### **Tusk Infostealer — CyberDefenders**

**Scenario:** A blockchain development company detected unusual activity when an employee was redirected to an unfamiliar website while accessing a DAO management platform. Soon after, multiple cryptocurrency wallets linked to the organization were drained. Investigators suspect a malicious tool was used to steal credentials and exfiltrate funds.

Your task is to analyze the provided intelligence to uncover the attack methods, identify indicators of compromise, and track the threat actor’s infrastructure.

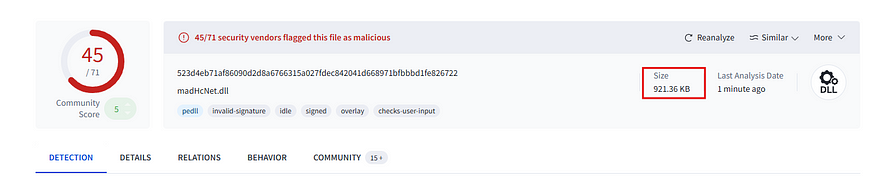
#### **Tasks**

MD5: E5B8B2CF5B244500B22B665C87C11767

Use this hash on online threat intel platforms (e.g., VirusTotal, Hybrid Analysis) to complete the lab analysis.

1. **In KB, what is the size of the malicious file?**

Let us submit the MD5 hash to VirusTotal to find more information about this.

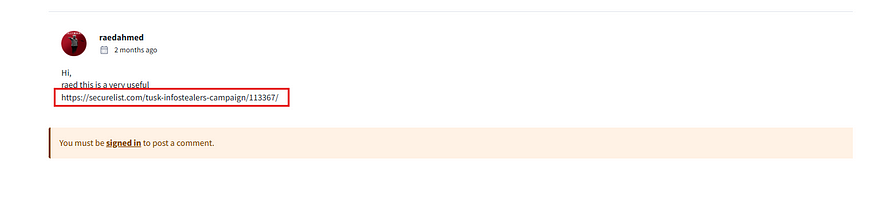


**Answer:** 921.36

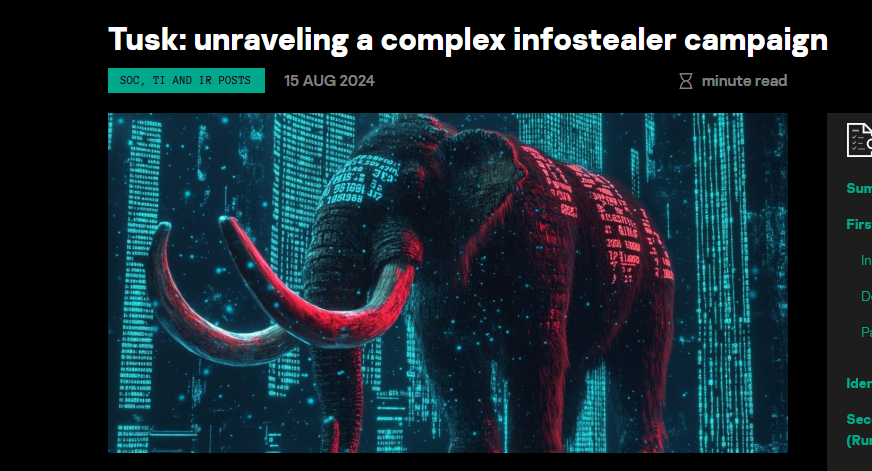
**2. What word does the threat actor use in log messages to refer to victims, drawing inspiration from ancient tusk hunters?**

It is strange that the reports relating to this hash are not available on hybrid analysis platforms.

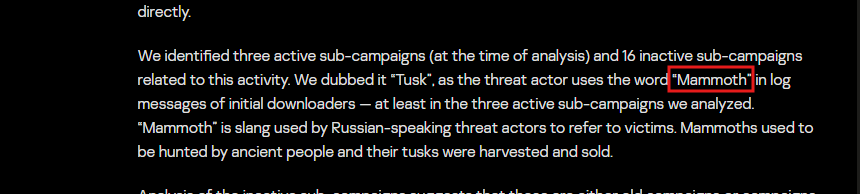
But, there is a link provided in the community tab in VirusTotal.



This link has so much information about the malware.



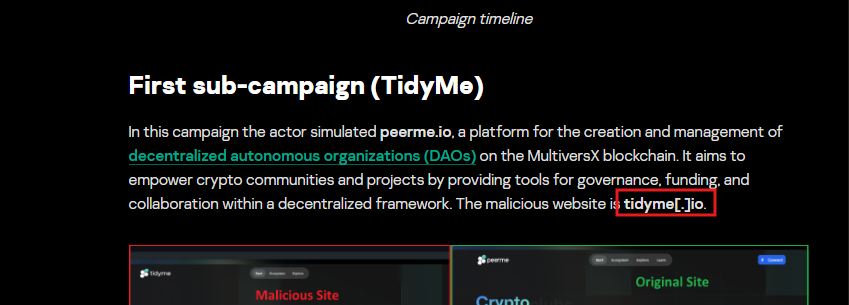
The answer to this question is available at the start of this report.



**Answer:** Mammoth

**3. The threat actor set up a malicious website to mimic a platform designed for creating and managing decentralized autonomous organizations (DAOs) on the MultiversX blockchain (peerme.io). What is the name of the malicious website the attacker created to simulate this platform?**

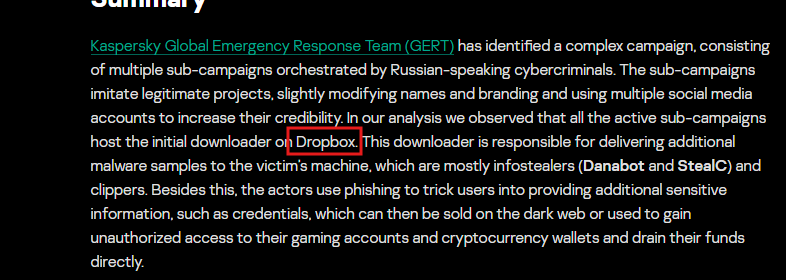
Reading further down this report we can find the answer. The malicious website is tidyme[.]io.



**Answer:** tidyme.io

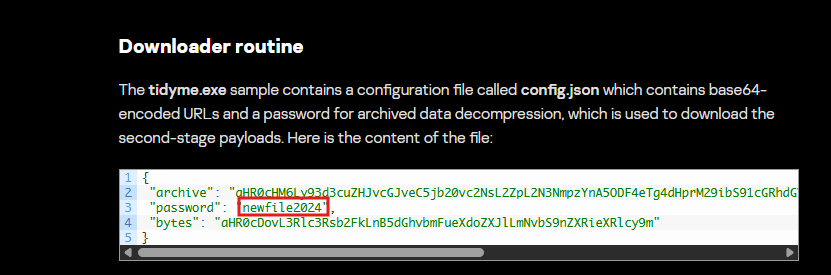
**4.Which cloud storage service did the campaign operators use to host malware samples for both macOS and Windows OS versions?**

The report states that the campaign uses Dropbox to host the initial downloader.



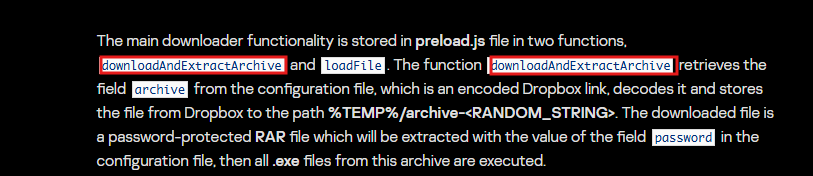
**Answer:** Dropbox.

**5. The malicious executable contains a configuration file that includes base64-encoded URLs and a password used for archived data decompression, enabling the download of second-stage payloads. What is the password for decompression found in this configuration file?**

****

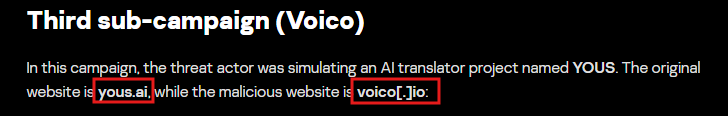
**Answer:** newfile2024

**6. What is the name of the function responsible for retrieving the field archive from the configuration file?**

****

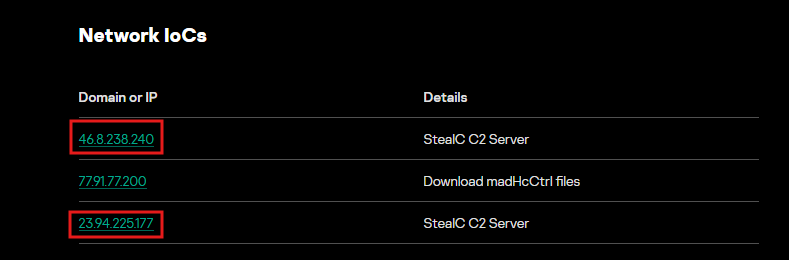
**Answer:** downloadAndExtractArchive

**7. In the third sub-campaign carried out by the operators, the attacker mimicked an AI translator project. What is the name of the legitimate translator, and what is the name of the malicious translator created by the attackers?**

****

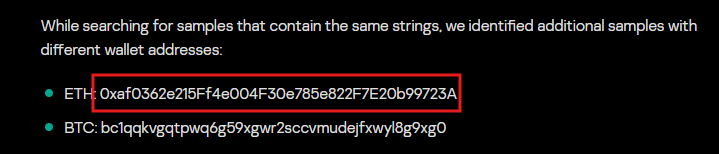
**Answer:** Yous.ai, voico.io

**8. The downloader is tasked with delivering additional malware samples to the victim’s machine, primarily infostealers like StealC and Danabot. What are the IP addresses of the StealC C2 servers used in the campaign?**

****

**Answer:** 46.8.238.240,23.94.225.177

**9. What is the address of the Ethereum cryptocurrency wallet used in this campaign?**

****

**Answer:** 0xaf0362e215Ff4e004F30e785e822F7E20b99723A

This is the end of the walkthrough.