Kraken - The Deep Sea Lurker Part 2

Oxtoxin.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 <u>here</u> 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 <u>VirusTotal</u> 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 (2	22) 🛈		
Scanned	Detections	Туре	Name
2023-05-15	<mark>46</mark> / 65	ZIP	03cd9b875668d603ac396a9b2efe1b13871513cbb693413497bb674b5df22af2.zip
2023-05-07	<mark>42</mark> / 70	Win32 EXE	Copy.exe
2023-05-24	30 / 71	Win32 EXE	SuperAraneid.exe
2023-05-20	<mark>34</mark> / 60	Windows shortcut	Payment.lnk
2023-05-18	<mark>49</mark> / 71	Win32 EXE	21d0345174d67986202fdecdf8e56493628d9e66eafdf4002a8dacb84c46d779
2023-05-15	<mark>46</mark> / 63	ZIP	Copy.zip
2023-05-24	<mark>32</mark> / 72	Win32 EXE	SuperAraneid.exe
2023-05-18	<mark>53</mark> / 71	Win32 EXE	osukps.exe
2023-05-13	<mark>35</mark> / 60	Windows shortcut	5b52facac06e5e115c54fec3f13b08ebba46f4850306fe9766ac0e7594de02ff.lnk
2023-05-20	<mark>43</mark> / 65	ZIP	PO-87098.zip
2023-05-13	<mark>40</mark> / 65	ZIP	P0-231062_zip.bin
2023-05-24	<mark>53</mark> / 71	Win32 EXE	CgLogListener.exe
2023-05-23	<mark>44</mark> / 65	ZIP	7ddacf946c3de29255d826fbce407672c991285e15bf4a0e33f28561847b7d6f.zip
2023-05-09	17 / 64	ZIP	3dab175a0cbfd28182ea5c9b27c10274.file
2023-05-23	<mark>50</mark> / 71	Win32 EXE	Observatory.exe
2023-05-20	<mark>35</mark> / 60	Windows shortcut	Payment.lnk
2023-05-24	<mark>22</mark> / 71	Win32 EXE	SuperAraneid.exe
2023-05-13	<mark>56</mark> / 71	Win32 EXE	ChessTables.exe
2023-05-13	<mark>45</mark> / 71	Win32 EXE	74b46e9615014e0e39d809cc469c7a061093210b.bin
2023-05-23	<mark>33</mark> / 60	Windows shortcut	Swift-Copy.Ink
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
- <u>MalwareBazaar</u>

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

Intezer 🕱 Snake Keylogger	+
Joe Sandbox 🙀 AgentTesla	+
Nucleon Malprob Malware	+
CERT.PL MWDB	+
ReversingLabs TitaniumCloud ByteCode-MSIL.Trojan.SnakeStealer	+
Spamhaus Hash Blocklist Suspicious file	+
Threatray malicious	+
Hatching Triage Suspicious	+
UnpacMe 🕷 win_masslogger_w0	+

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

		tata at				
		ident			Results found for "kraken"	×
C:\Windows\assembly\NativeImages_v4.0.30319_32KrakenStub\	read data or list directory I synchronize	directory file synchronous io non	false	object name r	BEHAVIOR SECTION	ī
		alort open for backup			C:\Windows\assembly\Nativolmages_v4.0.30319_32\KrakenS Ella Opened - Ella Artivities - Applysis Process: PagAem avaPID: 2380, Parent PID: 7148	
					< System Behavior	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\	read data or list directory synchronize	directory file synchronous io non	false	object name r	UNCATEGORIZED	
		alert open for backup ident			Source: 1.2.RegAsm.exe.400000.0.unpack, KrakenStub Key, Mouse, Clipboard, Microphone and Screen Capturing < Joe Sandbox Signatures	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\	read data or list	directory file	false	success or wa	Binary or memory string: OriginalFilenameKrakenStub.ex System Summary < Joe Sandbox Signatures	1
	directory synchronize	alert open for backup			Source: 1.2.RegAsm.exe.400000.0.unpack, KrakenStub	
		ident			System Summary < Joe Sandbox Signatures	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\	read data or list	directory file	false	object name r	Courses & O. Den Anne and 4000000. Courses in Mashing Olivit	-
	directory synchronize	synchronous io non			kraken	

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

I took a look also <u>UnpackMe</u> 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

		Unpacked Child 🛠				
f5378176e99b5df1 x32) (exe) (.NET) (8467918035449a13ff 80 KB 24/06/2090 (T	c239e0ea8d771096ab41d5bae9991 ime Stomped		Malpedia: win_m	asslogger_w0	Download 날
	l	File Hashes			Metadata	
capa.featu O rehash	0x432006f			File Type	PE32 executable (GUI) In Mono/.Net assembly, for	ntel 80386 MS Windows
sha256 O	af5378176e99b5df184	67918035449a13ffc239e0ea8d771096ab41d5bae9991		Machine Type	IMAGE_FILE_MACHINE_	1386
md5 O	0decbfc776d969e2274	0cd0e6cc20424		Compile Time	Sat Jun 24 05:37:08 20	90 UTC
sha1 O	9031399123e81da0401	elefl3afe3allf8efc5e0		File Size	80 KB (81920 bytes)	
				Linker Version	80.0	
	File Ve	rsion Information		Characteristics	IMAGE_FILE_EXECUTAE IMAGE_FILE_LARGE_AD	LE_IMAGE DRESS_AWARE
LegalCopyright	Copyright © 202	2		Compressed	false	
Assembly Version	n 1.0.0.0			Entry Point	0x155be	
InternalName	KrakenStub.exe			Image Base	0x400000	
FileVersion	1.0.0.0			EP Bytes	ff2500204000000000	000000000000000000000000000000000000000
CompanyName				Sections	3	
LegalTrademarks	3			Checksum	0	
Comments				Signature	17744	
ProductName	KrakenStub			Subsystem	IMAGE_SUBSYSTEM_W	NDOWS_GUI
ProductVersion	1.0.0.0					
FileDescription	KrakenStub				D'	
OriginalFilename	KrakenStub.exe		-	1 iburuu	Le	
charsetID	1200			Commilian		
Translation	0x0000 0x04b0			Compiler	VB.NET	
LangID	0x0000			Linker	Microsoft Linker	0

RareCommodityHelper.exe

- Sha256: 413ec94d35627af97c57c6482630e6b2bb299eebf164e187ea7df0a0eb80ecc6
- VirusTotal
- <u>MalwareBazaar</u>

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 <mark> </mark>	+

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

C:\Windows\assembly\NativeImages_v4.0.30319_32\KrakenStub\	read data or list directory synchronize	directory file synchronous io non alert open for backup ident	false	object name r	Results found for "kraken" X BEHAVIOR SECTION C:Windowslassembly/WativeImages v4.0.30319 32(KrakenS
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\	read data or list directory synchronize	directory file synchronous io non alert open for backup ident	false	object name r	File Opened < File Activities < Analysis Process: RegAsm.exePID: 5124, Parent PID: 7040 < System Behavior UNCATEGORIZED Source: 12. RepAsm.exe.400000.0.unpack. KrakenStub
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\	read data or list directory synchronize	directory file synchronous io non alert open for backup ident	false	success or wa	Key, Mouse, Clipboard, Microphone and Screen Capturing < Joe Sandbox Signatures Binary or memory string: OriginalFilenameKrakenStub.ex System Summary < Joe Sandbox Signatures Source: 12. ReaAsm.oxe.400000.0.unpack. KrakenStub
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\	read data or list	directory file	false	object name r	System Summary < Joe Sandbox Signatures

x32 exe .NET 81 KB 24/06/2090 Time Stomped

Malpedia: win_masslogger_w

File Type

Machine Type

Compile Time

File Size Linker Version Metadata

80.0

PE32 executable (GUI) Intel 80386 Mono/.Nct assembly, for MS Windows

IMAGE FILE MACHINE 1386

Sat Jun 24 05:37:08 2090 UTC 80.5 KB (82432 bytes)

Download 🛓

8

	File Hashes
capa.featu rchash	Q 0x432006f
sha256	Q f4f8f1f18ea61000e6aldad4ace9d43c9005f9f2c5b12678ccf59441b2bb96ee
md5	Q de9c613b7aefa695785a51bc2825ac68
sha1	Q cf9663181cc5420f37317a6f4a1e426543f6ea66

	File Version Information	Characteristics	IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LARGE_ADDRESS_AWARE
LegalCopyright	Copyright © 2022	Compressed	false
Assembly Version	1.0.0.0	Entry Point	0x1574e
InternalName	KrakenStub.exe	Image Base	0x400000
FileVersion	1.0.0.0	EP Bytes	ff25002040000000000000000000000000000000
CompanyName		Sections	3
LegalTrademarks		Checksum	0
Comments		Signature	17744
ProductName	KrakenStub	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI
ProductVersion	1.0.0.0		
FileDescription	KrakenStub		R.
OriginalFilename	KrakenStub.exe		Le
charsetID	1200	Library	.NET
Translation	0x0000 0x04b0	Compiler	VB.NET
LangID	0x0000	Linker	Microsoft Linker

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 <u>Relations tab</u>, 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) ①							
Scanned	Detections	Туре	Name				
2023-05-20	<mark>34</mark> / 60	Windows shortcut	Payment Ink				
2023-05-20	<mark>34</mark> / 60	Windows shortcut	Invoice.Ink				
2023-05-23	<mark>35</mark> / 61	ZIP	79571f0ad832a31a1121f7c698496de7e4700271ccf0a7ed7fe817688528a953				
2023-05-20	<mark>35</mark> / 60	Windows shortcut	Payment.lnk				
2023-05-20	<mark>34</mark> / 60	Windows shortcut	Invoice.Ink				
2023-05-14	37 / 71	Win32 EXE	money generator.exe				
2023-05-25	<mark>35</mark> / 60	Windows shortcut	beec3ec08fba224c161464ebcc64727912c6678dd452596440809ce99c8390fd				
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

Unfortunetly 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

<u>UnpackMe</u> provides a unique service of proactive lookback on samples analyzed by the platform based on a given <u>Yara rule</u>

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:
        $$$1 = "KrakenStub" ascii wide
        $$2 = "KrakenStub.exe" ascii wide
        $$3 = "Kraken_Keylogs_" ascii wide
        $$4 = "Kraken_Password_" ascii wide
        $$5 = "Kraken_Screenshot_" ascii wide
        $$6 = "Kraken_Clipboard_" ascii wide
        $$7 = "KrakenClipboardLog.txt" ascii wide
        $$7 = "KrakenClipboardLog.txt" ascii wide
        $$1 = "Kraken_Sof ($$*)
}
```

And here is the result of the hunt:

Matches: 11 In 12 week lookback window				+	Scan C	overage: 100 %		+
Observed Lifespan First Seen Last Seen	17 Weeks 24/01/2023 24/05/2023							
EXE 11		<50KB <100KB <250KB <500KB <1MB <5MB <10MB <25MB <50MB <100MB	0 11 0 0 0 0 0 0 0 0 0 0 0			win_masslogger_w0	8	

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 <u>one of them</u>

	File Hashes
capa.fea rehash	tu Q 0x432006f
sha256	Q 3d680334931e422f3876eaa6df752da015a902270f73cdfb8f6812910b48c3c2
md5	Q 877585dac8c00884cef2c3bc36e4b263
sha1	Q 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	ff25002040000000000000000000000000000000		
Sections	3		
Checksum	0		
Signature	17744		
Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI		

	De	
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 <u>HackForums</u>, so I tried my luck and searched through the marketplace forum for "Kraken" keywords, and after quite some time and found <u>this thread</u> :**#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, <u>@jw4lsec</u> 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.