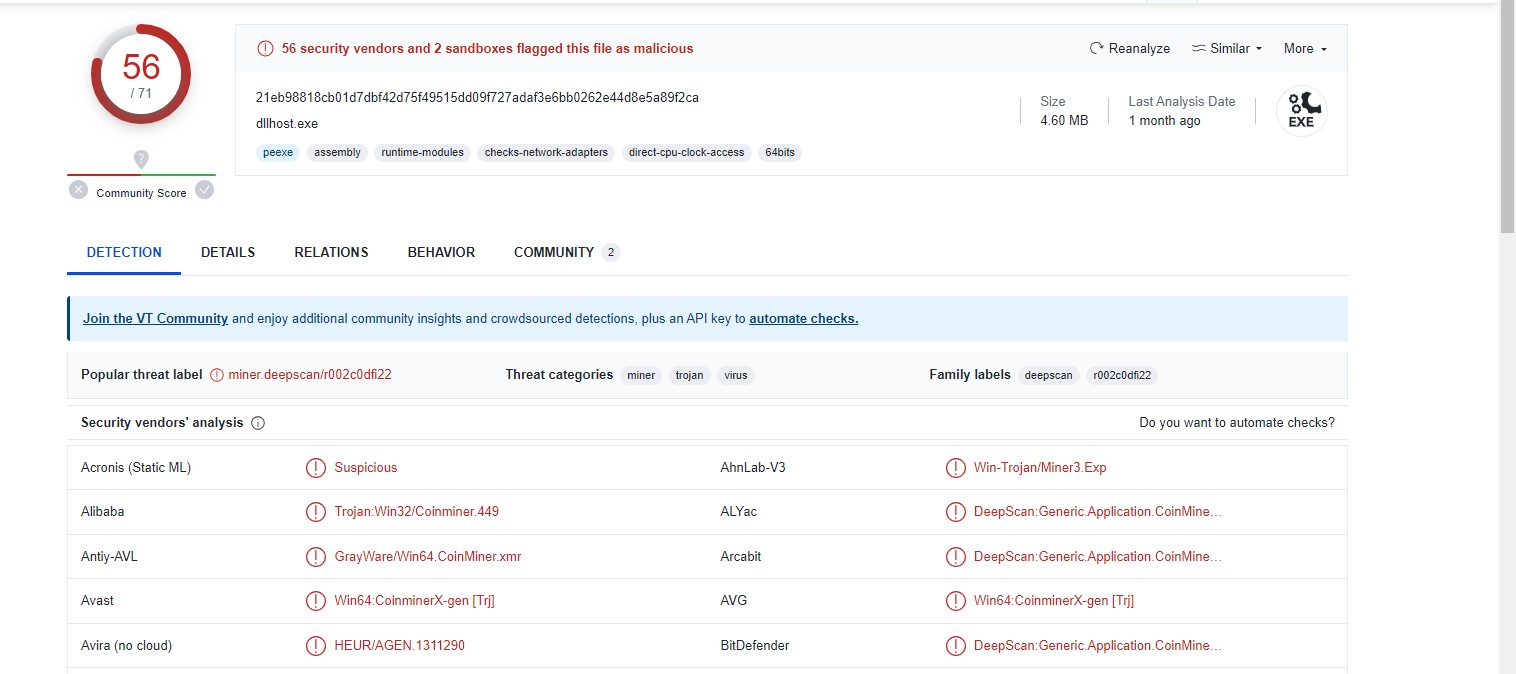
**Crypto Mining Malware Analysis Report**

**Fingerprint**

File Name: dllhost.exe

**Virus total output**



**Hashes**

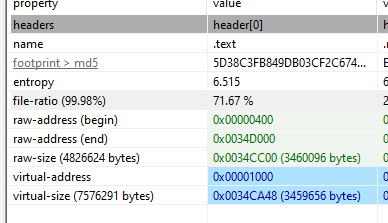
MD5: c5a455de612db6ecc5bd9801ff9826a2

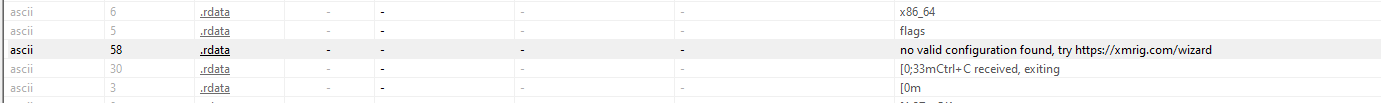
SHA-1: c83769ca9d63070af1b3121bf70358e6e90dc7b6

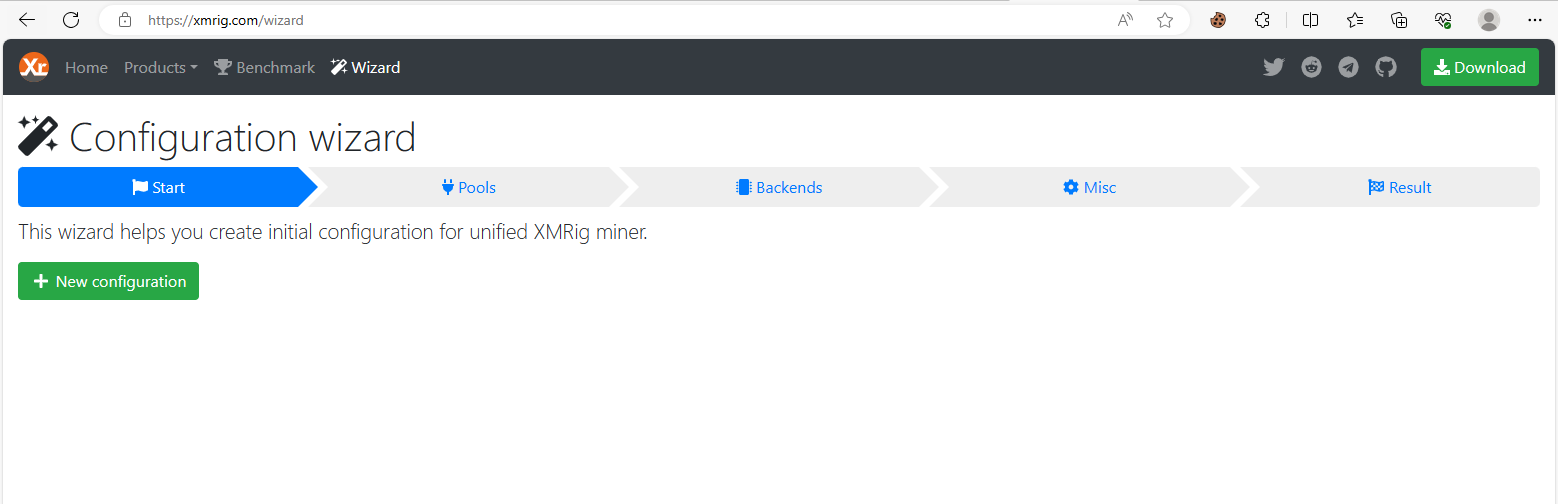
SHA-256: 21eb98818cb01d7dbf42d75f49515dd09f727adaf3e6bb0262e44d8e5a89f2ca

**Basic Static Analysis**

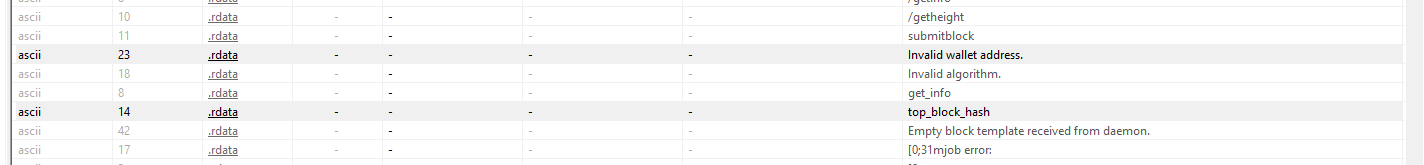
Malware Seems Packed because ***rawsize*** is too smaller than virtual size



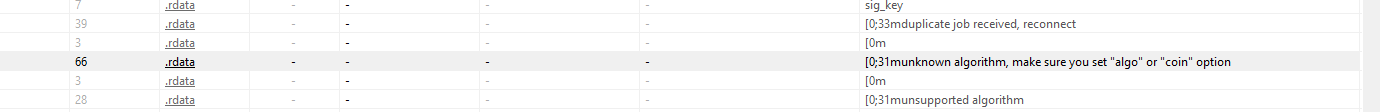




<https://xmrig.com/wizard> is crypto mining pool



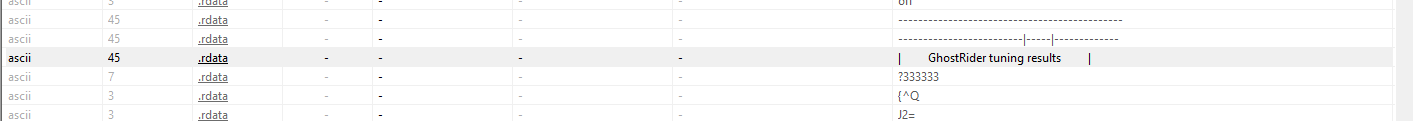
Wallet address, block hash

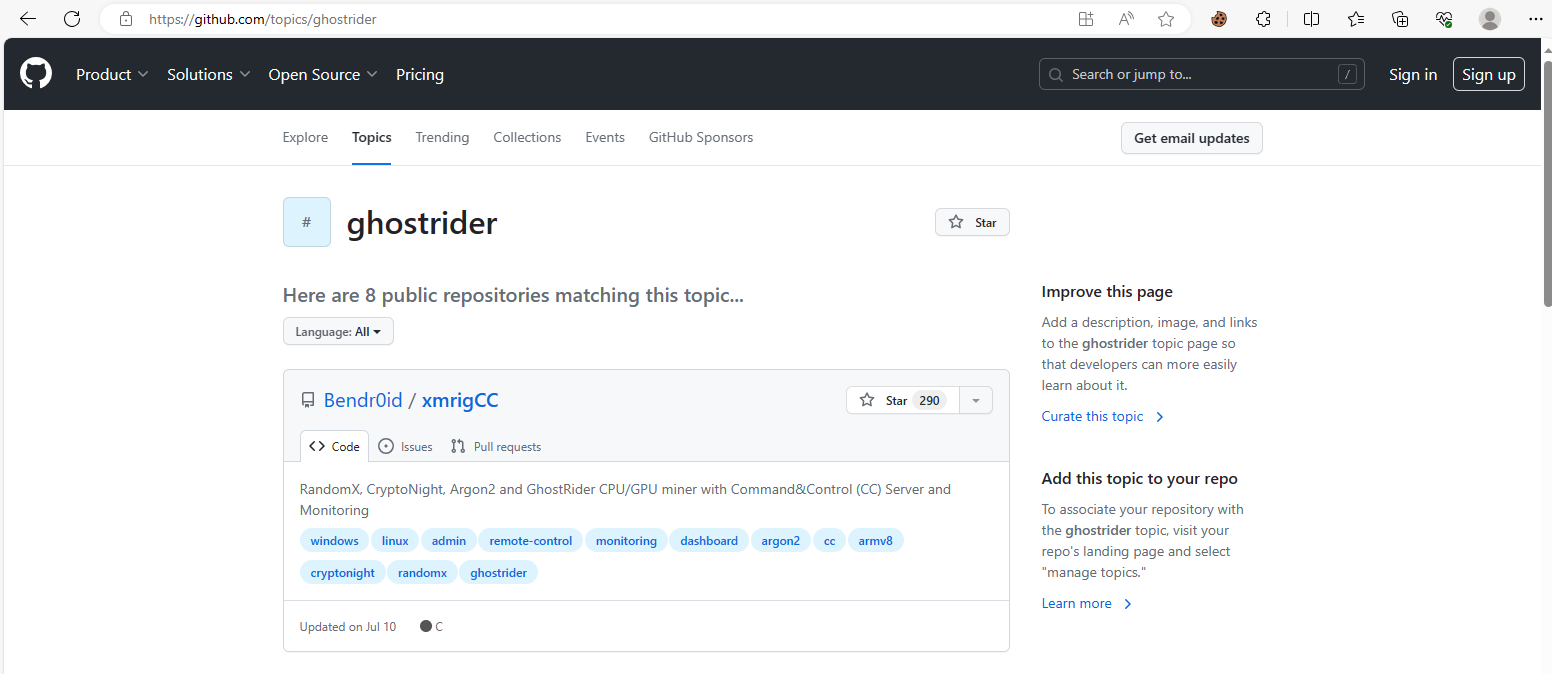


Algo, Coin

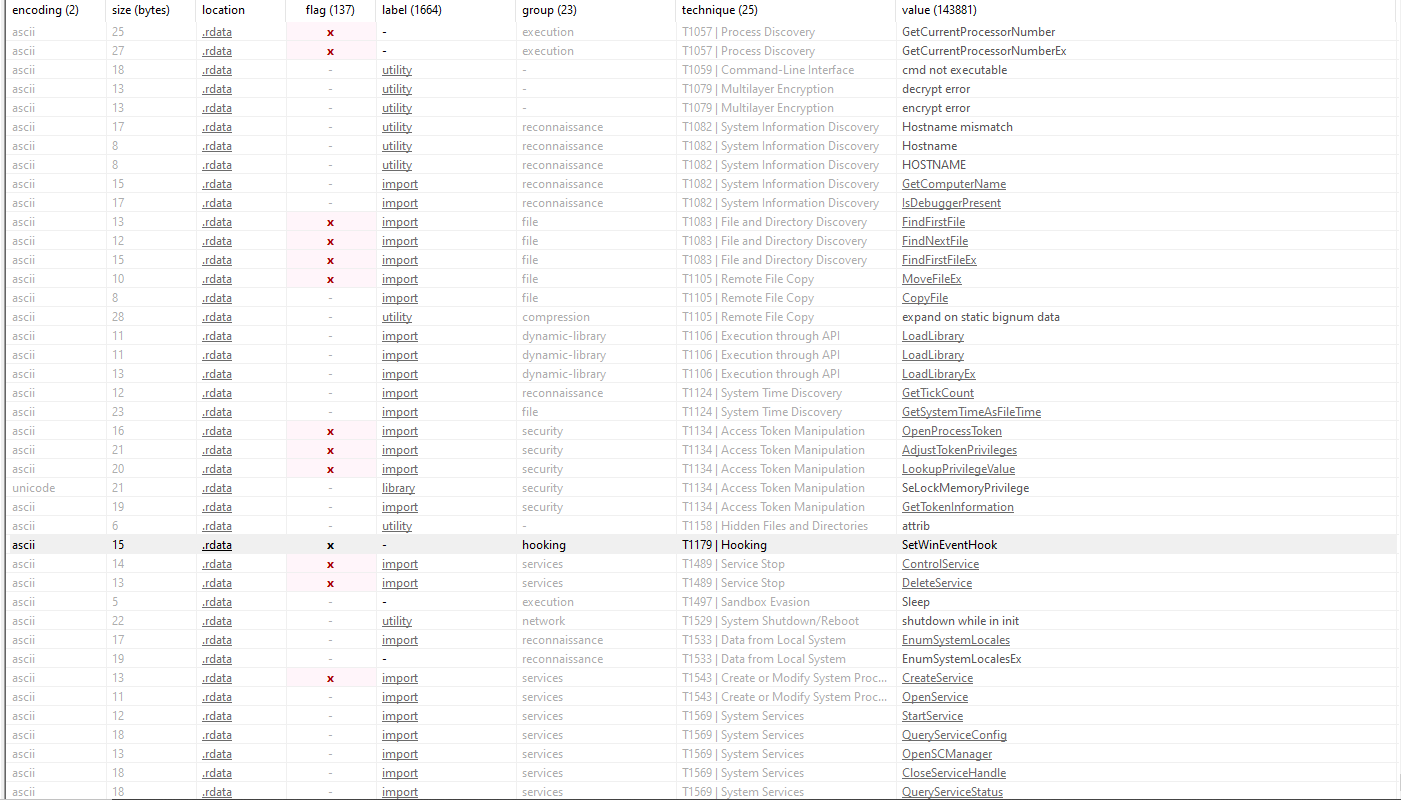


Wallet address, block hash, Algo, Coin, Mining these are related to cryptocurrency mining





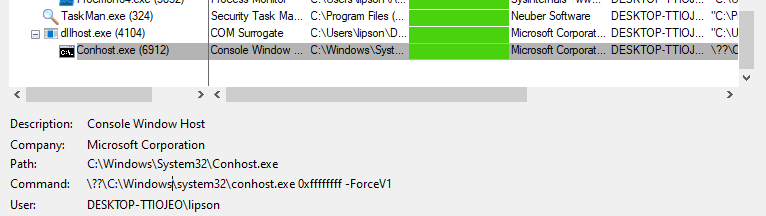
XmrigCC is a Powerful CPU miner which can be controlled from a C2 server



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

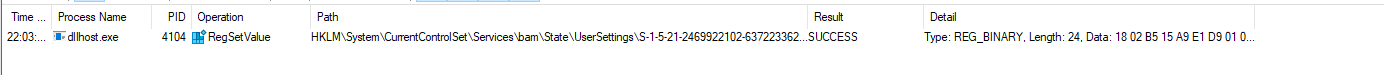
**Dynamic Analysis**

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

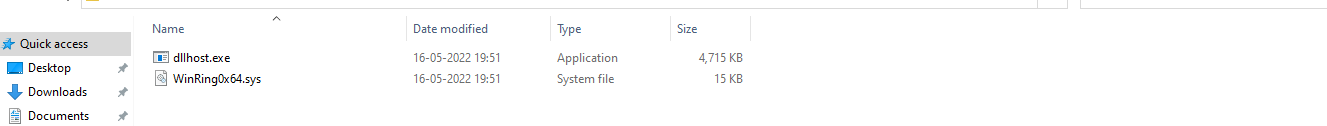
But it still running in background !

\??\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.

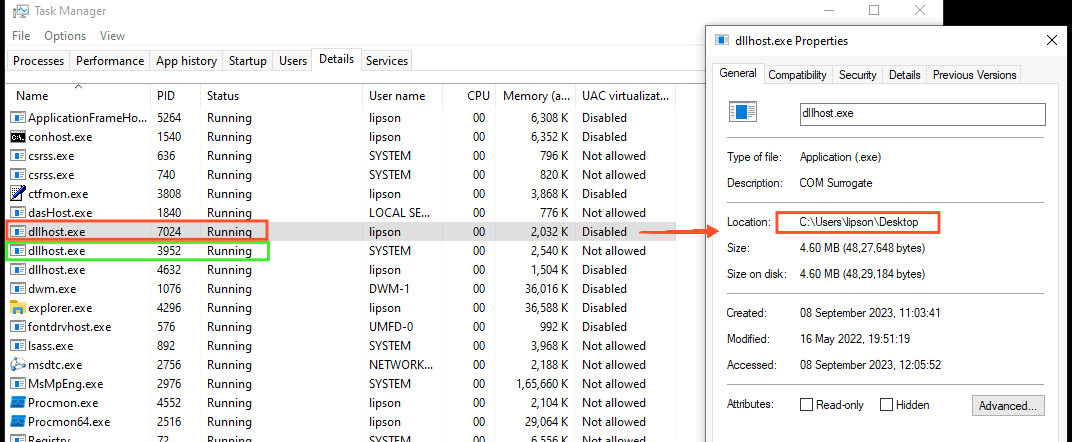
**The winring0x64.sys file contains code that allows the malware to do things like:**

* 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.



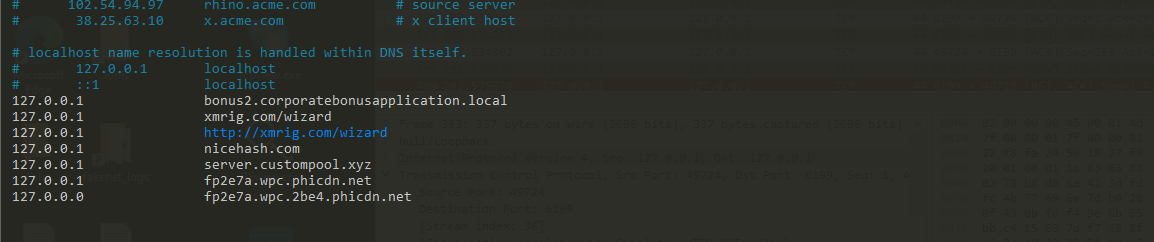
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2469922102-637223362-2435246517-1001[\\Device\HarddiskVolume3\Users\lipson\Desktop\dlIhost.exe](file:///\\Device\HarddiskVolume3\Users\lipson\Desktop\dlIhost.exe)

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

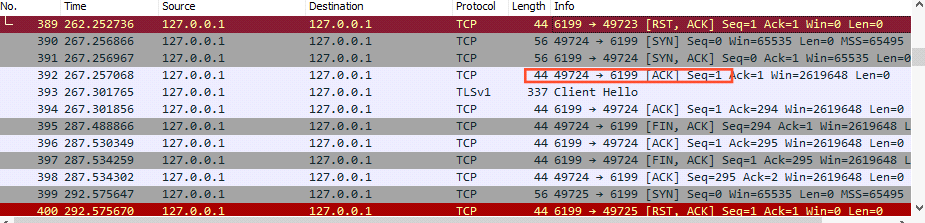
**Network Traffic Analysis**

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.

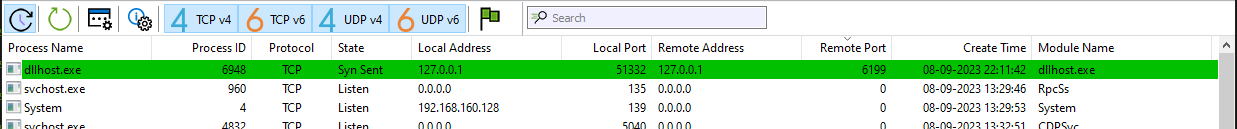
* **Inetsim** (which can create fake internet and services such as DNS, HTTP and much more)
* **Remnux** (C2 SERVER)



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

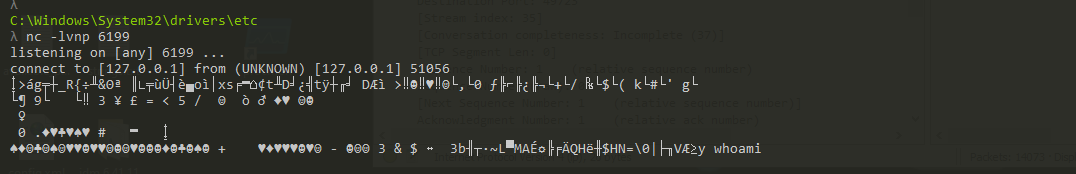


(Wireshark output)

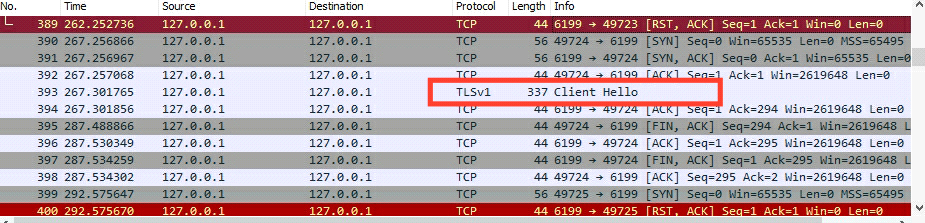


(Tcpview output)

The Malware was attempting to communicate with port 6199.



I established a connection, but it's not readable



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 dlIhost {

meta:

author = "Lipsonlazark"

description = "A detection rule against dlIhost.exe crypto miner"

strings:

$file\_name = "dlIhost.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/](http://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.