Kraken - The Deep Sea Lurker Part 2

0xtoxin.github.io/threat hunting/KrakenKeylogger-pt2/

May 26, 2023

Part 2 of analyzing the KrakenKeylogger Malware

5 minute read

0xToxin

Threat Analyst & IR team leader - Malware Analysis - Blue Team

Intro

In the second part of analyzing the “KrakenKeylogger”, I will be diving into some proactive “threat hunting” steps I’ve done during my research about the Kraken.
If you haven’t already read the first part of analyzing the Kraken, be sure to check it out here
With that saying let’s begin!

What we have?

Let’s start with what we currently have and how can we pivot with it:

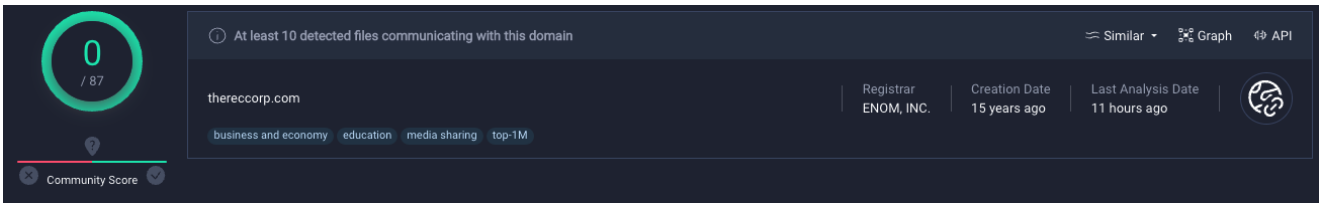
- **C2:** thereccorp.com
- **Payload fetching domain:** masherofmasters.cyou
- **Binary Name:** KrakenStub

The hunting will be splitted into 4 part:

1. thereccorp.com analysis
2. masherofmasters.cyou analysis
3. UnpackMe Yara Hunt
4. OSINT research

thereccorp.com Analysis

We start off with our final C2 domain `thereccorp.com`, searching the domain in VirusTotal will respond us with a solid **0/87** vendors detection:



going to the `relations` tab and looking at the `Communicating Files` files we can see 22 files which all were flagged as malicious:

Communicating Files (22)

Scanned	Detections	Type	Name
2023-05-15	46 / 65	ZIP	03cd9b875668d603ac396a9b2efe1b13871513cbb69341349?bb674b5df22af2.zip
2023-05-07	42 / 70	Win32 EXE	Copy.exe
2023-05-24	30 / 71	Win32 EXE	SuperAraneid.exe
2023-05-20	34 / 60	Windows shortcut	Payment.lnk
2023-05-18	49 / 71	Win32 EXE	21d0345174d67986202fdecdf8e56493628d9e66eafdf4002a8dacb84c46d779
2023-05-15	46 / 63	ZIP	Copy.zip
2023-05-24	32 / 72	Win32 EXE	SuperAraneid.exe
2023-05-18	53 / 71	Win32 EXE	osukps.exe
2023-05-13	35 / 60	Windows shortcut	5b52facac06e5e115c54fec3f13b08ebba46f4850306fe9766a:0e7594de02ff.lnk
2023-05-20	43 / 65	ZIP	PO-87098.zip
2023-05-13	40 / 65	ZIP	PO-231062_zip.bin
2023-05-24	53 / 71	Win32 EXE	CgLogListener.exe
2023-05-23	44 / 65	ZIP	7ddacf946c3de29255d826fbce407672c991285e15bf4a0e33?28561847b7d6f.zip
2023-05-09	17 / 64	ZIP	3dab175a0cbfd28182ea5c9b27c10274.file
2023-05-23	50 / 71	Win32 EXE	Observatory.exe
2023-05-20	35 / 60	Windows shortcut	Payment.lnk
2023-05-24	22 / 71	Win32 EXE	SuperAraneid.exe
2023-05-13	56 / 71	Win32 EXE	ChessTables.exe
2023-05-13	45 / 71	Win32 EXE	74b46e9615014e0e39d809cc469c7a061093210b.bin
2023-05-23	33 / 60	Windows shortcut	Swift-Copy.lnk
2023-05-16	12 / 63	ZIP	8abdc59ea5c9fed19dbb1f1585ac13fe.file
2023-05-19	49 / 71	Win32 EXE	PiaNO.exe

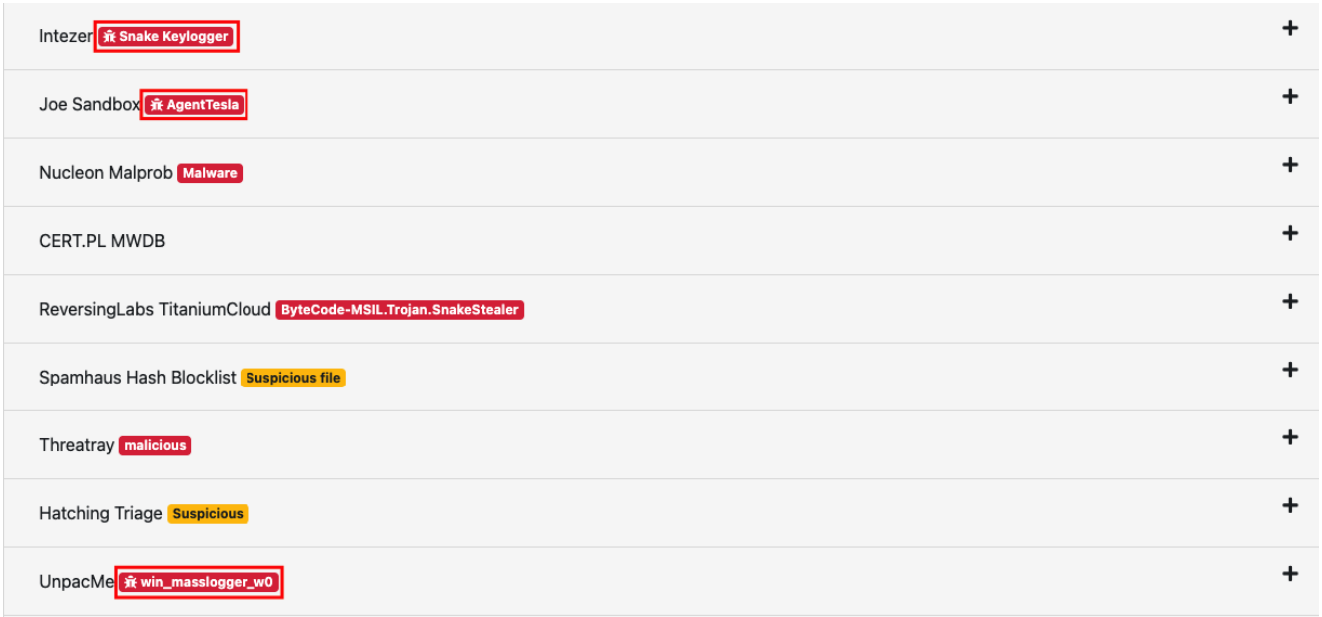
all files are pretty recent (oldest one dated to `7th of May 23`), this in fact helps us to understand that the campaign is pretty new and keeps being distributed.

Some files were already analyzed by various sandboxes and this helped me a lot by downloading the file from those sandboxes reports (most Sandboxes I know allow downloading the examined sample). Let's have a look at couple samples that were actually flagged falsely

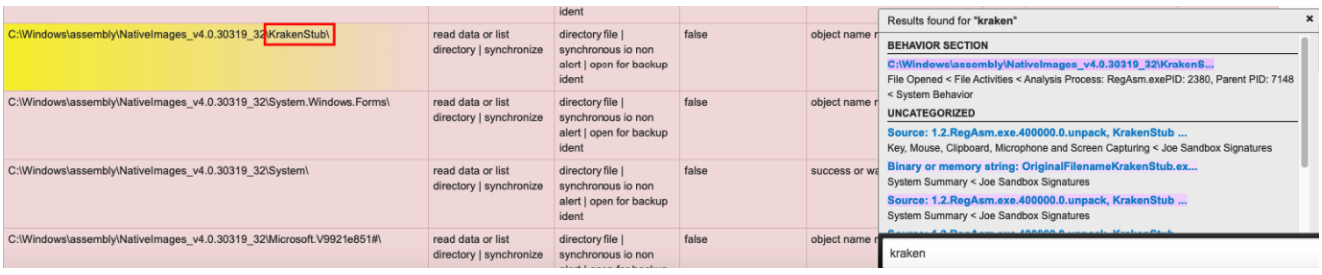
RareCommodityHelper.exe

- Sha256: 8a6bebf08f6c223ed9821ee3b80e420060c66770402687f5c98555f9b0cd02a3
- VirusTotal
- MalwareBazaar

Looking at the `Vendor Threat Intelligence` tab in the MalwareBazaar report we can see that 3 different family associated with the sample.

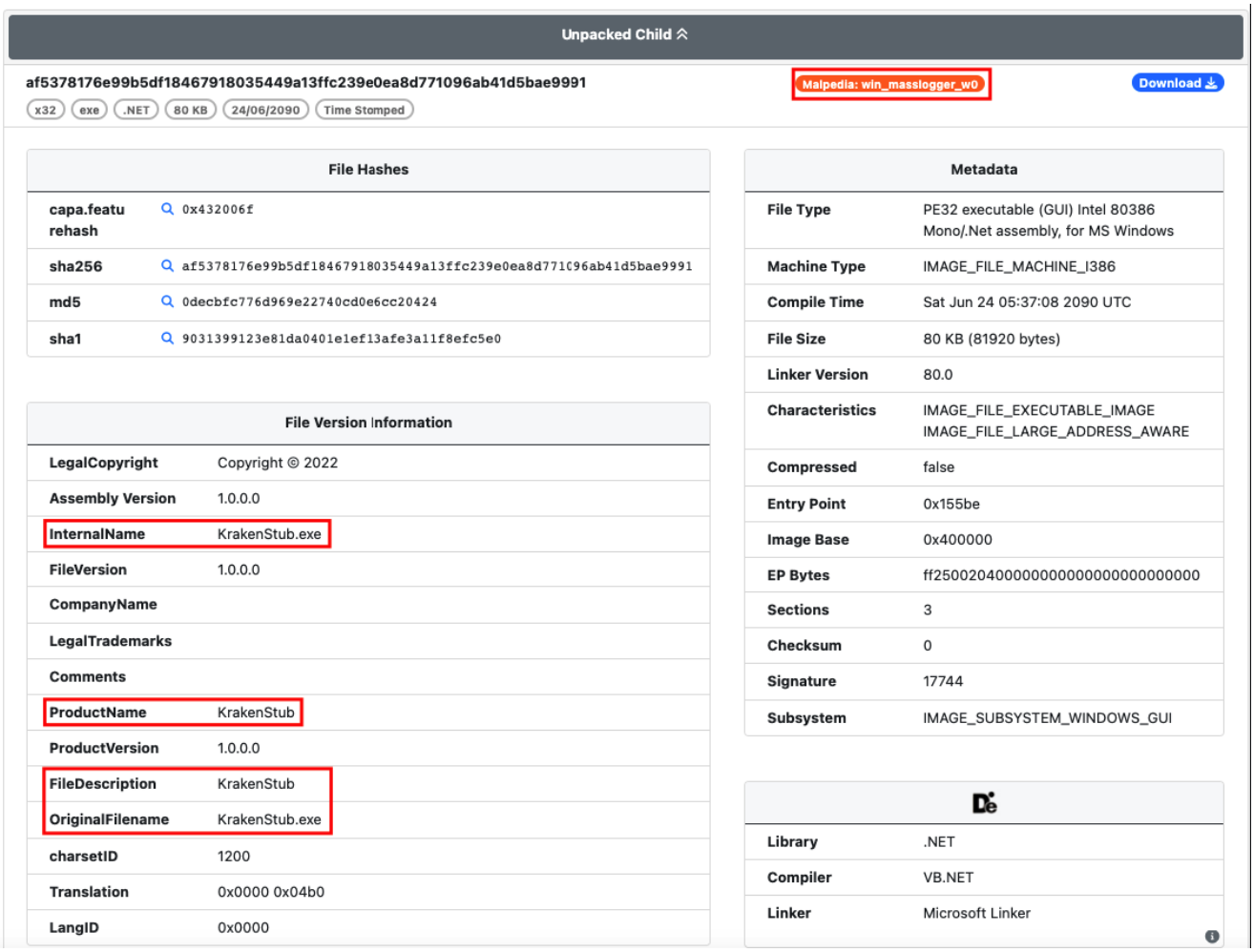


I've opened the report of JoeSandBox and simply searched for the string `kraken` and surprisingly look what popped up:



Why would `AgentTesla` malware will have `KrakenStub` named file during it's execution?

I took a look also UnpackMe report.
Looking at the Unpacked binary that was flagged as `masslogger` we can see the `ProductName`, `FileDescription`, `OriginalFilename` and `InternalName` share the same suspicious string we're looking for: `KrakenStub`



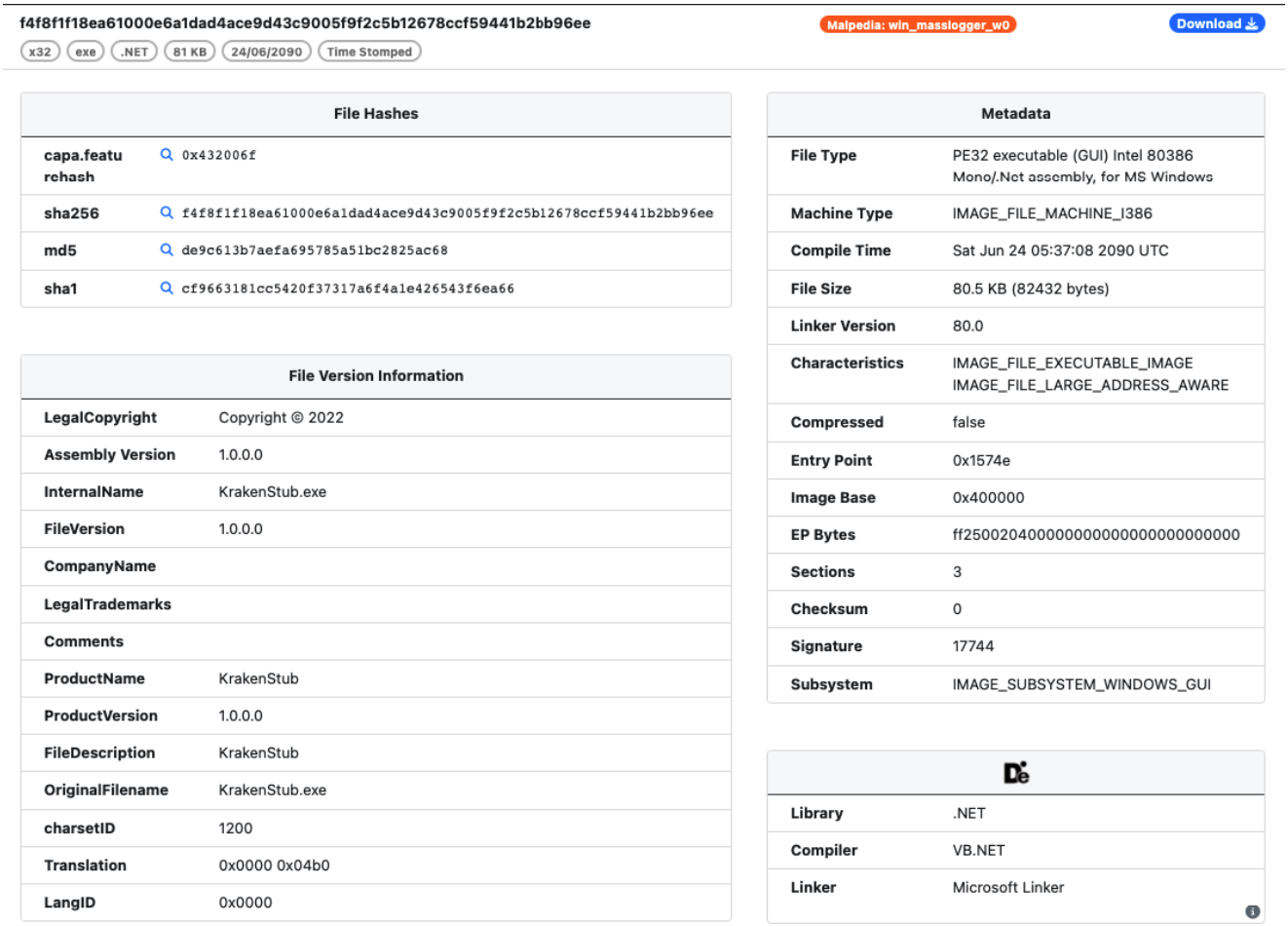
RareCommodityHelper.exe

- Sha256: 413ec94d35627af97c57c6482630e6b2bb299eebf164e187ea7df0a0eb80ecc6
- VirusTotal
- MalwareBazaar

Going with the same approach as before, I took a look at the report of the different vendors under MalwareBazaar page and found again 3 different families:

Intezer Snake Keylogger	+
Joe Sandbox AgentTesla	+
Nucleon Malprob Malware	+
CERT.PL MWDB	+
ReversingLabs TitaniumCloud Win32.Trojan.Zusy	+
Spamhaus Hash Blocklist Suspicious file	+
Threatray malicious	+
Hatching Triage Suspicious	+
UnpacMe win_masslogger_w0	+

I once again checked if our suspicious `Kraken` string can be found either in JoeSandbox or UnpackMe reports and guess what?



Kraken was found in both of them once again.
At this point I felt comfortable with my findings from the C2 IOC.
Let's move to the second domain we have.

masherofmasters.cyou Analysis

Typically when I encounter a domain I will investigate it in 3 main sources:

1. VirusTotal
2. URLscan
3. URLhaus

those 3 are my ***go to*** sources for inital domain information gathering.

VirusTotal

Looking at the domain on VirusTotal can give us a lot of data, such as DNS records, JARM fingerprints, SSL Certs, WhoIS lookup and much more, but the interesting part that I look when doing a proactive hunt is the Relations tab , this tab can tell us which IP's this domain was assigned to, if it has subdomains and which **associated files** this domain had connection with:

Communicating Files (7)

Scanned	Detections	Type	Name
2023-05-20	34 / 60	Windows shortcut	Payment.lnk
2023-05-20	34 / 60	Windows shortcut	Invoice.lnk
2023-05-23	35 / 61	ZIP	79571f0ad832a31a1121f7c698496de7e4700271ccf0a7ed7fe817688528a953
2023-05-20	35 / 60	Windows shortcut	Payment.lnk
2023-05-20	34 / 60	Windows shortcut	Invoice.lnk
2023-05-14	37 / 71	Win32 EXE	money generator.exe
2023-05-25	35 / 60	Windows shortcut	beec3ec08fba224c161464ebcc64727912c6678dd452596440809ce99c8390fd

Based on the given list, we can see that 5 files were `.lnk` files, which correlated with our execution flow explained in part 1. (from here you can take the files and see the execution flow when they're detonated and compare to your findings)

URLscan

Unfortunetlly at the time of investigation the domain was already terminated and no previous scans were made on URLscan so I couldn't find nothing about it here…

URLhaus

When I searched the domain in URLhaus I found about 12 hits:

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2023-05-11 19:17:14	https://masherofmasters.cyou/chin/se1.exe	Offline	MassLogger opendir	abuse_ch
2023-05-11 19:17:13	https://masherofmasters.cyou/chin/eng1.exe	Offline	opendir SnakeKeylogger	abuse_ch
2023-05-11 19:17:12	https://masherofmasters.cyou/chin/eng1.hta	Offline	opendir	abuse_ch
2023-05-11 19:17:12	https://masherofmasters.cyou/chin/ka1.exe	Offline	MassLogger opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/ka1.hta	Offline	opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/ob1.hta	Offline	opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/se1.hta	Offline	opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/no.hta	Offline	opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/no.exe	Offline	MassLogger opendir	abuse_ch
2023-05-11 19:17:11	https://masherofmasters.cyou/chin/ob1.exe	Offline	MassLogger opendir	abuse_ch
2023-05-11 19:16:17	https://masherofmasters.cyou/chin/coco1.hta	Offline	AgentTesla hta opendir	abuse_ch
2023-05-11 19:16:16	https://masherofmasters.cyou/chin/coco1.exe	Offline	AgentTesla exe opendir	abuse_ch

Some of the files are being flagged as `MassLogger` others were flagged as `SnakeKeylogger` and also `AgentTesla` , I investigated all the files and actually the ones that were marked as `AgentTesla` were indeed that malware but the samples which were flagged as `MassLogger` and `SnakeKeylogger` were actually our beloved `Kraken`…

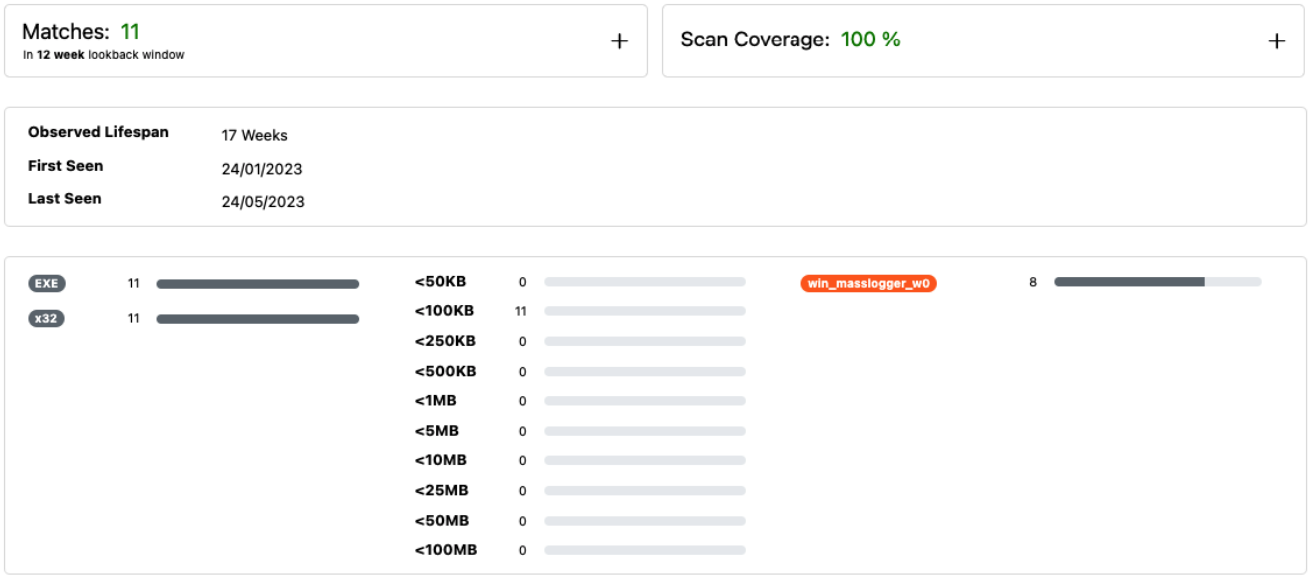
UnpackMe Yara Hunt

UnpackMe provides a unique service of proactive lookback on samples analyzed by the platform based on a given Yara rule
The rule I've created was simply based on unique strings that I found in the sample:

```
rule Win_KrakenStealer {
    meta:
        description = "Win_KrakenStealer rules"
    strings:
                $s1 = "KrakenStub" ascii wide
                $s2 = "KrakenStub.exe" ascii wide
                $s3 = "Kraken_Keylogs_" ascii wide
                $s4 = "Kraken_Password_" ascii wide
                $s5 = "Kraken_Screenshot_" ascii wide
                $s6 = "Kraken_Clipboard_" ascii wide
                $s7 = "KrakenClipboardLog.txt" ascii wide

    condition:
        uint16(0) == 0x5a4d and 5 of ($s*)
}
```

And here is the result of the hunt:



In a 12 weeks lookback there were 11 samples that fitted the given Yara Rule, **8** of them were marked as `MassLogger`, so I took a look at one of them

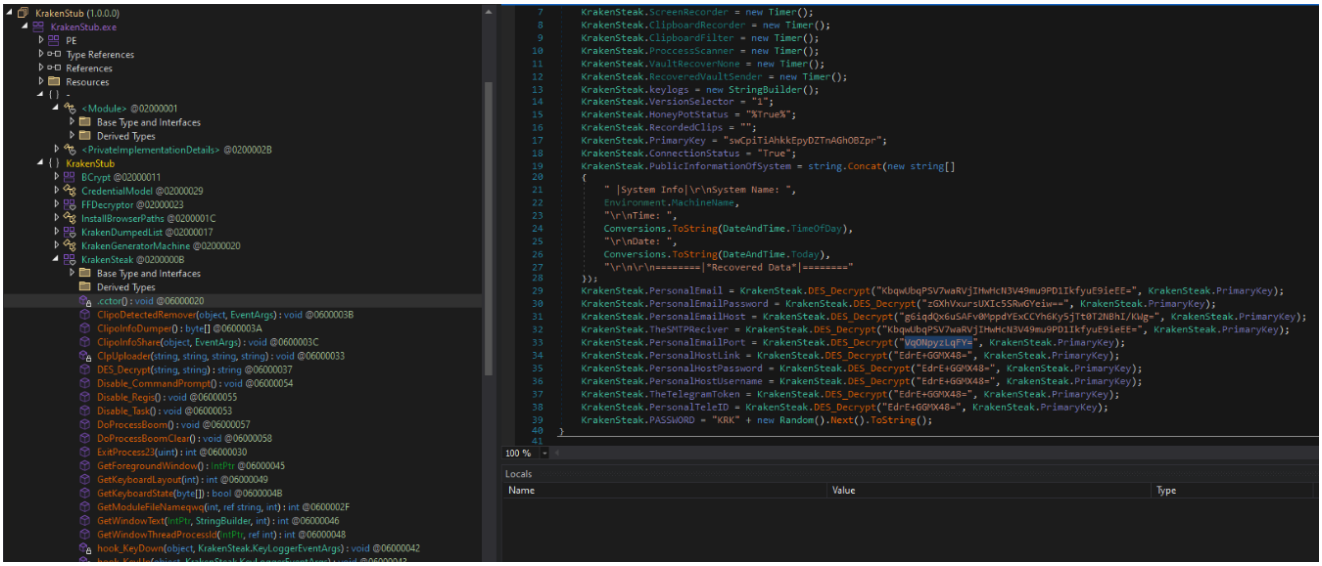
File Hashes	
capa.featurehash	0x432006f
sha256	3d680334931e422f3876eaa6df752da015a902270f73cdfb8f6812910b48c3c2
md5	877585dac8c00884cef2c3bc36e4b263
sha1	1288ab36ba6257e02b748615e979377e381d74b0

File Version Information	
LegalCopyright	Copyright © 2022
Assembly Version	1.0.0.0
InternalName	KrakenStub.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	KrakenStub
ProductVersion	1.0.0.0
FileDescription	KrakenStub
OriginalFilename	KrakenStub.exe
charsetID	1200
Translation	0x0000 0x04b0
LangID	0x0000

Metadata	
File Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Machine Type	IMAGE_FILE_MACHINE_I386
Compile Time	Sat Jun 24 05:37:08 2090 UTC
File Size	80.5 KB (82432 bytes)
Linker Version	80.0
Characteristics	IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LARGE_ADDRESS_AWARE
Compressed	false
Entry Point	0x1576e
Image Base	0x400000
EP Bytes	ff25002040000000000000000000000
Sections	3
Checksum	0
Signature	17744
Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI

.NET	
Library	.NET
Compiler	VB.NET
Linker	Microsoft Linker

and by simply looking at the `File Version Information` we can see that it's 99% our `Kraken` , I downloaded the sample and opened it in `DnSpy` and guess what?



It was our `Kraken`! so we found about 11 samples that are flagged falsely.
And with that our hunt for samples is done, from here you can pretty much correlate some IOC's so see whether or not it's the same threat actor.

OSINT Research

At this part I wanted to try and find the origin of the malware, so I tried two things:

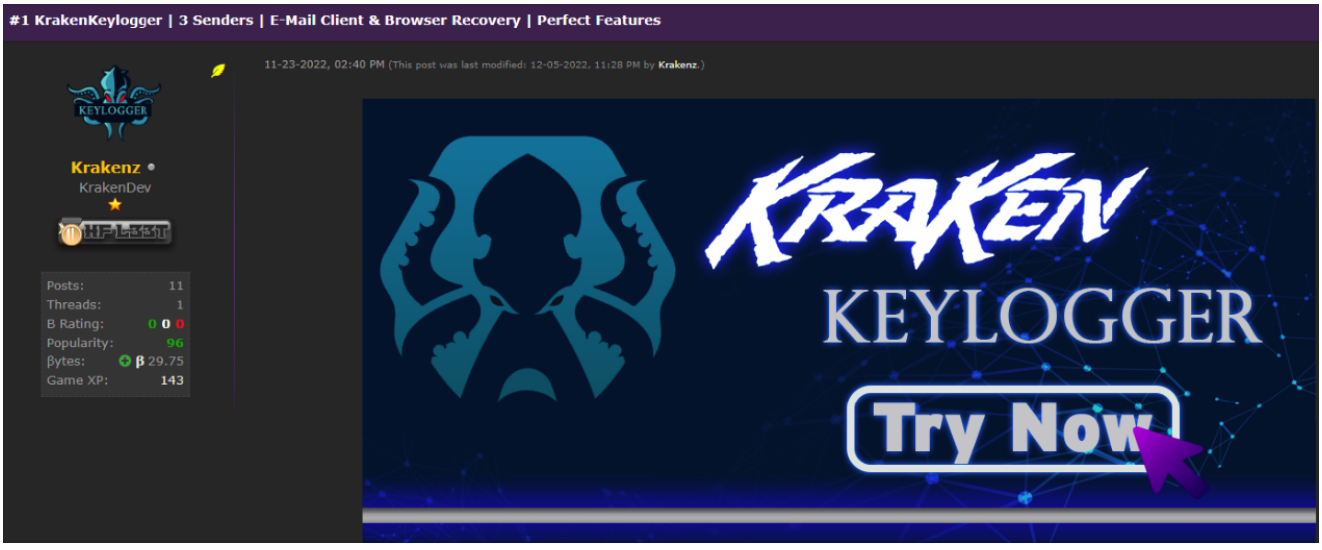
1. Search engine dorking
2. Underground forums

Search Engine Dorking

I tried to search the term `"KrakenStub" malware` both in Google and DuckDuckGo, besides giving me 2 analysis one of JoeSandbox and the second one of Vmray I couldn't finding anything useful but it always good to try and search using search engines because you can't really know what you can find…

Underground Forums

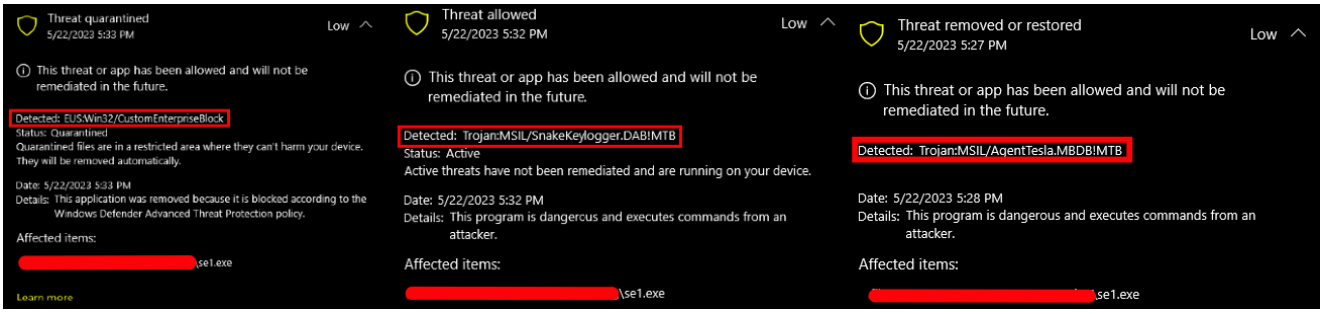
there are several underground/hacking forums that you can find on the clean web without the needs going to TOR and pivoting around the darknet.
One of the most known hacking forums out there is HackForums , so I tried my luck and searched through the marketplace forum for "Kraken" keywords, and after quite some time and found this thread :***#1 KrakenKeylogger | 3 Senders | E-Mail Client & Browser Recovery | Perfect Features*** sold by a user named `Krakenz`:



What a perfect hit!
that particular finding made my day, I knew that this is it, I've closed the circle and I can close this case and fully resolved.

Extra Findings

After I've published part 1 of analyzing the Kraken, @jw4lsec and me had a small conversation and he shared with me that Windows Defender was flagging the sample I've shared during the investigation as a different malware upon each different execution attempt:



Summary

In the 2nd part of analyzing the Kraken I've showed you my way of thinking and approach to the process of threat hunting, especially when your guts tells you that something here is not right. I hope that during those 2 parts of analysis you've learned new things, feel free to PM me via any social media.