

Challenge: [Tusk Infostealer Lab](#)

Platform: CyberDefenders

Category: Threat Intel

Difficulty: Easy

Tools Used: Kaspersky Threat Intelligence Portal, VirusTotal

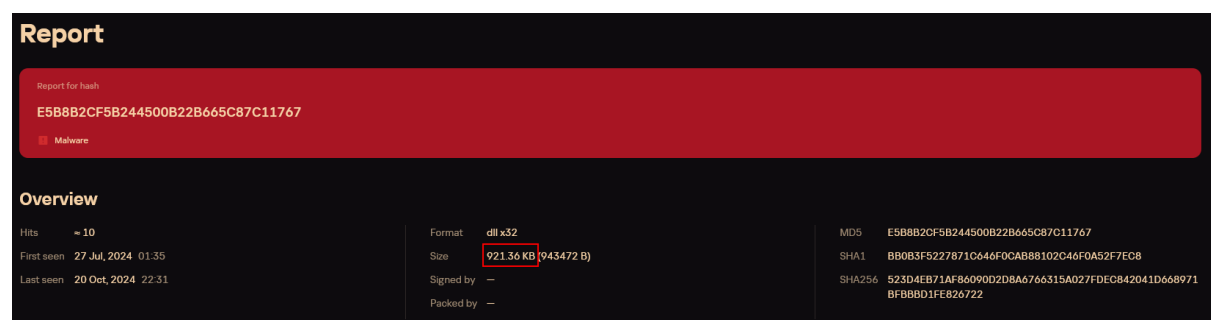
Summary: This lab involved using threat intelligence tools in order to investigate a tusk infostealer campaign. This lab was not particularly difficult, but it was fun to use the Kaspersky Threat Intelligence Portal as I am typically used to VirusTotal.

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 analyse the provided intelligence to uncover the attack methods, identify indicators of compromise, and track the threat actor's infrastructure.

In KB, what is the size of the malicious file?

Personally, this is my first time using Kaspersky Threat Intelligence Portal, I typically use VirusTotal or Cisco Talos. To find the size of the file, enter the provided hash into the Lookup search:



The screenshot shows a report for a malicious file. The hash is E5B8B2CF5B244500B22B665C87C11767. The file is identified as Malware. The overview section shows the file size as 921.36 KB (943472 B). The file is a DLL (dll x32). The report also includes MD5, SHA1, and SHA256 hashes.

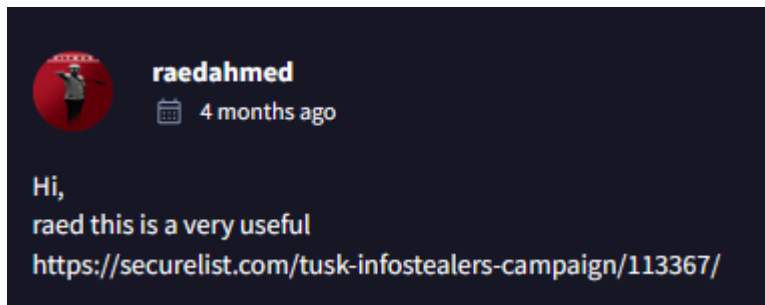
Report for hash	
E5B8B2CF5B244500B22B665C87C11767	
Malware	

Overview	
Hits	~ 10
First seen	27 Jul, 2024 01:35
Last seen	20 Oct, 2024 22:31
Format	dll x32
Size	921.36 KB (943472 B)
Signed by	—
Packed by	—
MD5	E5B8B2CF5B244500B22B665C87C11767
SHA1	BB0B3F5227871C646F0CAB88102C46F0A52F7EC8
SHA256	523D4EB71AF86090D2D8A6766315A027FDEC842041D668971BFBBD1FE826722

Answer: 921.36

What word do the threat actors use in log messages to describe their victims, based on the name of an ancient hunted creature?

Given the specific nature of the question, this is likely something that can't be answered by a threat intelligence tool. We likely need to find reports. Thankfully, I was able to find a link in the Community tab on VirusTotal for a report about tusk infostealers using the given hash:



If you go through this [report](#) you can find some messages that were sent to the C2 server:

Неудачное открытие файла, через 4 минуты повторяю...:	Unsuccessful file opening, after 4 minutes I repeat...:
Глобальная ошибка:	Global error:
Мамонт открыл лаунчер...	Mammoth opened the launcher...
Мамонт свернул лаунчер...	Mammoth collapsed the launcher...
Мамонт закрыл лаунчер...	Mammoth closed the launcher...

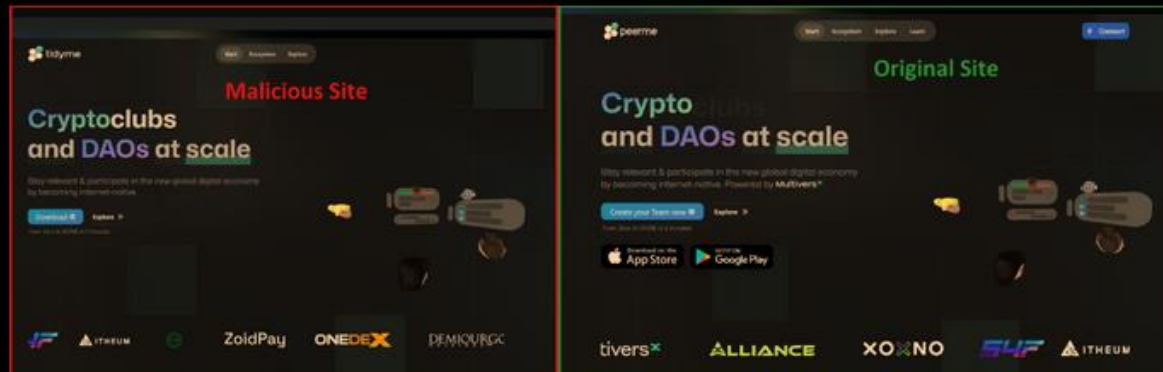
Answer: Mammoth

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?

Using the same report from the previous question, it details a campaign called TidyMe, which involved the threat actor simulating peerme.io, a DAO platform. The malicious website that was created to simulate the platform was called tidyme[.]io:

First sub-campaign (TidyMe)

In this campaign the actor simulated **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**.



First sub-campaign: malicious and original sites

Answer: tidyme.io

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

If you continue reading about the TidyMe campaign, you will eventually come across the section that talks about how several malware samples for macOS and Windows were hosted on DropBox:

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?

By now, you can probably guess that you need to continue reading the report. Under the Downloader routine section, it outlines the configuration file used by tidyme.exe:

Downloader routine

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": "aHR0cHM6Ly93d3cuZHJvcGJveC5jb20vc2NsL2ZpL2N3NmpzYnA5ODF4eTg4dHprM29ibS9lcGRhdGVsbw==",  
    "password": "newfile2024",  
    "bytes": "aHR0CDovL3RlICRSb2ZFkLnB5dGhvbmFueXdoZXJlLnNvbS9nZXRIeXRlcyc9m"  
}
```

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?

Once again, scroll through the report until you get to the third sub-campaign section called Voico. Here you can find the legitimate and malicious websites:

Third sub-campaign (Voico)

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

Answer: 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?

Domain or IP	Details
46.8.238.240	StealC C2 Server
77.91.77.200	Download madHcCtrl files
23.94.225.177	StealC C2 Server

Answer: 46.8.238.240, 23.94.225.177

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

● ETH: 0xaf0362e215Ff4e004F30e785e822F7E20b99723A

Answer: 0xaf0362e215Ff4e004F30e785e822F7E20b99723A