Vidar Stealer

TECHNICAL ANALYSIS REPORT

Index
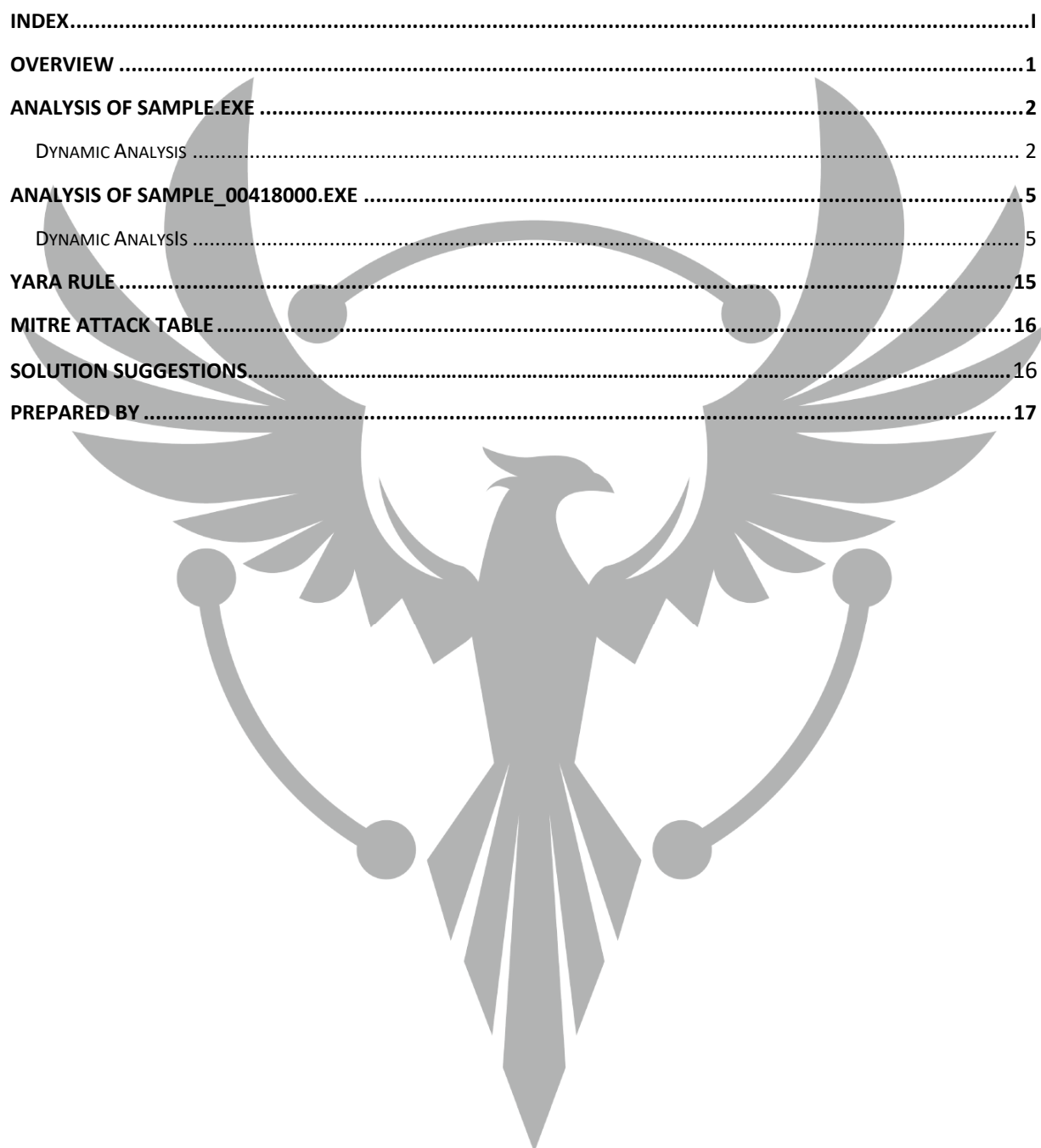
Overview

The malware from the Vidar family appears as an EXE file. This malicious software can access personal information, cryptocurrency wallet data, and cookie information on infected computers. It was first discovered in late 2018 and has been regularly updated and improved since then. The malware can be spread through malicious links or attachments sent via email, downloaded fake files or applications, malvertising, and social engineering attacks.
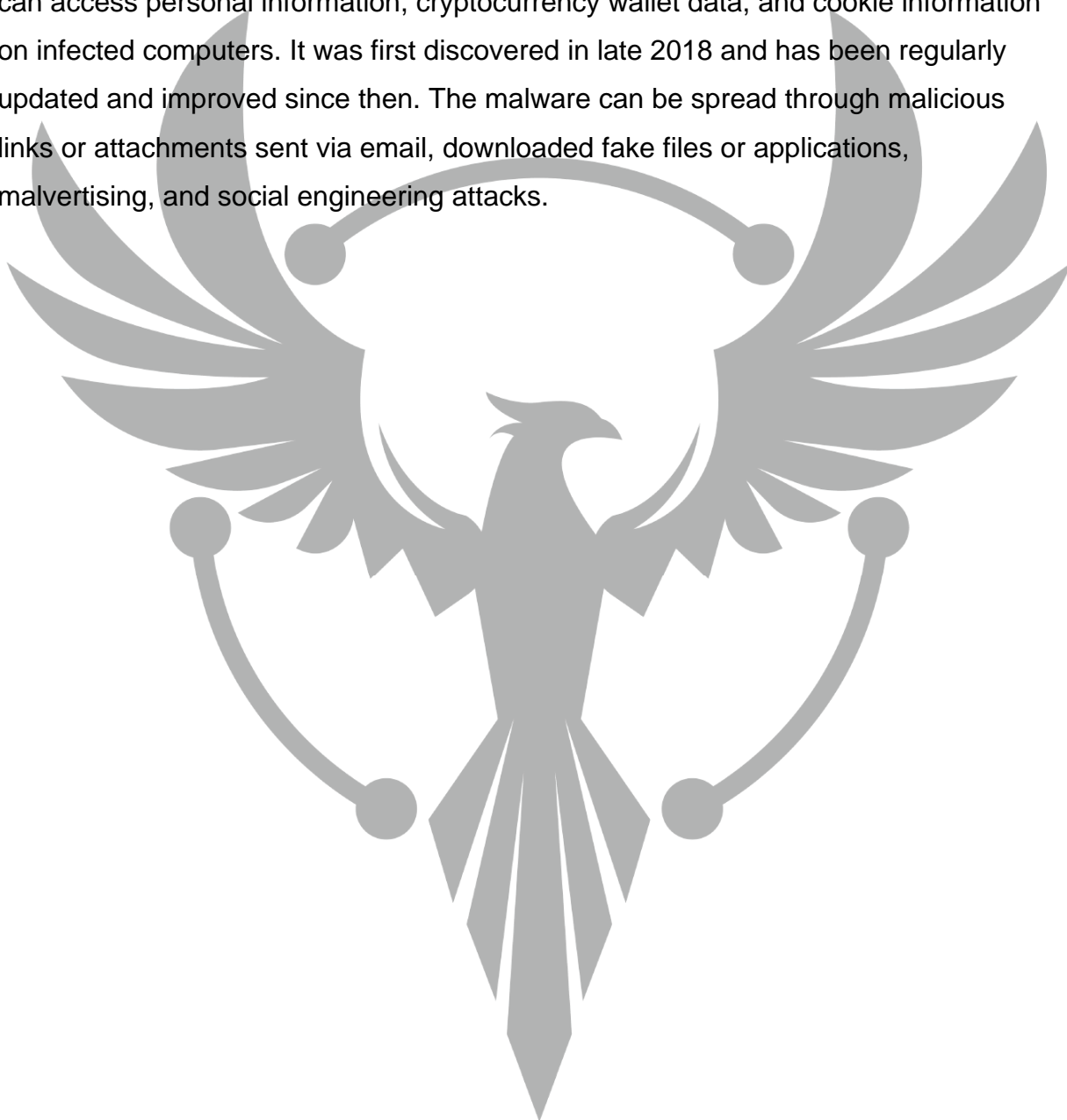
Analysis of sample.exe

File Name	sample.exe
MD5	701477F861BDE9756D5FC3ACE9D2F019
SHA256	2E0F06DF176B574CD8F629F8E0D32FDEDC72DD20
File Type	PE32/EXE

The MD5, SHA-1, and SHA-256 hashes of the malware are listed in the table. The original name is 48aa1381548b2590a3ae1d740852fdefdf51c46666ee2d86e50aeae66afbda60.exe, but it has been renamed to sample.exe for ease of analysis.

Dynamic Analysis


```
mov     dword ptr [ebp+var_820+4], edx
push    42h ; 'B'
push    77Eh
lea     eax, [ebp+var_7B0]
push    eax
push    offset a3h8w2npbk4nrdu ; "3h8W2nPBk4nRDUrB6Y0h0HLpyqaFdsG77R2qmHs"...
call    sub_401080
```

Figure 2. The string used by the malware

When the malware is examined, the string named **3h8W2nOBk4nRDUrB6Y0HLpyqaFdsG77R2qmHs** draws attention. When the function it calls is examined, it is seen that it is a harmless Shellcode that performs jump operations in memory. It is understood that this string was inserted to confuse.

Figure 3. Jump operations in Memory

Figure 4. The string used by the malware

When the malware is examined, another string named
tsUYxh4R2BMPl6IVK7msKOJi8MeYnj3B4ogS6KP stands out. This string is
assigned to the function named **sub_401000**.

Figure 5. Injected PE file

Upon entering and examining the function **sub_401000**, it is understood that a PE file is injected into sample.exe with the pop esi instruction. The dump was followed in the memory map and then saved as **SAMPLE_00418000.EXE**. The .exe file that was recorded was analyzed statically and dynamically.

Analysis of sample_00418000.exe

File Name	sample_00418000.exe
MD5	35EBCE61CD83460135893269B991E740
SHA256	DA39750642B84880BD1E882E3EF53C7E72C42366
File Type	PE32/EXE

The MD5 and SHA-256 information of the dropped .exe file is given in the table. It is named sample_00418000.exe for ease of analysis.

Dynamic Analysis

Figure 6. APIs used by malware

In the first phase, the malware collects general information about the system. The APIs it uses are given in the table below.

	Gets the current system date and time. The information is in Coordinated Universal Time (UTC) format.
GetSystemTimeAsFileTime	
GetCurrentProccessId	Gets the process identifier of the calling process

GetCurrentThreadId	Gets the thread identifier of the calling thread
GetTickCount	Gets the number of milliseconds (up to 49.7 days) since system initialization.
QueryPerformanceCounter	Gets the current value of the performance counter with a high resolution (<1us) timestamp that can be used for time interval measurements.

Figure 7. Impossible Disassembly Technique

When the dropped .exe file is examined in the Disassembler program, it is understood that the Impossible Disassembly technique is used. This technique is an Anti-Disassembly technique that aims to make reverse engineering difficult. As shown in the figure, data bytes are added to the conditional skip directive. These data bytes are designed to prevent the disassembly algorithm from disassembling the actual instruction after the jump instruction. The B8 opcode in the figure is not used at all because it is skipped. Since the disassembler cannot make sense of these parts, it misinterprets them. This technique is often used in malware and other unsafe software.

Figure 8. Impossible Disassembly technique before decoding

We analyze the impossible disassembly technique by replacing the B8 opcode in the figure with 90, that is, by filling it with NOP.

Figure 9. After analyzing the Impossible Disassembly technique

In this way, the malware can be analyzed without getting stuck in the Disassembler.

To avoid malware that uses Impossible Disassembly tactics:

- Download software from trusted sources.
- Keep the software up to date.
- Use an antivirus program.
- Analyze your computer's software with special tools designed for reverse engineering.

Figure 10. Telegram bot URL address

The dropped .exe file contains the URL address of the telegram bot used for the C&C server.

Figure 11. Telegram bot
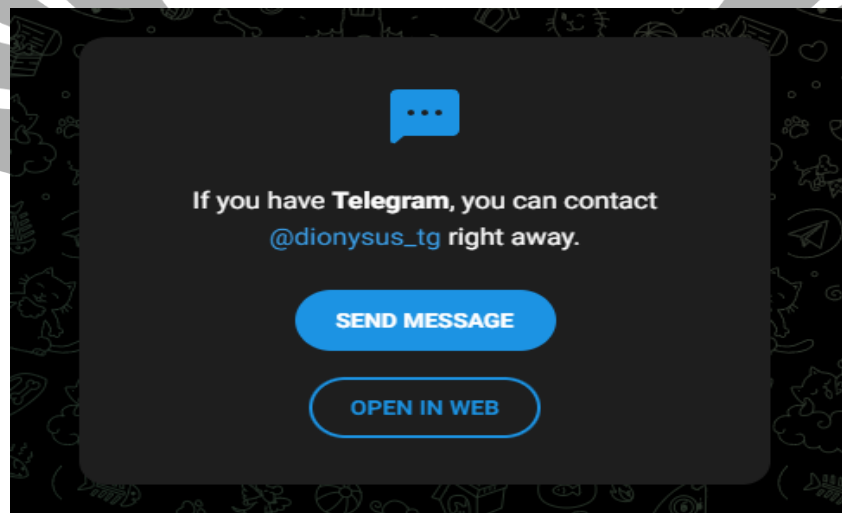

Figure 1. Steam URL address

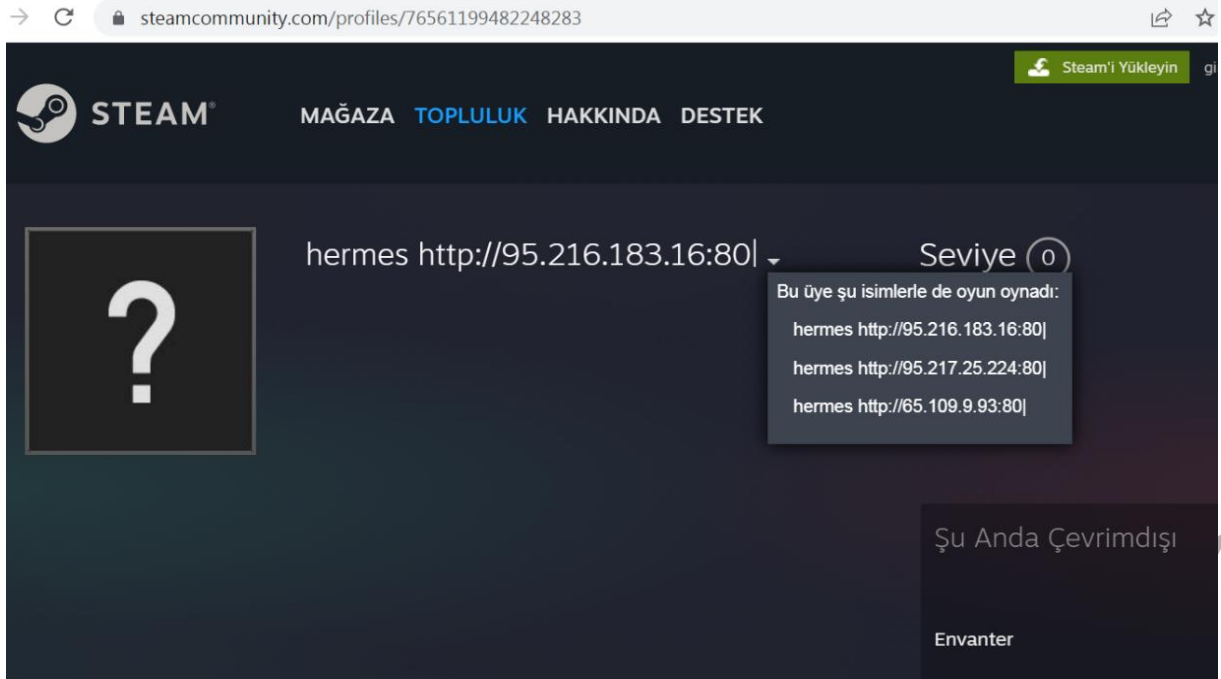The dropped .exe file contains the steamcommunity URL address.

Figure 2. Steam profile page

Using the steamcommunity URL address, the malware sends an HTTP GET request to hermes http[:]//95[.]216[.]183[.]183[.]16[:]80, hermes http[:]//95[.]217[.]25[.]224[:]80, hermes http[:]//65[.]109[.]9[.]93[:]80. With this request,

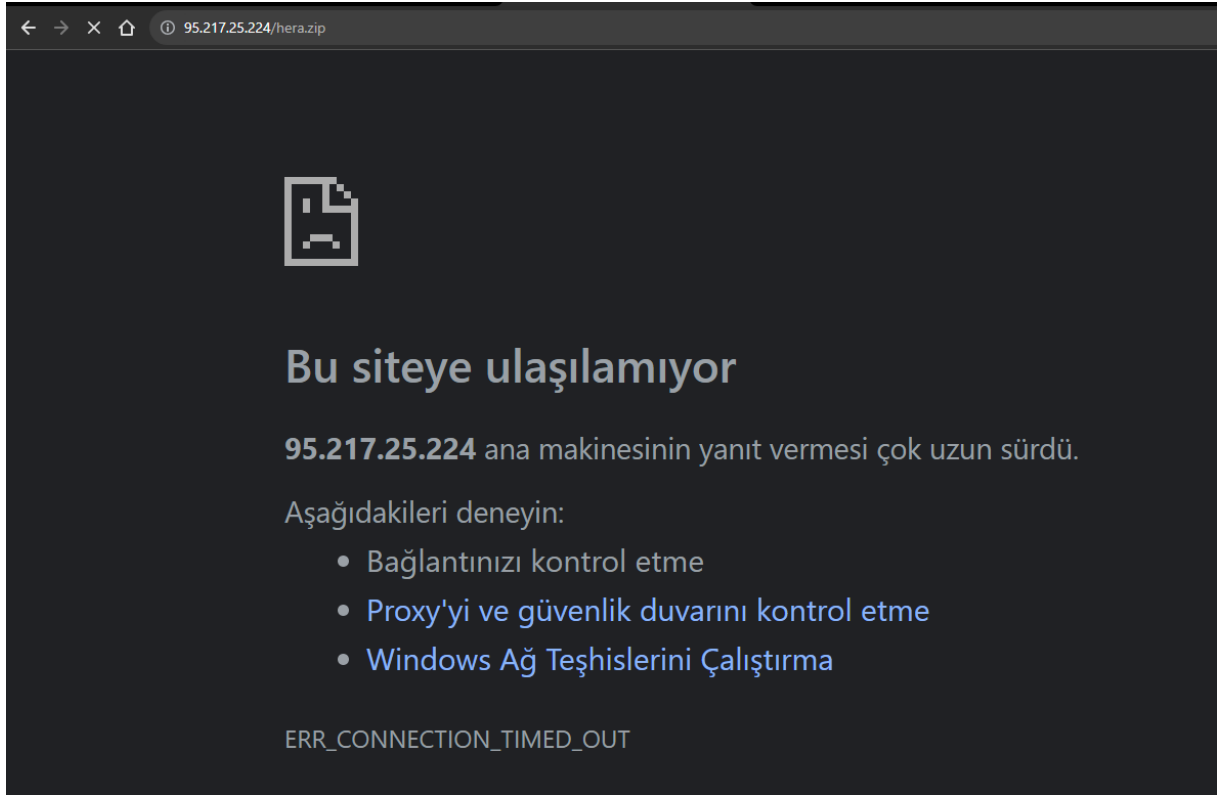the malware tries to pull a file named hera.zip from the server.

Figure 14. web server to pull hera.zip

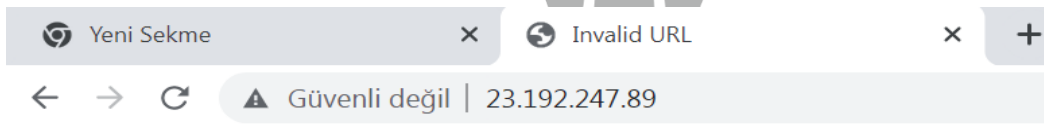It is seen that the server from which the file named hera.zip will be extracted is down.

Figure 15. Request discarded from local machine

Figure 3. Wireshark screenshot

At the same time, it is seen that the malware also sends requests to the IP address **23[.]192[.]192[.]247[.]89** from the local machine.

Invalid URL

The requested URL "[no URL]", is invalid.

Reference #9.5d161102.1697050990.e66b895

Figure 4. Invalid IP address

Looking at the IP address **23[.]192[.]192[.]247[.]89,** it is seen that it is invalid.

Figure 18. string references in the module

Figure 19. assembly view

The malware has a common function for encrypting strings and wallet addresses.

Figure 5. ida and pseudo code view

While many of these were strings used in wallet transactions, the decryption function (EC4620) was used in many parts of the malware.

Figure 21. decryption function

The general structure of the function is as shown in the picture, but it also leaves a message in memory.

Browser plugins targeted by the malware:

Plug-in ID	Plug-in Name
gojhcdgcpbpfigcaejpfhfegekdgiblk	Opera Wallet
pnndplcbkakcplkjnolgbkdgjikjednm	Tronium
egjidjbpglichdcondbcbdnbeeppgdph	Trust Wallet
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
jnlgamecbpmbajjfhmmmlhejkemejdma	Braavos
kkpllkodjeloidieedojogacfhpaihoh	Enkrypt
mcohilncbfahbmgdjkbpemcciiolgcge	OKX Web3 Wallet
epapihdplajcdnnkdeiahlgigofloibg	Sender
gjagmgiddbbciopjhllkdnddhcglnemk	Hashpack
kmhcihpebfmpgmihbkipmjlmmioameka	Eternl
bgpipimickeadkjlklgciifhnalhdjhe	GeroWallet
phkbamefinggmakgklpkljjmgibohnba	Pontem Wallet
ejjladinnckdgjemekebdpeokbikhfci	Petra Wallet
efbglgofoippbgcjepnhiblaibcnclgk	Martian Wallet
cjmkndjhnagcfbpiemnkdpomccnjblmj	Finnie
aijcbedoijmgnlmjeegjaglmepbmpkpi	Leap Terra

YARA Rule

```
import "hash"

rule sample{

meta:

        author="Team3"

        description="Vidar Stealer"

        first date="16.09.2023"

        report date="16.10.2023"

        file name="sample.exe"

strings:

        $dnm_a="3h8W2nPBk4nRDUrB6Y0h0HLpyqaFdsG77R2qmHs6N
8ItqBhW4SbYsSYEyutCXGUpq"

        $dnm_b="http://ocsp.entrust.net00"

        $dnm_c="tsUYxh4R2BMPl6IVK7msKOJi8MeYnj3B4ogS6KPyHbG
wtYiJEr9efHvkNOaoLGqUp"

        $dnm_d="http://ocsp.digicert.com0X"

        $dnm_e="http://pki.eset.com/csp0"

Condition:

        Hash.md5(0,filesize)=="701477F861BDE9756D5FC3ACE9D2F01
9" or all of them

}
```

MITRE ATTACK TABLE

Execution	Persistence	Defense Evasion	Credential Access	C&C
Windows Management Instrumentation	Account Manipulation	Deobfuscate/Decode Files or Information	OS Credential Dumping	Encrypted Channel
Native API		Obfuscated Files or Information	Input Capture	Ingress Tool Transfer
		Virtualization/Sandbox Evasion	Credentials in Registry	Non-Application Layer Protocol
		Process Injection		Application Layer Protocol

Solution Suggestions

1. Up-to-date, reliable anti-virus software must be used on the systems,

2. Network packets should be filtered and monitored,

3. Make sure that the links clicked are correct and reliable,

4. More reliable cryptocurrency storage methods such as cold wallets should be preferred,

5. Your crypto accounts should use two-factor authentication,

6. In case of suspicion, the network should be monitored and intervened accordingly.

Prepared By

Elif ÇAĞLAR

https://www.linkedin.com/in/elif-%C3%A7a%C4%9Flar-27902b214/

Ömer Faruk SÖNMEZ

https://www.linkedin.com/in/omertheroot

Melike TAŞDELEN

https://www.linkedin.com/in/melike-taşdelen-90345926a/