

**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.

```

(kali㉿kali)-[~/CD/tusk]
$ unzip -P cyberdefenders.org 222-Tusk-Infostealer.zip
Archive: 222-Tusk-Infostealer.zip
  extracting: hash.txt

(kali㉿kali)-[~/CD/tusk]
$ cat hash.txt
MD5: E5B8B2CF5B244500B22B665C87C11767

```

43 / 72 Community Score

43/72 security vendors flagged this file as malicious

523d4eb71af86090d2d8a6766315a027fdec842041d668971bfbbbd1fe826722

madHcNet.dll

Size: 921.36 KB | Last Analysis Date: 3 days ago

pedi signed checks-user-input overlay idle invalid-signature

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

## Questions and Answers

**What is the size of the malicious file?**

**Answer:** 921.36 KB

Basic properties

MD5	e5b8b2cf5b244500b22b665c87c11767
SHA-1	bb0b3f5227871c646f0cab88102c46f0a527fec8
SHA-256	523d4eb71af86090d2d8a6766315a027fdec842041d668971bfbbbd1fe826722
Vhash	1950a6665d5c0d5d1555103040300250032121321035x332206b259
Authentihash	f286f239bb9277a110618490db2eae77d5cf3a92cf75c72fa4468fd5fb7f5ac
Imphash	1e157842e5cd99d6e1fd082c5f05c3fa
SSDEEP	24576vIUhWq3/gquYUJ/vg0eUnDaE0Jqr1T9A-vUR4quYUJ/vgeXE0ouxfC
TLSH	T13E155B225F58C037D5252A7ACC26BE0243D7A201E205A4B3DEDBB4CDF77A916E152CB
File type	Win32 DLL executable windows win32 pe pedi
Magic	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID	Windows Control Panel Item (generic) (45.4%) Win32 EXE PECompact compressed (generic) (32.7%) Win64 Executable (generic) (8.2%) Win32 Dynamic Link Library ...
DetectItEasy	PE32 Compiler: Embarcadero Delphi (XE8) Linker: Turbo Linker (2.25*,Delphi) [DLL32,signed] Sign tool: Windows Authenticode (2.0) [PKCS #7]
Magika	PEBIN
File size	921.36 KB (943472 bytes)

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?**

We identified three active sub-campaigns (at the time of analysis) and 16 inactive sub-campaigns related to this activity. We dubbed it "Tusk", as the threat actor uses the word "Mammoth" in log messages of initial downloaders – at least in the three active sub-campaigns we analyzed.

"Mammoth" is slang used by Russian-speaking threat actors to refer to victims. Mammoths used to be hunted by ancient people and their tusks were harvested and sold.

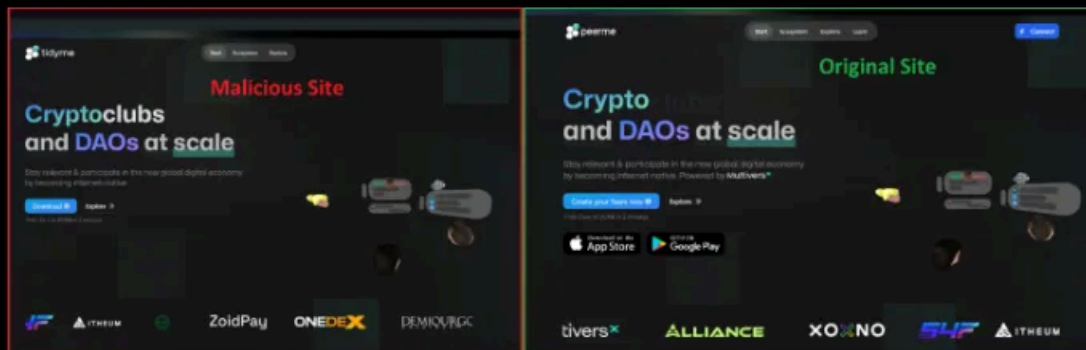
A quick Google and you'll find the article about tusk info stealer campaign from SecureList by Kaspersky. From this point onward all the answers will be from the article.

**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?**

## First sub-campaign (TidyMe)

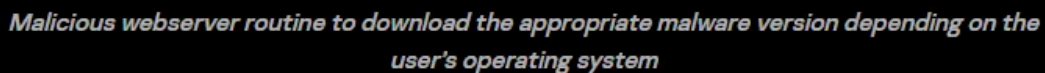
In this campaign the actor simulated [peerme.io](https://peerme.io), a platform for the creation and management of [decentralized autonomous organizations \(DAOs\)](#) on the MultiversX blockchain. It aims to empower crypto communities and projects by providing tools for governance, funding, and collaboration within a decentralized framework. The malicious website is [tidyme.io](https://tidyme.io).



*First sub-campaign: malicious and original sites*

**Answer:** [tidyme.io](https://tidyme.io)

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



This campaign has several malware samples for macOS and Windows, both hosted on Dropbox. In this post we will explore Windows samples only.

**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?

The **tidyme.exe** sample contains a configuration file called **config.json** which contains base64-encoded URLs and a password for archived data decompression, which is used to download the second-stage payloads. Here is the content of the file:

```
{
  "archive": "aHR0cHM6Ly93d3cuZHZvcGJveC5jb20vc2NsL2ZpL2N3NmpzYnA5ODF4eTg4dHprM29ibS91cGRhdGVst",
  "password": "newfile2024",
  "bytes": "aHR0cDovLzRlR3Rsb2FkLnB5dGhvbmFueXdoZXJlLnNvbS9nZXRicXRLcy9m"
}
```

The table below lists the decoded URLs:

**Answer:** newfile2024

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

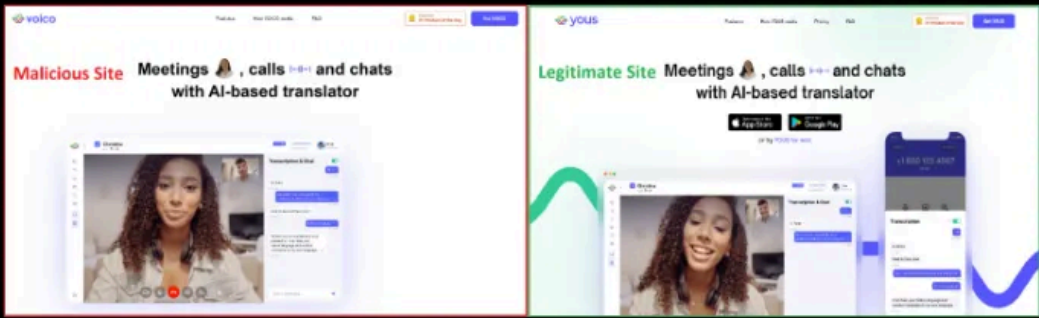
The main downloader functionality is stored in `preload.js` file in two functions, `downloadAndExtractArchive` and `loadFile`. The function `downloadAndExtractArchive` retrieves the field `archive` from the configuration file, which is an encoded Dropbox link, decodes it and stores the file from Dropbox to the path `%TEMP%/archive-<RANDOM_STRING>`. The downloaded file is a password-protected RAR file which will be extracted with the value of the field `password` in the configuration file, then all `.exe` files from this archive are executed.

**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?**

### Third sub-campaign (Voico)

In this campaign, the threat actor was simulating an AI translator project named YOUS. The original website is [yous.ai](https://yous.ai), while the malicious website is [voico.io](https://voico.io):



The image shows two side-by-side screenshots of websites. The left screenshot is labeled 'Malicious Site' and shows the 'voico' website. The right screenshot is labeled 'Legitimate Site' and shows the 'yous' website. Both websites feature a video call interface with a woman's face and a chat window. The 'yous' website has a green and blue color scheme, while the 'voico' website has a red and white color scheme.

*Third sub-campaign: malicious and original sites*

**Answer:** [yous.ai](https://yous.ai) , [voico.io](https://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?

Network IoCs	
Domain or IP	Details
<a href="#">46.8.238.240</a>	StealC C2 Server
<a href="#">77.91.77.200</a>	Download madHcCtrl files
<a href="#">23.94.225.177</a>	StealC C2 Server
<a href="#">89.169.52.59</a>	C2
<a href="#">81.19.137.7</a>	C2
<a href="#">194.116.217.148</a>	C2
<a href="#">85.28.47.139</a>	C2
<a href="#">tidyme.io</a>	Campaign main domain
<a href="#">tidyme.app</a>	Campaign main domain
<a href="#">tidymeapp.io</a>	Campaign main domain
<a href="#">runeonlineworld.io</a>	Campaign main domain

**Answer:** 46.8.238.240, 23.94.225.177

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

While searching for samples that contain the same strings, we identified additional samples with different wallet addresses:

- ETH: 0xaf0362e215Ff4e004F30e785e822F7E20b99723A
- BTC: bc1qqkvqtpwq6g59xgwr2sccvmudejfxwyl8g9xg0

**Answer:** 0xaf0362e215Ff4e004F30e785e822F7E20b99723A