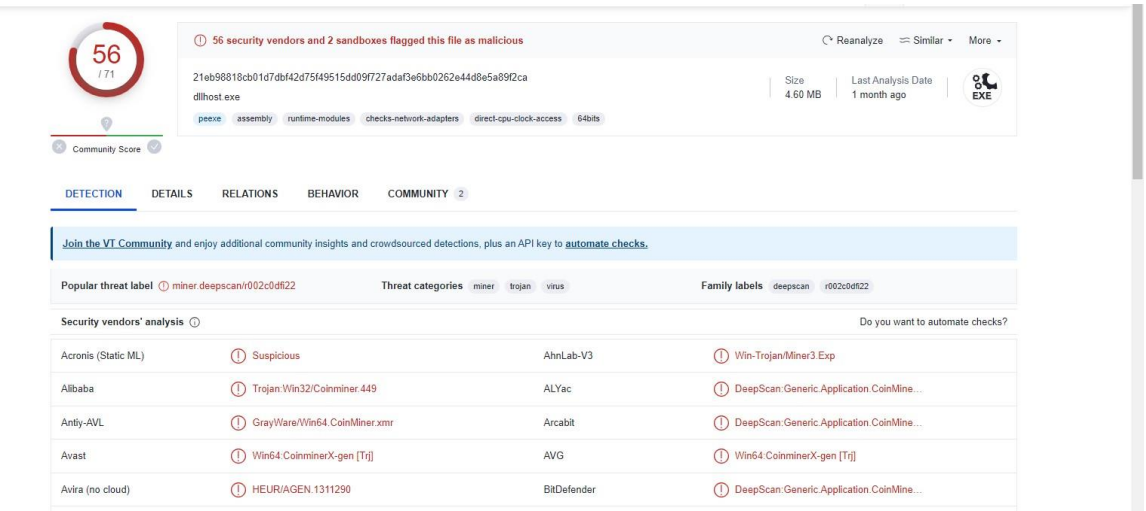
Crypto Mining Malware Analysis Report

Fingerprint

File Name: dllhost.exe

Virus total output



Hashes

MD5: c5a455de612db6ecc5bd9801ff9826a2

SHA-1: c83769ca9d63070af1b3121bf70358e6e90dc7b6

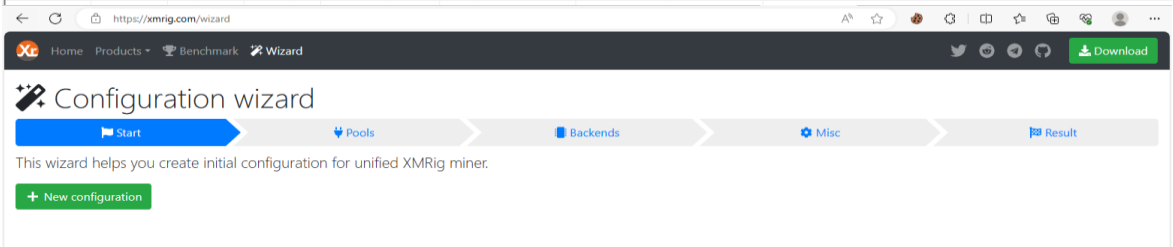
SHA-256: 21eb98818cb01d7dbf42d75f49515dd09f727adaf3e6bb0262e44d8e5a89f2ca

Basic Static Analysis

Malware Seems Packed because ***rawsize*** is too smaller than virtual size

property	value
headers	header[0]
name	.text
footprint > md5	5D38C3FB849DB03CF2C674...
entropy	6.515
file-ratio (99.98%)	71.67 %
raw-address (begin)	0x00000400
raw-address (end)	0x0034D000
raw-size (4826624 bytes)	0x0034CC00 (3460096 bytes)
virtual-address	0x00001000
virtual-size (7576291 bytes)	0x0034CA48 (3459656 bytes)

ascii	6	.rdata	-	-	-	-	x86_64
ascii	5	.rdata	-	-	-	-	flags
ascii	58	.rdata	-	-	-	-	no valid configuration found, try https://xmrig.com/wizard
ascii	30	.rdata	-	-	-	-	[0;33mCtrl+C received, exiting
ascii	3	.rdata	-	-	-	-	[0m



https://xmrig.com/wizard is crypto mining pool

ascii	10	.rdata	-	-	-	-	/getheight
ascii	11	.rdata	-	-	-	-	submitblock
ascii	23	.rdata	-	-	-	-	Invalid wallet address.
ascii	18	.rdata	-	-	-	-	Invalid algorithm.
ascii	8	.rdata	-	-	-	-	get_info
ascii	14	.rdata	-	-	-	-	top_block_hash
ascii	42	.rdata	-	-	-	-	Empty block template received from daemon.
ascii	17	.rdata	-	-	-	-	[0;31mjob error:

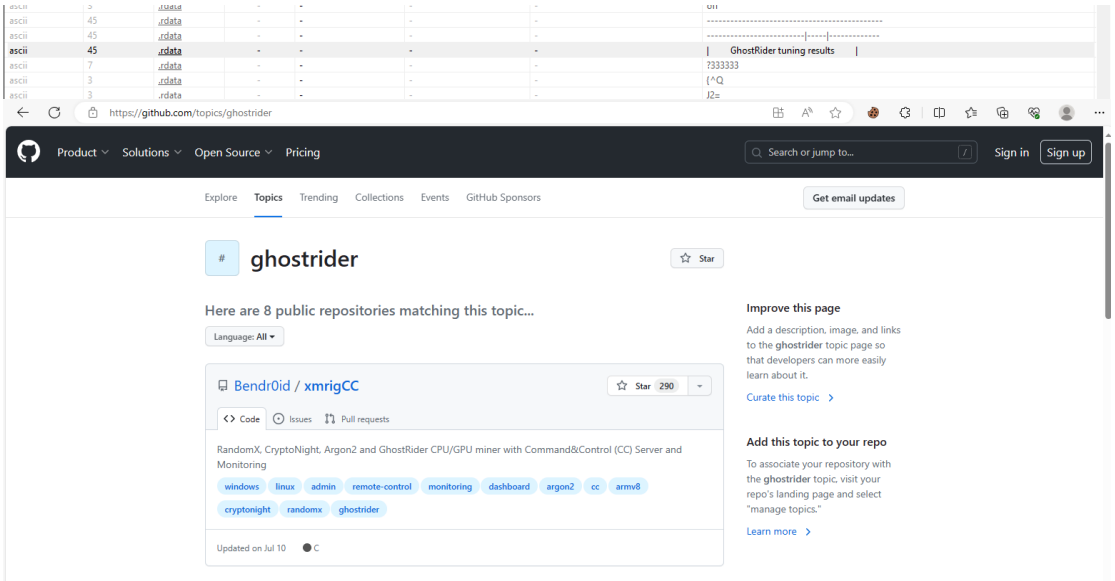
Wallet address, block hash

	7	.rdata	-	-	-	-	sig_key
	39	.rdata	-	-	-	-	[0;33mduplicate job received, reconnect
	3	.rdata	-	-	-	-	[0m
	66	.rdata	-	-	-	-	[0;31munknown algorithm, make sure you set "algo" or "coin" option
	3	.rdata	-	-	-	-	[0m
	28	.rdata	-	-	-	-	[0;31munsupported algorithm

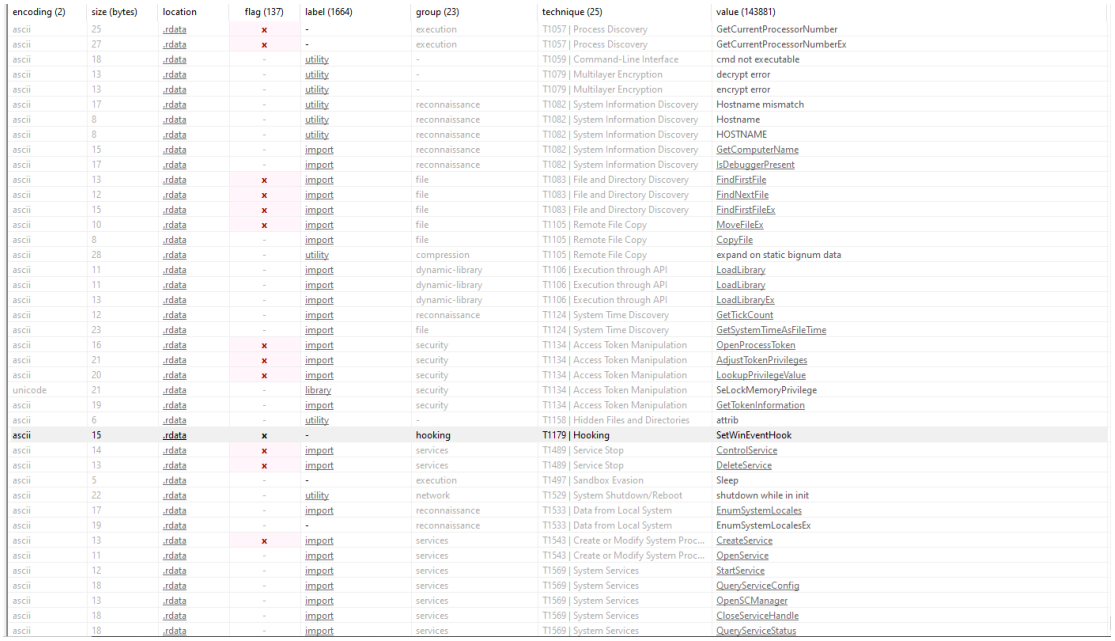
Algo, Coin

ascii	13	.rdata	-	-	-	-	mining.notify
ascii	3	.rdata	-	-	-	-	[0m
ascii	69	.rdata	-	-	-	-	[0;31minvalid mining.notify notification: params array has wrong size
ascii	3	.rdata	-	-	-	-	[0m
ascii	56	.rdata	-	-	-	-	[0;31minvalid mining.notify notification: invalid job id
ascii	3	.rdata	-	-	-	-	[0m
ascii	61	.rdata	-	-	-	-	[0;31minvalid mining.notify notification: invalid param array
ascii	3	.rdata	-	-	-	-	[0m
ascii	60	.rdata	-	-	-	-	[0;31minvalid mining.notify notification: param 4 is invalid
ascii	3	.rdata	-	-	-	-	[0m
ascii	59	.rdata	-	-	-	-	[0;31minvalid mining.notify notification: invalid blob size
ascii	3	.rdata	-	-	-	-	[0m
ascii	62	.rdata	-	-	-	-	invalid mining.subscribe response: extra nonce is not a string
ascii	77	.rdata	-	-	-	-	invalid mining.subscribe response: extra nonce has an odd number of hex chars
ascii	58	.rdata	-	-	-	-	Invalid mining.subscribe response: extra nonce is too long
ascii	16	.rdata	-	-	-	-	mining.authorize
ascii	28	.rdata	-	-	-	-	mining.authorize call failed
ascii	58	.rdata	-	-	-	-	invalid mining.authorize response: result is not a boolean
ascii	12	.rdata	-	-	-	-	login failed
ascii	3	.rdata	-	-	-	-	[0m
ascii	57	.rdata	-	-	-	-	invalid mining.subscribe response: result is not an array
ascii	60	.rdata	-	-	-	-	invalid mining.subscribe response: result array is too short
ascii	27	.rdata	-	-	-	-	mining.extranonce.subscribe
ascii	3	.rdata	-	-	-	-	[0m
ascii	16	.rdata	-	-	-	-	mining.subscribe
ascii	8	.rdata	-	-	-	-	00000000
ascii	6	.rdata	-	-	-	-	[1;32m
ascii	28	.rdata	-	-	-	-	[1;37mbenchmark finished in

Wallet address, block hash, Algo, Coin, Mining these are related to cryptocurrency mining



XmrigCC is a Powerful CPU miner which can be controlled from a C2 server



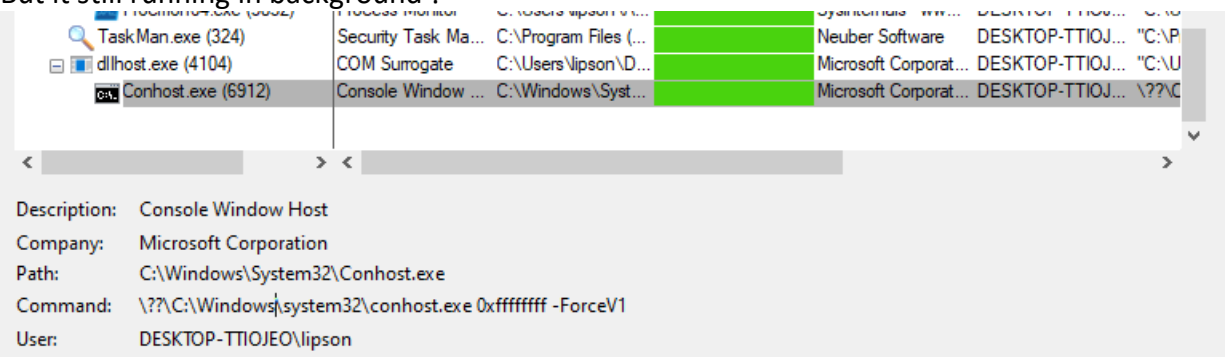
encoding (2)	size (bytes)	location	flag (137)	label (1664)	group (23)	technique (25)	value (143881)
ascii	25	.rdata	×	-	execution	T1057 | Process Discovery	GetCurrentProcessorNumber
ascii	27	.rdata	×	-	execution	T1057 | Process Discovery	GetCurrentProcessorNumberEx
ascii	18	.rdata	-	utility	-	T1059 | Command-Line Interface	cmd not executable
ascii	13	.rdata	-	utility	-	T1079 | Multilayer Encryption	decrypt error
ascii	13	.rdata	-	utility	-	T1079 | Multilayer Encryption	encrypt error
ascii	17	.rdata	-	utility	reconnaissance	T1082 | System Information Discovery	Hostname mismatch
ascii	8	.rdata	-	utility	reconnaissance	T1082 | System Information Discovery	Hostname
ascii	8	.rdata	-	utility	reconnaissance	T1082 | System Information Discovery	HOSTNAME
ascii	15	.rdata	-	import	reconnaissance	T1082 | System Information Discovery	GetComputerName
ascii	17	.rdata	-	import	reconnaissance	T1082 | System Information Discovery	IsDebuggerPresent
ascii	13	.rdata	×	import	file	T1083 | File and Directory Discovery	FindFirstFile
ascii	12	.rdata	×	import	file	T1083 | File and Directory Discovery	FindNextFile
ascii	15	.rdata	×	import	file	T1083 | File and Directory Discovery	FindFirstFileEx
ascii	10	.rdata	×	import	file	T1105 | Remote File Copy	MoveFileEx
ascii	8	.rdata	-	import	file	T1105 | Remote File Copy	CopyFile
ascii	28	.rdata	-	utility	compression	T1105 | Remote File Copy	expand on static bignum data
ascii	11	.rdata	-	import	dynamic-library	T1106 | Execution through API	LoadLibrary
ascii	11	.rdata	-	import	dynamic-library	T1106 | Execution through API	LoadLibrary
ascii	13	.rdata	-	import	dynamic-library	T1106 | Execution through API	LoadLibraryEx
ascii	12	.rdata	-	import	reconnaissance	T1124 | System Time Discovery	GetTickCount
ascii	23	.rdata	-	import	file	T1124 | System Time Discovery	GetSystemTimeAsFileTime
ascii	16	.rdata	×	import	security	T1134 | Access Token Manipulation	OpenProcessToken
ascii	21	.rdata	×	import	security	T1134 | Access Token Manipulation	AdjustTokenPrivileges
ascii	20	.rdata	×	import	security	T1134 | Access Token Manipulation	LookupPrivilegeValue
unicode	21	.rdata	-	library	security	T1134 | Access Token Manipulation	SeLockMemoryPrivilege
ascii	19	.rdata	-	import	security	T1134 | Access Token Manipulation	GetTokenInformation
ascii	6	.rdata	-	utility	-	T1158 | Hidden Files and Directories	attrib
ascii	15	.rdata	×	-	hooking	T1179 | Hooking	SetWinEventHook
ascii	14	.rdata	×	import	services	T1489 | Service Stop	ControlService
ascii	13	.rdata	×	import	services	T1489 | Service Stop	DeleteService
ascii	5	.rdata	-	-	execution	T1497 | Sandbox Evasion	Sleep
ascii	22	.rdata	-	utility	network	T1529 | System Shutdown/Reboot	shutdown while in init
ascii	17	.rdata	-	import	reconnaissance	T1533 | Data from Local System	EnumSystemLocales
ascii	19	.rdata	-	-	reconnaissance	T1533 | Data from Local System	EnumSystemLocalesEx
ascii	13	.rdata	×	import	services	T1543 | Create or Modify System Proc...	CreateService
ascii	11	.rdata	-	import	services	T1543 | Create or Modify System Proc...	OpenService
ascii	12	.rdata	-	import	services	T1569 | System Services	StartService
ascii	18	.rdata	-	import	services	T1569 | System Services	QueryServiceConfig
ascii	13	.rdata	-	import	services	T1569 | System Services	OpenSCManager
ascii	18	.rdata	-	import	services	T1569 | System Services	CloseServiceHandle
ascii	18	.rdata	-	import	services	T1569 | System Services	QueryServiceStatus

The malware employs various API calls, which are part of the techniques adversaries commonly use to execute their malicious activities.

Dynamic Analysis

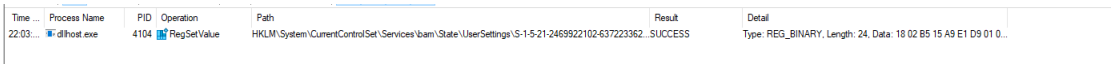
When I executed the malware, it opened a command prompt and closed quickly

But it still running in background !

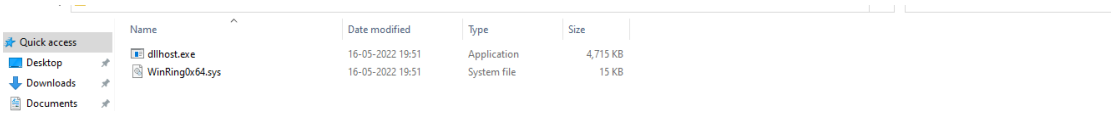


\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

its normal running ***conhost*** in background but in this case, it created by malware which we ran. it can be used to run commands in the background



have found something related to registry, mentioned conhost.exe it set some value to registry, could be indicative of an attempt to manipulate console processes or persistence



also, found another file called WinRing0x64.sys which is a kernel mode driver, and which is the most privileged part of the operating system. The winring0x6.sys file contains code that allows the malware to mine for digital currency.

The winring0x64.sys file contains code that allows the malware to do things like:

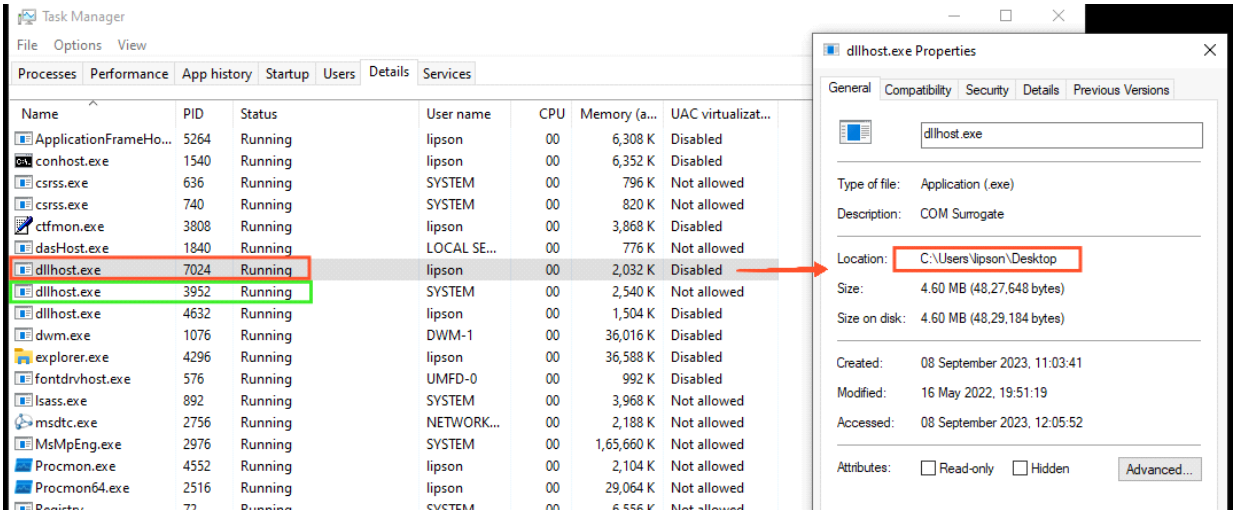
- ✓ Mine for digital currency
- ✓ Install other malware
- ✓ Take control of the computer
- ✓ Damage the computer

imported library's by WinRing0x64 to perform mining

- explorerframe.dll

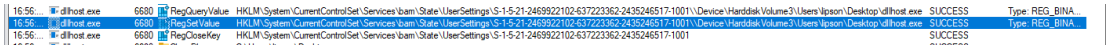
- wshbth.dll
- napinsp.dll
- pnrpnsp.dll
- winrnr.dll
- rasadhlp.dll
- dhcpcsvc.DLL
- dhcpcsvc6.DLL
- NLAapi.dll
- uxtheme.dll
- kernel.appcore.dll
- IPHLPAPI.DLL
- DNSAPI.dll
- mswsock.dll
- CRYPTBASE.DLL
- UMPDC.dll
- USERENV.dll
- powrprof.dll
- KERNELBASE.dll
- CRYPT32.dll
- bcryptPrimitives.dll
- gdi32full.dll
- win32u.dll
- bcrypt.dll
- msvcp_win.dll
- clbcatq.dll
- NSI.dll
- combase.dll
- KERNEL32.DLL
- SHELL32.dll
- ADVAPI32.dll
- ole32.dll
- SHCORE.dll
- RPCRT4.dll
- GDI32.dll
- PSAPI.DLL
- sechost.dll
- USER32.dll
- WS2_32.dll
- msvcrt.dll
- SHLWAPI.dll
- ntdll.dll

Additionally, there are suspicions that the malware duplicated the COM surrogate process, with the "dllhost.exe" file discreetly operating in the background.



the green one is genuine but the red one is the mimicked one

I attempted to terminate the background process "dllhost.exe," and upon doing so, I observed the malware setting another registry value.



HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2469922102-637223362-2435246517-1001\\Device\HarddiskVolume3\Users\lipson\Desktop\dllhost.exe

This is an important aspect: the malware sets a registry value to establish persistence in the system. This ensures that the file will automatically run upon system restart, even if it's been moved

Network Traffic Analysis

first, I tried to analysis used inetsim in remnux. I encountered difficulties with the first approach and then attempted another method involving a DNS server pointing to localhost.

- **Inetsim** (which can create fake internet and services such as DNS, HTTP and much more)
- **Remnux** (C2 SERVER)

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
127.0.0.1               bonus2.corporatebonusapplication.local
127.0.0.1               xmrig.com/wizard
127.0.0.1               http://xmrig.com/wizard
127.0.0.1               nicehash.com
127.0.0.1               server.custompool.xyz
127.0.0.1               fp2e7a.wpc.phicdn.net
127.0.0.0               fp2e7a.wpc.2be4.phicdn.net
```

I included several addresses I obtained from examining the strings and checking VirusTotal.

No.	Time	Source	Destination	Protocol	Length	Info
389	262.252736	127.0.0.1	127.0.0.1	TCP	44	6199 → 49723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
390	267.256866	127.0.0.1	127.0.0.1	TCP	56	49724 → 6199 [SYN] Seq=0 Win=65535 Len=0 MSS=65495
391	267.256967	127.0.0.1	127.0.0.1	TCP	56	6199 → 49724 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
392	267.257068	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
393	267.301765	127.0.0.1	127.0.0.1	TLSv1	337	Client Hello
394	267.301856	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [ACK] Seq=1 Ack=294 Win=2619648 Len=0
395	287.488866	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [FIN, ACK] Seq=294 Ack=1 Win=2619648 L
396	287.530349	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [ACK] Seq=1 Ack=295 Win=2619648 Len=0
397	287.534259	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [FIN, ACK] Seq=1 Ack=295 Win=2619648 L
398	287.534302	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [ACK] Seq=295 Ack=2 Win=2619648 Len=0
399	292.575647	127.0.0.1	127.0.0.1	TCP	56	49725 → 6199 [SYN] Seq=0 Win=65535 Len=0 MSS=65495
400	292.575670	127.0.0.1	127.0.0.1	TCP	44	6199 → 49725 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

(Wireshark output)

TCP v4 | TCP v6 | UDP v4 | UDP v6 | Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
dllhost.exe	6948	TCP	Syn Sent	127.0.0.1	51332	127.0.0.1	6199	08-09-2023 22:11:42	dllhost.exe
svchost.exe	960	TCP	Listen	0.0.0.0	135	0.0.0.0	0	08-09-2023 13:29:46	RpcSs
System	4	TCP	Listen	192.168.160.128	139	0.0.0.0	0	08-09-2023 13:29:53	System
svchost.exe	4832	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	08-09-2023 13:32:51	CDPSvc

(Tcpview output)

The Malware was attempting to communicate with port 6199.

```
C:\Windows\System32\drivers\etc
λ nc -lvnp 6199
listening on [any] 6199 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 51056
[illegible]
λ whoami
```

I established a connection, but it's not readable

No.	Time	Source	Destination	Protocol	Length	Info
389	262.252736	127.0.0.1	127.0.0.1	TCP	44	6199 → 49723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
390	267.256866	127.0.0.1	127.0.0.1	TCP	56	49724 → 6199 [SYN] Seq=0 Win=65535 Len=0 MSS=65495
391	267.256967	127.0.0.1	127.0.0.1	TCP	56	6199 → 49724 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
392	267.257068	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
393	267.301765	127.0.0.1	127.0.0.1	TLSv1	337	Client Hello
394	267.301856	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [ACK] Seq=1 Ack=294 Win=2619648 Len=0
395	287.488866	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [FIN, ACK] Seq=294 Ack=1 Win=2619648 L
396	287.530349	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [ACK] Seq=1 Ack=295 Win=2619648 Len=0
397	287.534259	127.0.0.1	127.0.0.1	TCP	44	6199 → 49724 [FIN, ACK] Seq=1 Ack=295 Win=2619648 L
398	287.534302	127.0.0.1	127.0.0.1	TCP	44	49724 → 6199 [ACK] Seq=295 Ack=2 Win=2619648 Len=0
399	292.575647	127.0.0.1	127.0.0.1	TCP	56	49725 → 6199 [SYN] Seq=0 Win=65535 Len=0 MSS=65495
400	292.575670	127.0.0.1	127.0.0.1	TCP	44	6199 → 49725 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Why Because I don't have TLS certificate to communicate. The adversary is connecting to this port, suggesting the possibility of establishing a connection to a mining pool for cryptocurrency mining purposes.

YARA Rule

```
rule dllhost {
   meta:
      author = "Lipsonlazark"
      description = "A detection rule against dllhost.exe crypto miner"
   strings:
      $file_name = "dllhost.exe" ascii

      // Suspected name of functions and DLL functionalities.
      $function_name_4 = "CreateProcess" ascii
      $function_name_5 = "GetTickCount" ascii
      $function_name_6 = "CreateThreadpoolTimer" ascii
      $function_name_7 = "Sleep" ascii
      $function_name_8 = "mining" ascii
      $function_name_9 = "//randomx.xmrig.com" ascii

      // PE Magic Byte.
      $PE_magic_byte = "MZ" ascii

      // Hex String Function name.
      $Hex_string1 = {58 4D 52 00 4D 6F 6E 65 72 6F}
      $Hex_string2 = {43 72 79 70 74 41 63 71 75 69 72 65 43 6F 6E 74 65 78 74}

   condition:
      $PE_magic_byte at 0 and
      $file_name and
      $Hex_string1 and $Hex_string2 and $function_name_4 and $function_name_5 and
$function_name_6 and $function_name_7 and $function_name_8 or $function_name_9
}
```

//This yara rule specifically identify the Monero mining malware

CONCLUSION

I came up with some analysis on how it's executed based on the APIs it uses and the execution process. First, it performed some reconnaissance to identify the system, such as the current user and hostname. Afterward, it conducted some process discovery, including the current process, process ID, process memory info, and process threads. Next, it attempted to ping a remote server. Then, it downloaded some files from the internet. 'LoadLibrary' could have been used to load system-available DLLs into memory, enabling it to load additional functions for malicious activities. Additionally, it hid the directory using the 'T1158 - Hidden Files and Directories' technique. Finally, it created a new process, COM Surrogate, which mimicked a genuine Windows process also its has a persistance mechanism

Mitigation and Recommendations

- ✓ Use updated antivirus software.
- ✓ Regularly monitor running processes and services.
- ✓ Be aware that not all malwares can be detected by antivirus.
- ✓ Be cautious when downloading files from the internet or opening email attachments, especially from unknown or untrusted sources.

About the Author

Name: Lipson Lazar K
LinkedIn: www.linkedin.com/in/lipson-lazar-k-391b5a141/

Sample Malware: https://github.com/CRK101/MalwareAnalysis

Caution: Malware samples can be harmful and may lead to unintended infections or legal consequences if mishandled. Use them only in controlled, isolated environments for legitimate research and educational purposes.