# Name: Christon Mitchell Date: 05/05/2025

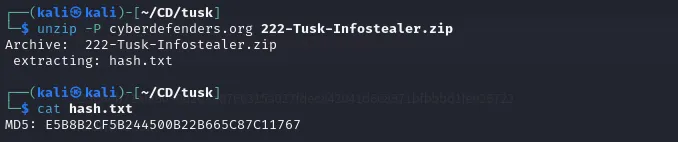
# CyberDefenders Blue Team Lab - Tusk Infostealer Write-up

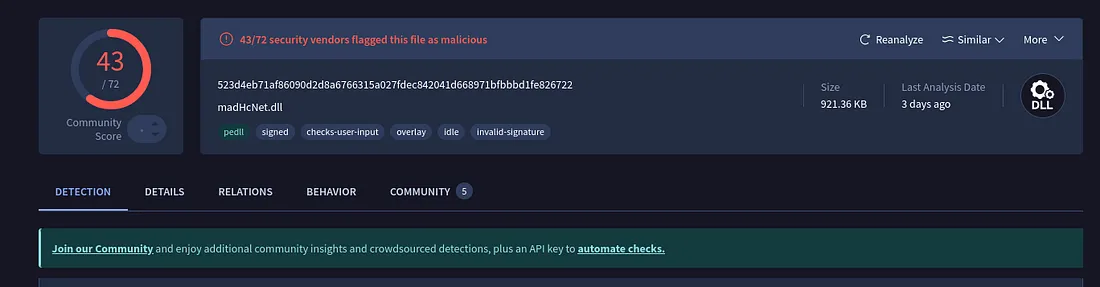
This is a write-up for the lab 'Tusk Infostealer'. Most of the answers can be found by googling, however, I found a website that has all the answers. I highly recommend you review the website and read the article before this write-up.  
  
<https://securelist.com/tusk-infostealers-campaign/113367/>

## Scenario

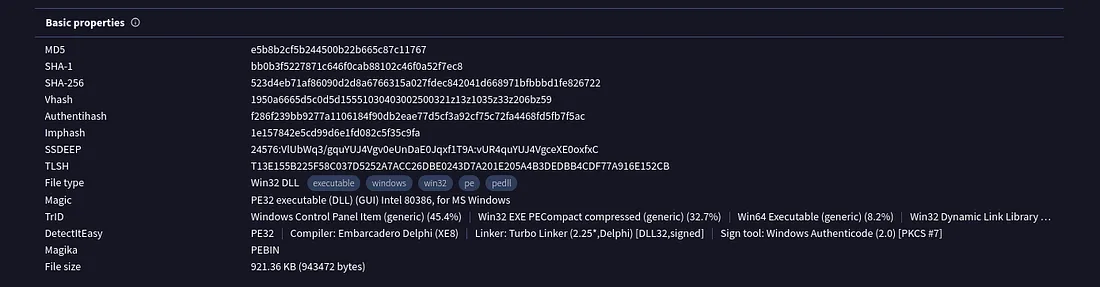
A blockchain development company detected unusual activity when an employee was redirected to an unfamiliar website while accessing a DAO management platform. Soon after, multiple cryptocurrency wallets linked to the organization were drained. Investigators suspect a malicious tool was used to steal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

## Lab Files

Extract the lab files and it contains an md5 hash.  
  
**MD5**: E5B8B2CF5B244500B22B665C87C11767  
  
I used the MD5 hash provided in the lab and searched for the sample on VirusTotal, since it wasn’t available on MalwareBazaar or other public repositories. The campaign site also appears to be inactive, so VirusTotal was the most reliable option for analysis.  
  


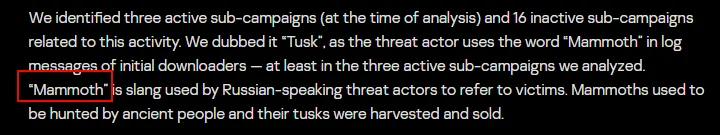


## Questions and Answers

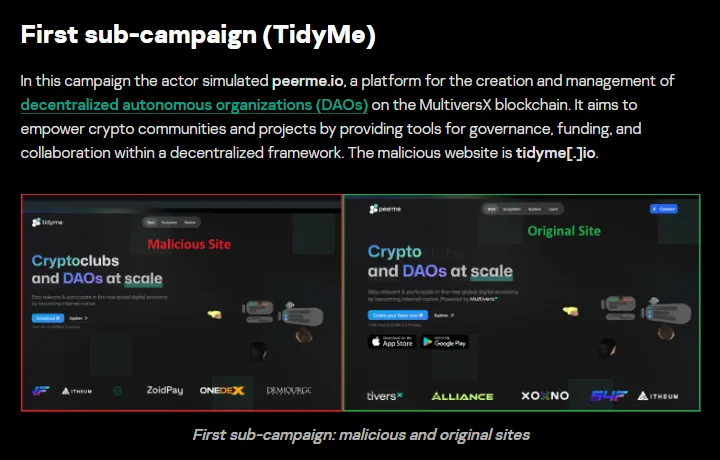
**What is the size of the malicious file?  
  
Answer:** 921.36 KB  
  


Go to the details tab in Virustotal to find file size

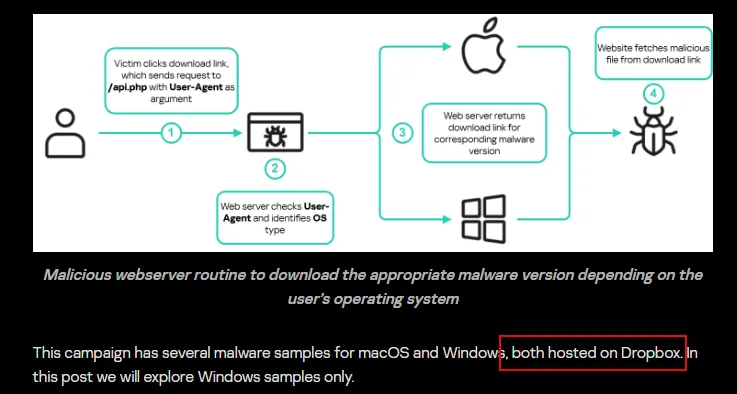
**What word does the threat actor use in log messages to refer to victims, drawing inspiration from ancient tusk hunters?**

****A quick Google and you’ll find the article about tusk info stealer campaign from SecureList by Kaspersky. From this point onward all the answers will be from the article.

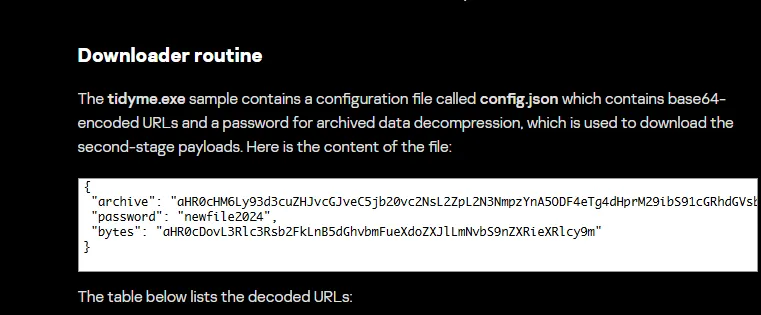
**Answer:** Mammoth

**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?**  
  
**Answer:** tidyme.io

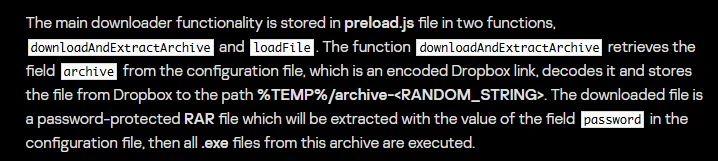
**Which cloud storage service did the campaign operators use to host malware samples for both macOS and Windows OS versions?**

****  
**Answer:** Dropbox

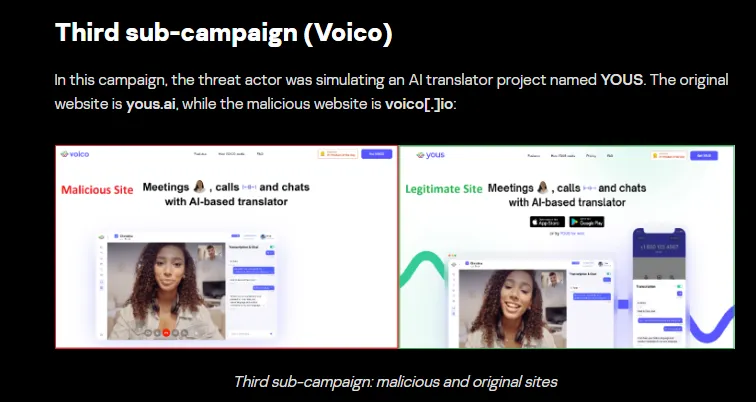
**The malicious executable contains a configuration file that includes base64-encoded URLs and a password used for archived data decompression, enabling the download of second-stage payloads. What is the password for decompression found in this configuration file?**

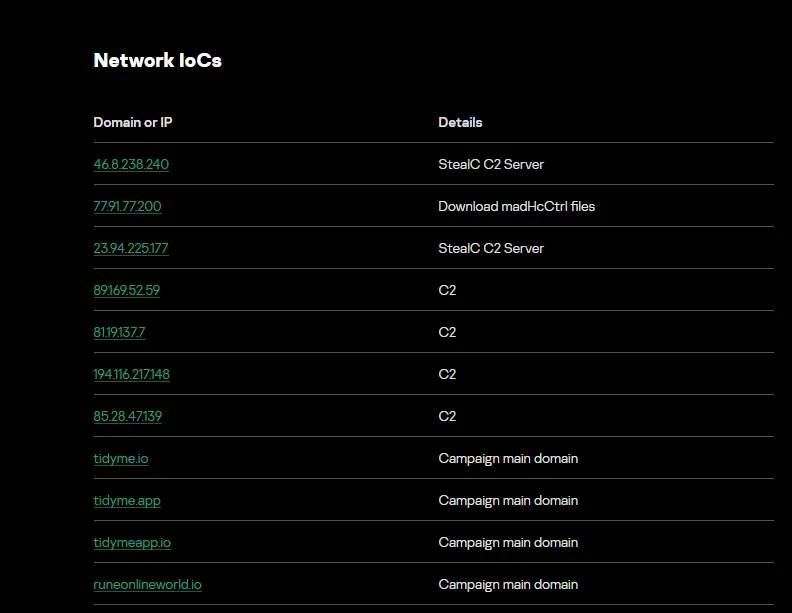
  
  
**Answer:** newfile2024

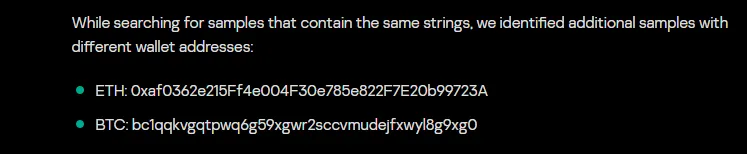
**What is the name of the function responsible for retrieving the field archive from the configuration file?**

**  
  
Answer:** downloadAndExtractArchive

**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](http://yous.ai) , voico.io

**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

**What is the address of the Ethereum cryptocurrency wallet used in this campaign?  
**  
**Answer:** 0xaf0362e215Ff4e004F30e785e822F7E20b99723A