Threat Intel Roundup: Outlook, SmartScreen, Lockbit

Week in Overview(13 Feb-20 Feb) - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **InfoSec Community Event on Jupyter Notebooks:**
    - The event focused on showcasing the application of Jupyter Notebooks within the InfoSec field.
    - Keynote speeches, presentations, and discussions highlighted various aspects such as threat hunting, data visualization, and building data-driven security tools.
    - Notable topics included red teaming with Jupyter Notebooks, threat hunting workflows, and collaboration methods for security analysis.
    - Attendees gained insights into practical use cases and innovative approaches to leveraging Jupyter Notebooks in security research and operations.
2. **STOP/DJVU Ransomware Campaign Statistics:**
    - Analysis revealed 53,068 unique records of potential STOP/DJVU ransomware installations.
    - The top 10 countries affected by unique installs included the United States, Brazil, and Pakistan, among others.
    - The statistics underscored the global impact of the ransomware campaign and highlighted the urgency of implementing robust cybersecurity measures.
3. **Android Bluetooth Vulnerability (CVE-2023-45866):**
    - CVE-2023-45866 represents a critical security vulnerability affecting Android smartphones.
    - Attackers can exploit the vulnerability to remotely lock out users or trigger data wipes via Bluetooth, potentially resulting in significant data loss.
    - Users are advised to disable Bluetooth when not in use, update their devices to the latest security patches, and avoid connecting to untrusted Bluetooth devices.
4. **Security Advisory Summary Report for CVE-2024-21412:**
    - CVE-2024-21412 is a critical vulnerability discovered in Microsoft Defender SmartScreen.
    - The vulnerability, exploited by advanced threat groups like Water Hydra, allows attackers to bypass security measures and potentially execute arbitrary code.
    - Mitigation strategies include applying security patches, implementing multi-layered security solutions, and enhancing threat intelligence capabilities.
5. **CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC:**
    - This security advisory presents a proof-of-concept (PoC) for CVE-2024-21413, a significant vulnerability in Microsoft Outlook.
    - The vulnerability, with a CVSS score of 9.8, enables remote code execution and poses a severe threat to users' systems.
    - The PoC demonstrates the potential leakage of NTLM information and bypassing of Office Protected View, highlighting the importance of comprehensive email security practices.

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:

- InfoSec Community Event on Jupyter Notebooks
- STOP/DJVU Ransomware Campaign Statistics
- Android Bluetooth Vulnerability (CVE-2023-45866)
- Security Advisory Summary Report for CVE-2024-21412
- CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC

🚨 Vulnerability of the Week

Outlook CVE-2024-21413

The vulnerability, termed the #MonikerLink bug, is assigned CVE-2024-21413 with a CVSS score of 9.8. It allows for remote code execution and potential leakage of local NTLM information. The vulnerability enables attackers to bypass Office Protected View, extending its threat to other Office applications.

Usage: The PoC script facilitates testing responsibly with proper authorization. It utilizes SMTP authentication to send emails, bypassing SPF, DKIM, and DMARC checks, simulating real-world attack scenarios effectively.

Parameters:

- **--server**: SMTP server hostname or IP.
- **--port**: SMTP server port.
- **--username**: SMTP server username for authentication.
- **--password**: SMTP server password for authentication.
- **--sender**: Sender email address.
- **--recipient**: Recipient email address.
- **--url**: Malicious path to include in the email.
- **--subject**: Email subject.

Importance of SMTP Authentication: SMTP authentication is crucial for demonstrating how emails sent bypass common validation checks, mimicking sophisticated attacker techniques. This emphasizes the importance of comprehensive email security practices.

Demos:

- 0-click NTLM Leak
- 1-click Remote Code Execution (RCE)

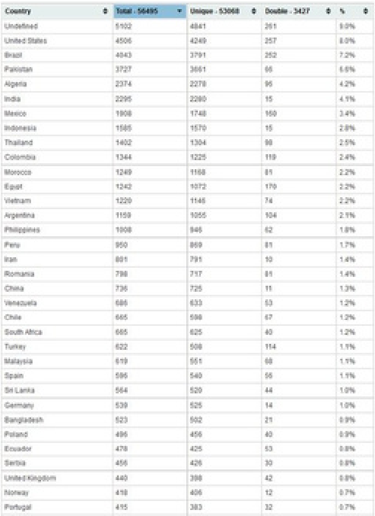
Changelog:

- [19. February 2024]: Added 0-Click NTLM Leak.
- [18. February 2024]: Added 1-click RCE.
- [16. February 2024]: Initial Release.

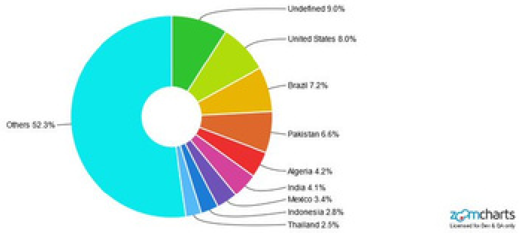
Credits: Checkpoint conducted the research.

https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability
https://twitter.com/xaitax/status/1759318090788037093

Malware or Ransomware



Country	Total - 56495	Unique - 53068	Double - 3427	%
Undefined	5102	4841	261	9.0%
United States	4506	4249	257	8.0%
Brazil	4043	3791	252	7.2%
Pakistan	3727	3661	66	6.6%
Algeria	2374	2278	96	4.2%
India	2295	2280	15	4.1%
Mexico	1908	1748	160	3.4%
Indonesia	1585	1570	15	2.8%
Thailand	1402	1304	98	2.5%
Colombia	1344	1225	119	2.4%
Morocco	1249	1168	81	2.2%
Egypt	1242	1072	170	2.2%
Vietnam	1220	1146	74	2.2%
Argentina	1159	1055	104	2.1%
Philippines	1008	946	62	1.8%
Peru	950	869	81	1.7%
Iran	801	791	10	1.4%
Romania	798	717	81	1.4%
China	736	725	11	1.3%
Venezuela	686	633	53	1.2%
Chile	665	598	67	1.2%
South Africa	665	625	40	1.2%
Turkey	622	508	114	1.1%
Malaysia	619	551	68	1.1%
Spain	596	540	56	1.1%
Sri Lanka	564	520	44	1.0%
Germany	539	525	14	1.0%
Bangladesh	523	502	21	0.9%
Poland	496	456	40	0.9%
Ecuador	478	425	53	0.8%
Serbia	456	426	30	0.8%
United Kingdom	440	398	42	0.8%
Norway	418	406	12	0.7%
Portugal	415	383	32	0.7%



https://twitter.com/1ZRR4H/status/1759622944957853960

A comprehensive analysis of the STOP/DJVU ransomware campaign reveals significant insights into its reach and impact across various countries. The provided data, sourced from the attackers' panel, sheds light on the scale of potential installations and highlights the geographical distribution of affected devices.

Campaign Overview:

- The STOP/DJVU ransomware campaign has been active since at least the first week of January 2024.
- The campaign employs sophisticated tactics to infect devices and encrypt user data, demanding ransom payments for decryption keys.

Key Statistics:

- Total Unique Records: 53,068 potential installations, including sandboxes and other environments.
- Top 10 Countries by Unique Installs:
    a. United States: 4,249 installs
    b. Brazil: 3,791 installs
    c. Pakistan: 3,661 installs
    d. Algeria: 2,278 installs
    e. India: 2,280 installs
    f. Mexico: 1,748 installs
    g. Indonesia: 1,570 installs
    h. Thailand: 1,304 installs
    i. Colombia: 1,225 installs
    j. Morocco: 1,168 installs

Insights:

- The data underscores the global reach of the STOP/DJVU ransomware campaign, with installations detected across diverse regions.
- Countries with significant numbers of unique installs, such as the United States, Brazil, and Pakistan, indicate widespread impact and active propagation of the ransomware.
- The distribution of installations suggests that attackers are targeting a broad range of geographical locations, potentially exploiting vulnerabilities in various regions' cybersecurity infrastructure.

Art of Detection

https://twitter.com/jupyterthon

An open community event dedicated to security researchers leveraging Jupyter Notebooks within the InfoSec field provided a platform for knowledge-sharing and collaboration. Attendees participated virtually, exchanging insights, favorite notebooks, and practical applications of Jupyter Notebooks in various security domains. The event featured keynote speeches and presentations from industry experts, covering a wide range of topics related to security operations, threat hunting, data visualization, and more.

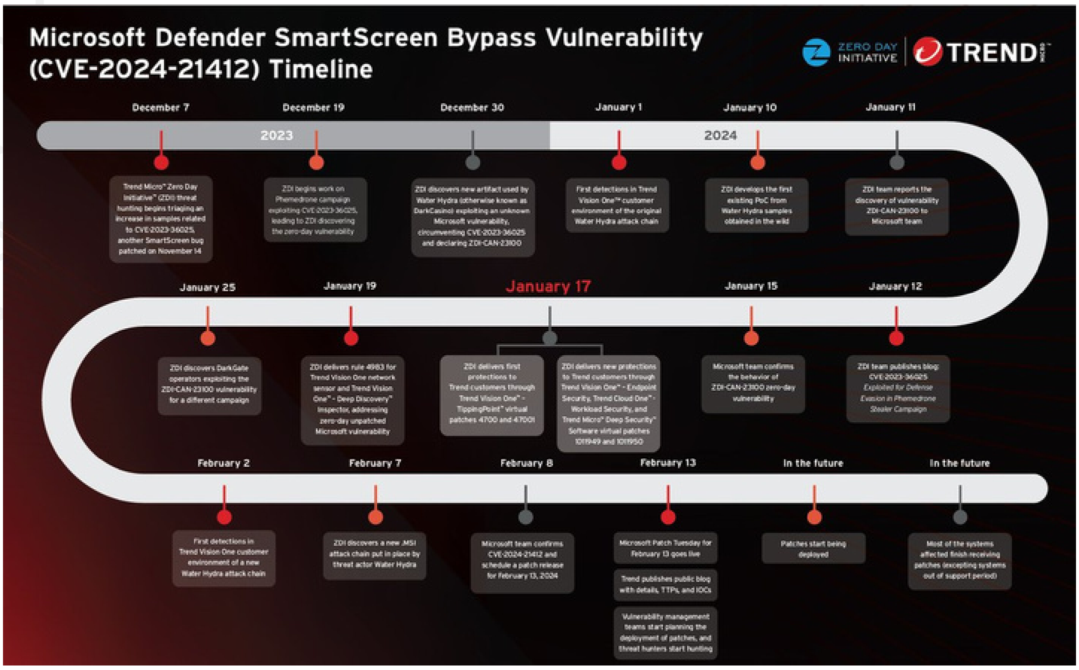
Keynote Address: The keynote speech titled "Barn Raising: Building a Community Around Jupyter Notebooks for DFIR, SecOps, and Detection Engineering Teams" by Ryan Marcotte Cobb highlighted the journey of growing a community of notebook users across different security teams. The keynote emphasized the adoption challenges, best practices, and the positive impacts of integrating Jupyter Notebooks into operational workflows.

Highlighted Talks: Several notable presentations showcased innovative approaches and practical use cases of Jupyter Notebooks in InfoSec:

- "Graphing Ransomware & Data Leak Sites Trends with Plotly" by Colin Cowie explored analytics of data leak sites using Plotly for visualizations.
- "Threat Hunting in Three Dimensions" by Ryan Fetterman demonstrated a threat hunting workflow leveraging Jupyter for visual analysis of complex data.
- "Red Teaming LLMs with Jupyter Notebooks: A Practical Guide" by Pete Bryan presented an approach for red teaming large language models using Jupyter Notebooks.
- "From Idea to Action: Building Data-Driven Security Tools with Streamlit" by Ashwin Patil showcased Streamlit's role in accelerating the development of data-driven security tools.

Insights and Discussions: Throughout the event, speakers and participants engaged in discussions on various topics, including hacking proprietary protocols, threat hunting methodologies, and risk scoring models. Attendees gained insights into effective collaboration methods, threat intelligence analysis, and the practical applications of Jupyter Notebooks in security research and operations.

1Day



Microsoft Defender SmartScreen Bypass Vulnerability (CVE-2024-21412) Timeline

December 7: Trend Micro™ Zero Day Initiative™ (ZDI) threat hunting begins triaging an increase in samples related to CVE-2023-36025, another SmartScreen bug patched on November 14

December 19: ZDI begins work on Phemedrone campaign exploiting CVE-2023-36025, leading to ZDI discovering the zero-day vulnerability

December 30: ZDI discovers new artifact used by Water Hydra (otherwise known as DarkCasino) exploiting an unknown Microsoft vulnerability, circumventing CVE-2023-36025 and declaring ZDI-CAN-23100

January 1: First detections in Trend Vision One™ customer environment of the original Water Hydra attack chain

January 10: ZDI develops the first existing PoC from Water Hydra samples obtained in the wild

January 11: ZDI team reports the discovery of vulnerability ZDI-CAN-23100 to Microsoft team

January 12: ZDI team publishes blog: CVE-2023-36025 *Exploited for Defense Evasion in Phemedrone Stealer Campaign*

January 15: Microsoft team confirms the behavior of ZDI-CAN-23100 zero-day vulnerability

January 17: ZDI delivers first protections to Trend customers through Trend Vision One™ - TippingPoint™ virtual patches 4700 and 47001

ZDI delivers new protections to Trend customers through Trend Vision One™ - Endpoint Security, Trend Cloud One™ - Workload Security, and Trend Micro® Deep Security™ Software virtual patches 1011949 and 1011950

January 19: ZDI delivers rule 4983 for Trend Vision One network sensor and Trend Vision One™ - Deep Discovery™ Inspector, addressing zero-day unpatched Microsoft vulnerability

January 25: ZDI discovers DarkGate operators exploiting the ZDI-CAN-23100 vulnerability for a different campaign

February 2: First detections in Trend Vision One customer environment of a new Water Hydra attack chain

February 7: ZDI discovers a new .MSI attack chain put in place by threat actor Water Hydra

February 8: Microsoft team confirms CVE-2024-21412 and schedule a patch release for February 13, 2024

February 13: Microsoft Patch Tuesday for February 13 goes live

Trend publishes public blog with details, TTPs, and IOCs

Vulnerability management teams start planning the deployment of patches, and threat hunters start hunting

In the future: Patches start being deployed

In the future: Most of the systems affected finish receiving patches (excepting systems out of support period)

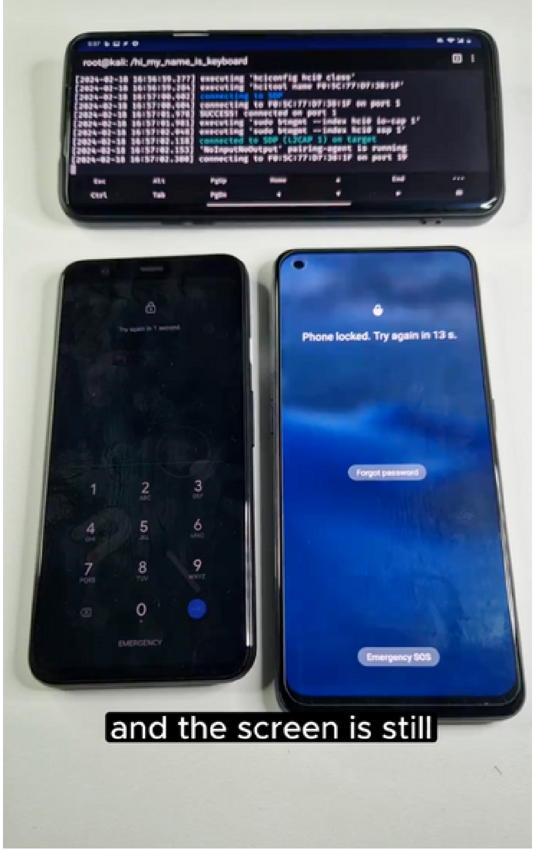
CVE-2024-21412 is a critical security vulnerability discovered in Microsoft Defender SmartScreen by the Trend Micro™ Zero Day Initiative™ (ZDI). This vulnerability was identified as part of a sophisticated zero-day attack chain orchestrated by the advanced persistent threat (APT) group known as Water Hydra (also referred to as DarkCasino). Notably, another unidentified group was also found exploiting the same vulnerability.

Patch Report: A special patch report was released by ZDI Senior Threat Researcher, Peter Girnus, who provided insights into the actively exploited nature of CVE-2024-21412 in the wild. The report delves into the specifics of the bug and the threat actors involved, offering crucial information for mitigation strategies.

Security Update: ZDI also issued a comprehensive security update regarding CVE-2024-21412, presenting insights from their zero-day initiative team. This update serves as a valuable resource for understanding the implications of the vulnerability and the necessary protective measures.

Impact: The exploitation of CVE-2024-21412 highlights the constant evolution of threat actors' tactics in bypassing security measures. It was observed that the bypass of CVE-2023-36025, a previously patched SmartScreen vulnerability, ultimately led to the discovery and exploitation of CVE-2024-21412. This underscores the agility of threat actors in identifying new attack vectors even around patched software components.

🌶️ Trending Exploit



```
root@kali: /hi_my_name_is_keyboard
[2024-02-18 16:56:59.277] executing 'hciconfig hci0 class'
[2024-02-18 16:56:59.284] executing 'hcitool name F0:5C:77:D7:38:1F'
[2024-02-18 16:57:00.082] connecting to SDP
[2024-02-18 16:57:00.085] connecting to F0:5C:77:D7:38:1F on port 1
[2024-02-18 16:57:00.978] SUCCESS! connected on port 1
[2024-02-18 16:57:01.981] executing 'sudo btmgmt --index hci0 io-cap 1'
[2024-02-18 16:57:02.040] executing 'sudo btmgmt --index hci0 ssp 1'
[2024-02-18 16:57:02.118] connected to SDP (L2CAP 1) on target
[2024-02-18 16:57:02.153] 'NoInputNoOutput' pairing-agent is running
[2024-02-18 16:57:02.300] connecting to F0:5C:77:D7:38:1F on port 19
```

https://twitter.com/androidmalware2/status/1759502513538044189

A critical security vulnerability, identified as CVE-2023-45866, has been discovered in Android smartphones, enabling attackers to remotely lock out users or even wipe data through Bluetooth exploitation. This vulnerability poses a significant threat to user privacy and data security.

Vulnerability Details: The vulnerability allows attackers to remotely exploit Bluetooth functionality on Android smartphones without requiring pairing. By leveraging this vulnerability, attackers can inject keystrokes into the device, potentially leading to unauthorized access or control over the device's functions.

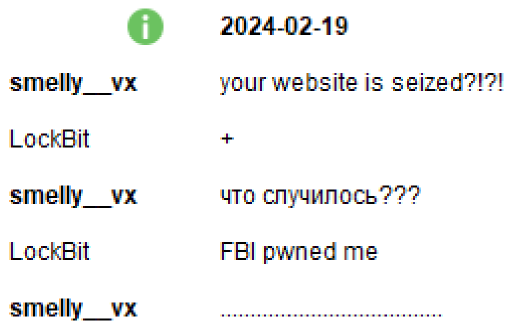
Impact: The exploitation of CVE-2023-45866 poses serious risks to Android smartphone users. Attackers can remotely lock out users from their devices or, if the "Auto factory reset" feature is enabled, trigger a factory reset after 20 incorrect unlock attempts, resulting in the loss of all user data.

Mitigation: Android users are advised to take immediate action to mitigate the risks associated with this vulnerability:

1. Disable Bluetooth when not in use to minimize exposure to potential attacks.
2. Update Android devices to the latest security patches provided by the device manufacturer.
3. Avoid connecting to untrusted or unknown Bluetooth devices.
4. Regularly back up important data to prevent permanent loss in the event of a factory reset.

Further Information: Additional details regarding the exploitation of this vulnerability can be found in the article provided by mobile-hacker.com: Exploiting 0-click Android Bluetooth Vulnerability to Inject Keystrokes Without Pairing

🕯️ The Topic of the Week



ⓘ	**2024-02-19**
smelly__vx	your website is seized?!?!
LockBit	+
smelly__vx	что случилось???
LockBit	FBI pwned me
smelly__vx	....

https://twitter.com/vxunderground/status/1759697172101022176

The administrative staff of the Lockbit ransomware group has confirmed the seizure of their websites. Lockbit, a notorious ransomware-as-a-service (RaaS) operation, has been associated with numerous high-profile cyberattacks, targeting organizations worldwide. The seizure of Lockbit's websites represents a significant blow to their infrastructure and operations. These websites likely served as crucial communication platforms for the ransomware group, facilitating negotiations with victims and providing information on their malicious activities.

While the exact circumstances surrounding the seizure remain undisclosed, it signals a potential disruption in Lockbit's ability to conduct their illicit activities. This development aligns with global efforts to combat ransomware and disrupt cybercriminal operations.

Organizations impacted by Lockbit ransomware attacks may benefit from this development, as it could potentially hinder the group's ability to execute attacks and demand ransom payments. However, it's essential for affected organizations to remain vigilant and continue implementing robust cybersecurity measures to protect against evolving threats.

Law enforcement agencies, cybersecurity firms, and international partners are likely involved in the efforts to seize Lockbit's infrastructure and hold its operators accountable. Such coordinated actions are critical in combating ransomware and dismantling cybercriminal networks.

As the situation develops, organizations should stay informed and collaborate with relevant authorities to mitigate the risks associated with ransomware attacks. Additionally, proactive measures such as data backups, network segmentation, and employee training remain essential components of a comprehensive cybersecurity strategy in defending against ransomware threats.

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.