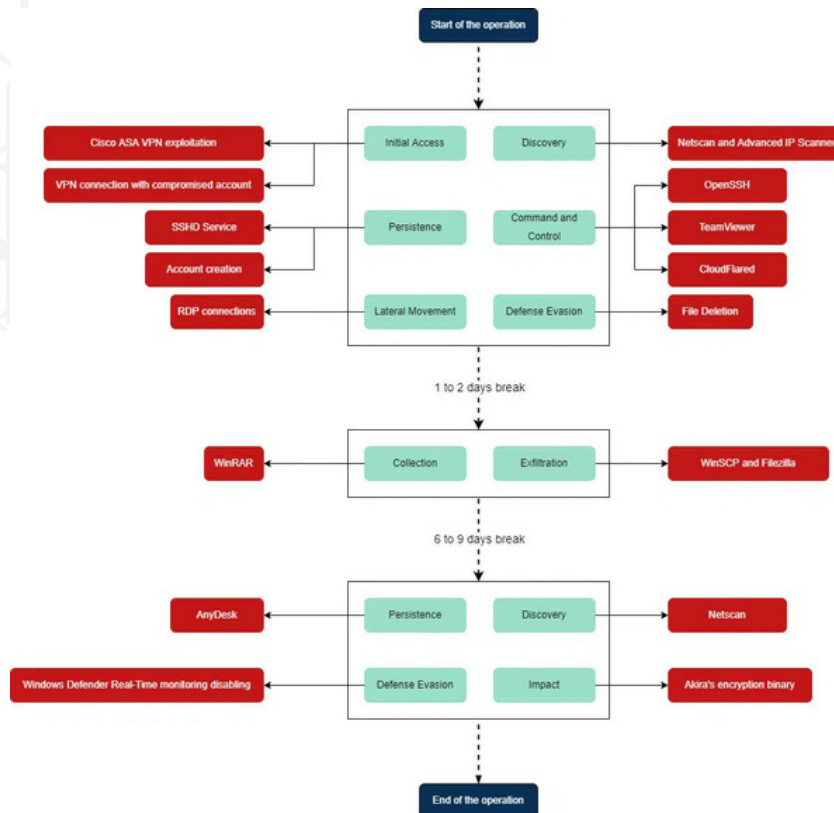
Apple has released updates to mitigate these vulnerabilities in the following versions:

- **iOS 17.1.2 and iPadOS 17.1.2:** [Support Link](#)
- **macOS 14.1.2:** [Support Link](#)
- **Safari 17.1.2:** [Support Link](#)

Users of affected Apple products are advised to update to these versions to protect against potential exploitation of these vulnerabilities.



Malware or Ransomware



<https://twitter.com/virusbtn/status/1731624888949948647>

In the first half of 2023, CERT Intrinsic encountered several incidents involving the Akira ransomware group. Companies became aware of the ransomware either through security alerts or by discovering encrypted files on their servers. CERT Intrinsic's analysis revealed that Akira's attacks were executed in three distinct phases.

CERT Intrinsic's Role

CERT Intrinsic, a French incident response team, primarily operates in France and handles about 50 major incidents annually. They specialize in responding to security breaches involving cybercriminality and ransomware attacks. CERT Intrinsic is certified by ANSSI as a State-Certified Security Incident Response Service Provider.

Akira Ransomware Characteristics

- **Operations Start:** March 2023
- **Targets:** Over 140 organizations across various sectors
- **Techniques:** Similar to Conti ransomware and other RaaS actors, including LSASS dumping, creation of schedule tasks, and use of tools like PCHunter64 or Advanced IP Scanner.
- **Encryption Strategy:** Deletes volume shadow copies, targets specific file extensions, and skips system files directories.
- **Victimology:** Predominantly in the USA (73%), followed by the UK and Canada. Targets include manufacturing, education, construction, retail, and consulting sectors.

Attack Phases

1. **Initial Infiltration:** Utilizing stolen passwords or exploiting vulnerabilities (e.g., CVE-2023-20269 in Cisco ASA and FTD), followed by network discovery and establishing persistence.
2. **Stealth and Preparation:** Data study and technical assessment.
3. **Active Encryption:** Setting up final persistence points, disabling protections, attempting to destroy backups, and executing the encryption binary.

Tactics, Techniques, and Procedures (TTPs)

- **Initial Access:** Compromised credentials, VPN sessions, and exploitation of vulnerabilities.
- **Execution:** Use of PowerShell, Windows Command Shell, and WMI for various tasks.
- **Persistence:** Creation of local and domain accounts, use of remote administration tools.
- **Privilege Escalation:** Compromising privileged accounts.
- **Defense Evasion:** Disabling or modifying system defenses, deleting evidence.
- **Discovery:** Network scanning and information gathering.
- **Lateral Movement:** Use of Remote Desktop Protocol and administrative shares for movement across the network.
- **Collection:** Archiving collected data for efficiency.
- **Command and Control:** Utilizing remote access software and file sharing services.
- **Exfiltration:** Using software like WinSCP and FileZilla for data exfiltration.
- **Impact:** Data destruction, encryption for impact, and inhibiting system recovery.

Malware Distribution Sites

Tax Reductions, Rebates and Credits



To be a modern, progressive, effective, autonomous and credible organization for optimizing revenue by providing quality service and promoting compliance with tax and related laws

Our Mission

Enhance the capability of the tax system to collect due taxes through application of modern techniques, providing taxpayer assistance and by creating a motivated, satisfied, dedicated and professional workforce

Our Values

*Integrity
Professionalism
Teamwork
Courtesy
Fairness
Transparency
Responsiveness*

*For assistance and information on tax matters
Please contact our help line center through Telephone:
National 051-111-772-772
International 0092051-111-772-772
E-mail helpline@fbr.gov.pk*

*or
Visit our tax facilitation center (located in all major cities) or any Regional Tax Office
or
Visit our website at www.fbr.gov.pk*

https://twitter.com/ginkgo_g/status/1731870687562752375

The Advanced Persistent Threat (APT) group known as "Patchwork," primarily associated with activities in Pakistan, has been observed deploying a new cyber attack campaign. This campaign involves the use of a malicious PDF document link and a secondary payload hosted on a compromised content delivery network (CDN).

Attack Details

1. Initial Attack Vector

- The attack initiates with a file named `Tax_Deduction_Revised_Q1-2024.pdf.lnk`, which is a disguised shortcut file (MD5: 218d85723396dddaf75fc5853338997).
- The file masquerades as a legitimate PDF document related to tax deduction, likely targeting individuals or entities interested in financial documents.

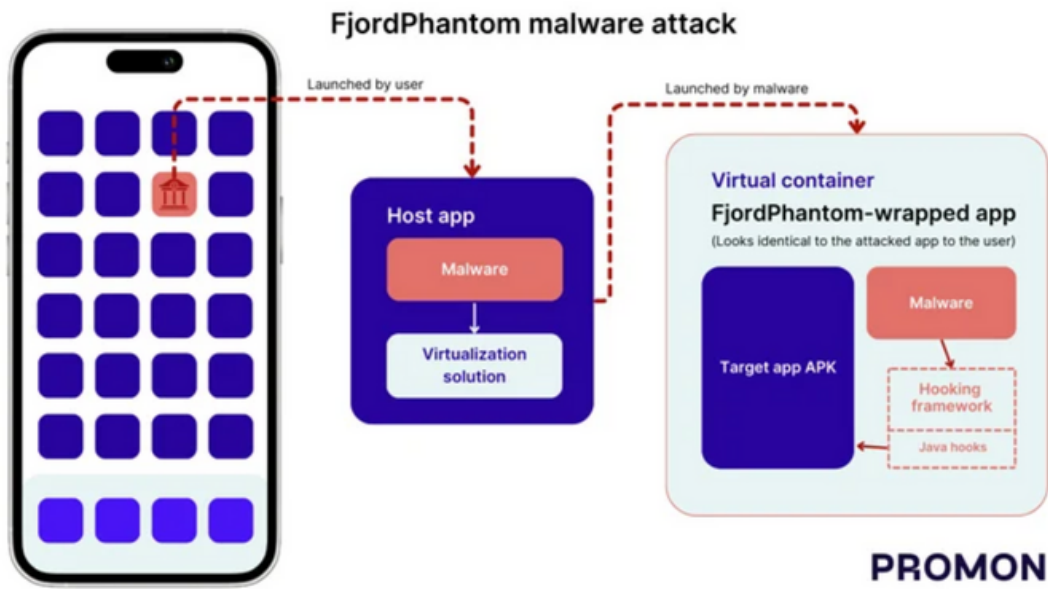
2. Malicious URLs and Payloads

- The first stage of the attack involves downloading a file from `hxxps://tyfk1.b-cdn.net/dox`, which is saved as `Tax_Deduction_Revised_Q1-2024.pdf` in the `C:\Users\Public` directory. This file is likely a decoy to maintain the appearance of legitimacy.
- The second stage involves downloading an executable from `hxxps://tyfk1.b-cdn.net/dix`, which is saved as `Services.exe` in the `C:\Windows\Tasks` directory (MD5: 6582a4df50948aaf2dcfbc6d8b84a58e). This executable is a malicious payload, potentially a backdoor or other form of malware.

3. Command and Control (C2) Server

- The campaign utilizes `kungkao[.]online` as a command and control server. This server is likely used for exfiltrating data, receiving commands, or downloading additional payloads.

Mobile Malware



<https://thehackernews.com/2023/11/malicious-apps-disguised-as-banks-and.html>

A new sophisticated Android malware, named FjordPhantom, has been identified by cybersecurity researchers. This malware has been actively targeting users in Southeast Asian countries, including Indonesia, Thailand, and Vietnam, since early September 2023.

Method of Spread: FjordPhantom is primarily disseminated through messaging services, including email, SMS, and various messaging apps. The malware lures victims into downloading a counterfeit banking app, which, while containing legitimate features, also harbors malicious components.

Social Engineering Technique: The malware employs a social engineering strategy similar to telephone-oriented attack delivery (TOAD). Victims are duped into calling a fake call center, where they are guided through the process of setting up and using the fraudulent app.

Technical Details: A notable feature of FjordPhantom is its use of virtualization to execute malicious code within a container, thereby evading Android's sandbox protections. This technique allows the malware to access sensitive data without needing root access. The malware operates by loading the legitimate banking app in a virtual container, simultaneously employing a hooking framework to manipulate key APIs. This allows it to capture sensitive information from the application's screen and suppress warning dialogs about malicious activities.

Response from Google: In response to the threat, a Google spokesperson highlighted the role of Google Play Protect in safeguarding users. This system can warn against or block apps exhibiting malicious behavior, even those installed from outside the Google Play Store.

Modularity of the Malware: According to security researcher Benjamin Adolphi, FjordPhantom is modular, meaning it can be tailored to attack various banking apps depending on the specific app embedded within the malware.



Art of Detection



<https://twitter.com/BertJanCyber/status/1731748206118117608>

Bert-JanP has developed a set of KQL (Kusto Query Language) queries to enhance the tracking and management of vulnerabilities listed by CISA (Cybersecurity and Infrastructure Security Agency) as known exploited vulnerabilities. These queries are designed for use with platforms like Microsoft Defender for Endpoint and Azure Sentinel.

Queries Developed

1. **ListCISAExploitedVulnerabilities()**

- This query is designed to list all the vulnerabilities identified by CISA as exploited.
- [GitHub Link](#)

2. **New Active CISA Known Exploited Vulnerability Detected**

- This query helps in detecting newly active vulnerabilities that CISA has recently added to its list of known exploited vulnerabilities.
- [GitHub Link](#)

3. **Due Date Passed CISA Known Exploited Vulnerabilities**

- This query is used to identify vulnerabilities from CISA's list where the recommended patch or mitigation due date has passed.
- [GitHub Link](#)

Importance of These Queries

These KQL queries are crucial for cybersecurity teams to:

- Stay updated with the latest vulnerabilities identified by CISA.
- Quickly respond to new threats by identifying newly listed exploited vulnerabilities.
- Ensure compliance and security by tracking vulnerabilities that have passed their mitigation due dates.

Application

The queries can be integrated into security monitoring systems that support KQL, such as Microsoft Defender for Endpoint and Azure Sentinel. They enable organizations to proactively manage their security posture by aligning with CISA's advisories and recommendations.



Proxylife

Booking.com

Your account violates Partnership Agreement

Dear Partner,

We have noticed that your account has repeatedly violated the terms of the Booking.com partnership agreement. We regret to inform you that if you do not rectify all violations, your account will be permanently blocked with no possibility of reactivation. You must access the Extranet through the special link provided in this email. The link will only be available for 24 hours.

To access the list of your violations, please click on "Show Violations" within this email. Afterward, open a secured archive, where you will find a comprehensive list of the violations associated with your account.

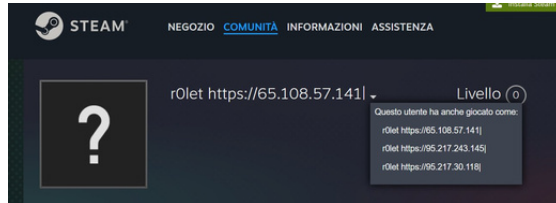
Accessing key:
457697

If you have any questions, visit our dedicated Partner Help page.

Thanks for your mentions!
 Best regards,
 Booking Control Team

[Show Violations](#)

Copyright © 1996-2023 Booking.com B.V. All rights reserved. This email was sent by Booking.com B.V., Haringvliet 597, 1017 CE Amsterdam, Netherlands.



STEAM

NEGOZIO COMUNITÀ INFORMAZIONI ASSISTENZA

r0let <https://65.108.57.141> Livello 0

Questo utente ha anche giocato come:

- r0let <https://65.108.57.141>
- r0let <https://95.217.243.145>
- r0let <https://95.217.30.118>

Malware URLs

The table below shows all malware URLs that are associated with this particular tag (max 1000).

Show: 50 entries Search:

Dateadded (UTC)	URL	Status	Tags	Reporter
2023-12-05 04:48:09	https://drive.google.com/uc?export=download&confirm=no_an...	Online	bookinggoogledrive (pw=457697)	JAMESWT_MHT

Malware URLs

The table below shows all malware URLs that are associated with this particular tag (max 1000).

Show: 50 entries Search:

Dateadded (UTC)	URL	Status	Tags	Reporter
2023-12-05 04:48:09	https://drive.google.com/uc?export=download&confirm=no_an...	Online	bookinggoogledrive (pw=457697)	JAMESWT_MHT

https://twitter.com/JAMESWT_MHT/status/1731900205811777939

A recent malware campaign has been identified, targeting users with a deceptive message stating "Your #Booking Admin Account #violates our partnership terms." This campaign involves a multi-stage infection process, leveraging email (EML) files that contain malicious links (LNK), leading to a password-protected Zip file (password: 457697), which ultimately delivers a script (Scr) associated with the Vidar Stealer malware.

Sources Analyzed

- MalwareBazaar Database:** The MalwareBazaar database was accessed for samples related to this campaign, but it required CAPTCHA verification, preventing detailed analysis.
- URLhaus Database:** URLhaus provided an overview of malware URLs tagged with **bookinggoogledrive**. The first sighting of this tag was on September 28, 2023, with the most recent being December 5, 2023, totaling 37 sightings.
- ANY.RUN Analysis:** An interactive analysis of the malicious activity associated with the campaign was conducted on ANY.RUN. However, specific details of this analysis were not accessible due to website restrictions.

Command and Control (C2) Servers

The campaign utilizes several C2 servers for coordinating the attack and exfiltrating data. Identified C2 server IPs include:

- 65.108.57.[141]
- 95.217.243.[145]
- 95.217.30.[18]

Vidar Stealer Malware

Vidar Stealer is a type of malware known for its capabilities to steal sensitive information from infected systems. It typically targets a wide range of data, including but not limited to credentials, browser history, and financial information.



TTP Analysis

The Kimsuky threat group, believed to be backed by North Korea, has been active since 2013, initially focusing on South Korean targets related to North Korea and expanding its scope internationally since 2017. This group primarily targets sectors like national defense, media, diplomacy, and academia, aiming to steal sensitive information and technology. Initially reliant on spear phishing for infiltration, Kimsuky has recently shifted to using LNK (shortcut) malware, which is delivered via spear phishing emails containing compressed files. When these files are decompressed, they reveal both legitimate documents and malicious LNK files.

Infiltration and Malware Tactics:

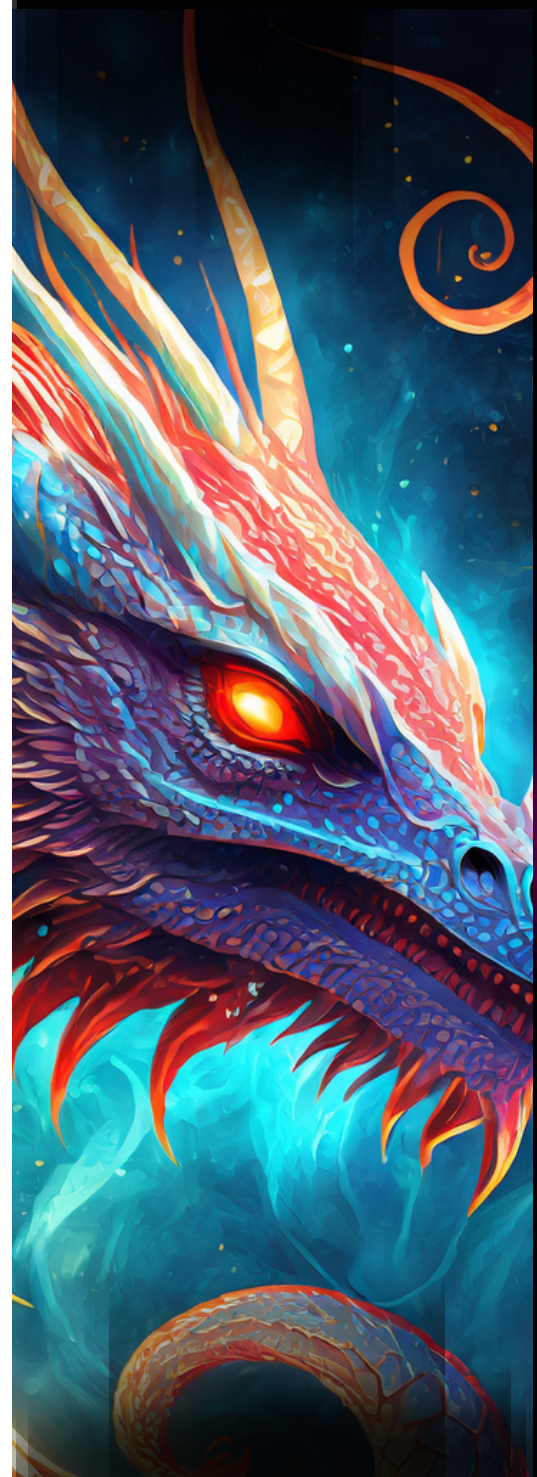
Upon execution, the LNK files release script malware that can steal information and download further payloads. The group has been using a variety of malware, including self-developed ones like AppleSeed and PebbleDash, and others like X RAT, HVNC, Amadey, and Metasploit Meterpreter. These tools enable remote control, keylogging, and data theft. Notably, the group has been using Amadey and RftRAT, which have been adapted using Autolt scripting language, making them harder to detect by security software.

Specific Malware Analysis:

The Kimsuky group's use of X RAT (QuasarRAT) involves encrypted payloads to bypass security measures. This RAT is injected into normal processes for stealthy operation. Amadey, a malware sold on illegal forums, is used for downloading additional malware and stealing information. It is typically installed via a DLL-format dropper, which creates persistence mechanisms and injects the malware into legitimate processes. RftRAT, similar in size and packing to Amadey, is a backdoor malware for executing remote commands.

Conclusion and Recommendations:

The Kimsuky group continues to evolve its cyberattack strategies, now incorporating Autolt to create more elusive malware. They predominantly target South Korean users through spear phishing and LNK malware, emphasizing the need for heightened vigilance. Users are advised to scrutinize email senders, avoid unknown files, and keep their software, including OS and browsers, updated with the latest security patches to mitigate the risk of such attacks.





Scam Contract



<https://cointelegraph.com/news/inferno-drainer-shut-down-after-stealing-millions-crypto-wallet-scam-kit>

A cryptocurrency hacker has successfully executed "address poisoning attacks" on users of Safe Wallet, resulting in the theft of over \$2 million in just one week. The total number of victims has now reached 21, with cumulative losses estimated at around \$5 million over the past four months.

Details of the Attack:

- **Method:** The attacker employs address poisoning, a technique where they create a crypto address resembling the victim's regular transaction addresses, particularly matching the beginning and ending characters.
- **Execution:** The hacker sends a small amount of cryptocurrency from this similar-looking address to the target, thereby "poisoning" their transaction history. When the victim makes a transaction, they might mistakenly send a large amount to the hacker's address.
- **Recent Impact:** According to Scam Sniffer, a Web3 scam detection platform, around ten Safe Wallets lost \$2.05 million since November due to these attacks. One of the victims reportedly had \$10 million in their Safe Wallet but lost \$400,000.

Response and Analysis:

- **Scam Sniffer's Report:** Scam Sniffer has been actively reporting and compiling data on these attacks using Dune Analytics.
- **Safe Wallet's Stance:** As of the report, Cointelegraph has reached out to Safe Wallet for comments, but there has been no response yet.

Conclusion: The address poisoning scam targeting Safe Wallet users highlights a growing concern in the crypto community regarding sophisticated hacking techniques. Users are advised to be extra vigilant with their transaction practices and to double-check addresses before sending funds. The situation is developing, and further updates from Safe Wallet are awaited.



0Day

```
POST /dview8/core/task HTTP/1.1
Host: [target]:17500
Content-Type: application/json
Content-Length: 64

{"taskType":"coreservice_action_script","context":"\\mspaint\\"}
```

<https://twitter.com/steventseeley/status/1731815163613806924>

A critical remote code execution vulnerability, identified as CVE-2023-44414, has been discovered in D-Link's D-View software. This vulnerability has a high severity rating with a CVSS score of 9.8.

Vulnerability Details

- **CVE ID:** CVE-2023-44414
- **CVSS Score:** 9.8 (Critical) - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Affected Vendor:** D-Link
- **Affected Product:** D-View
- **Vulnerability Type:** Remote Code Execution (RCE)

The vulnerability exists within the `coreservice_action_script` action of D-Link D-View. It stems from the exposure of a dangerous function that can be exploited by remote attackers. Notably, this vulnerability does not require authentication, making it particularly severe as it allows unauthenticated remote attackers to execute arbitrary code on affected installations.

The exploitation of this vulnerability can lead to code execution in the context of the SYSTEM, providing attackers with high-level control over the affected system.

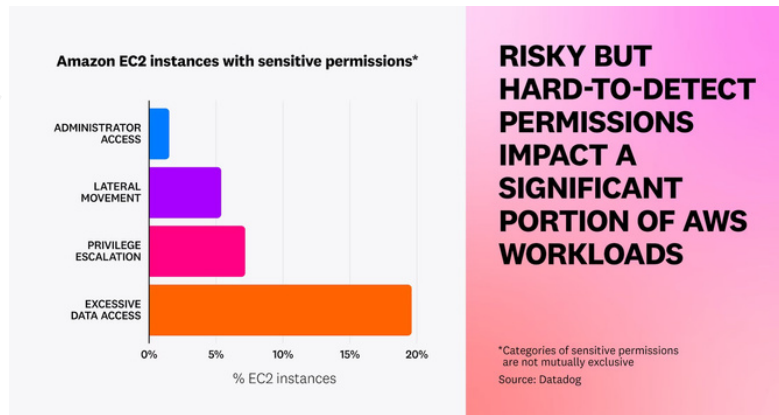
Disclosure Timeline

- **2022-12-23:** The vulnerability was initially reported to the vendor by the Zero Day Initiative (ZDI).
- **2023-08-25:** ZDI requested an update from the vendor.
- **2023-08-30:** The vendor responded, stating they did not have the case on record.
- **2023-08-31:** ZDI forwarded the original report to the vendor.
- **2023-09-29:** ZDI informed the vendor of their intention to publish the advisory as a zero-day on 2023-10-04.
- **2023-10-04:** Coordinated public release of the advisory.





The Topic of the Week



<https://twitter.com/clintgibler/status/1730617923138670856>

Datadog's "State of Cloud Security" report provides an in-depth analysis of the security posture of thousands of organizations using AWS, Azure, or Google Cloud. The report focuses on common risks leading to cloud security incidents and offers insights into areas such as long-lived credentials, multi-factor authentication (MFA), IMDSv2 enforcement, and over-privileged workloads.

Key Findings

1. Long-lived Credentials as a Risk

- Long-lived credentials, which do not expire and can be easily leaked, continue to pose a major security threat.
- In AWS, 76% of IAM users have active access keys, 50% of Azure AD applications have active credentials, and 27% of Google Cloud service accounts have active access keys.
- Approximately half of these access keys are over a year old, indicating a tendency for access keys to live longer than they should.

2. Insufficient Enforcement of MFA

- MFA is crucial for securing cloud identities but is not sufficiently enforced.
- In AWS, 31% of IAM users with console access have no MFA enforced.
- 45% of AWS organizations had IAM users authenticate to the AWS console without using MFA.
- Only 20% of Azure organizations had all Azure AD users authenticate with MFA.

3. IMDSv2 Adoption Rising but Unenforced

- IMDSv2 enforcement in AWS has increased to 21% of EC2 instances, up from 7% in the previous year.
- However, enforcement varies based on the age of deployment, with newer instances more likely to enforce IMDSv2.

4. Increasing Adoption of Public Access Blocks in Cloud Storage

- Public storage buckets are a common source of data leakage.
- 72% of AWS S3 buckets are covered by a public S3 access block, up from 52%.
- 21% of Azure blob storage containers are in accounts that block public access.

5. Excessive Privileges in Cloud Workloads

- A significant portion of cloud workloads have more privileges than necessary.
- In AWS, 23% of EC2 instances have administrator or highly sensitive permissions.
- In Google Cloud, 37% of VMs have sensitive permissions to a project.

6. Public Exposure of Virtual Machines

- 7% of EC2 instances, 3% of Azure VMs, and 13% of Google Cloud VMs are publicly exposed to the internet.
- Commonly exposed ports include HTTP, HTTPS, SSH, and RDP.



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