

Email: ahmadhossam85@gmail.com

## Malware Analysis

### Sample Identification

- File Type **EXE**
- File Hashes (Used PEstudio and VirusTotal)
  - MD5**  
4d84641b65d8bb6c3ef03bf59434242d
  - SHA-1**  
e5d8d5eecf7957996485cbc1cdbead9221672a1a
  - SHA-256**  
b8d7fb4488c0556385498271ab9ffdf0eb38bb2a330265d9852e3a6288092aa
  - Vhash**  
015056657d7d555bz5nz1fz
  - Authentihash**  
d541c26aeae4953a4f773d3217fbd712b1afc3d2c492697faad436872d8fdea4
  - Imphash**  
c686e5b9f7a178eb79f1cf16460b6a18
  - Rich PE header hash**  
07c8a52db8264e1777fc1b52e8d00bf5
  - SSDEEP**  
1536:/DMcoFQf0U4u//dpkDM5Rw8IP3NHpwOqJICS4A9On359M0fLEd2xmjo:eu  
DKD+I3NJFqnjPLEd2xq
  - TLSH**  
T127C3C062FD9082F3D55341F2122F3F1B99BEFD74641818A7D36089884F7  
6493AA1F663
- File Name  
b8d7fb4488c0556385498271ab9ffdf0eb38bb2a330265d9852e3a6288092aa.exe
- Other Names (VirusTotal)
  - 4d84641b65d8bb6c3ef03bf59434242d.exe
  - VirusShare\_4d84641b65d8bb6c3ef03bf59434242d
  - 032\_10\_17\_2020\_16\_15\_34\_032\_1602947800qkpxkf.exe.MRG
  - b8d7fb4488c0556385498271ab9ffdf0eb38bb2a330265d9852e3a6288092aa.vir
  - b.exe
- File History (PEstudio and VirusTotal)

Creation Time  
2020-06-15 16:24:05 UTC  
First Submission  
2020-06-17 09:32:29 UTC  
Last Submission  
2024-01-20 17:31:32 UTC  
Last Analysis  
2024-05-20 20:01:58 UTC

## Imports

- Import functions found from **KERNAL32.dll** and **USER32.dll** libraries

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)											
file settings about											
c:\users\user\desktop\sample.b8d77b4-											
indicators (sections > name > flag)	imports (6)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (3)	technique (1)	type (1)	ordinal (1)	library (0)	
footprints (count > 10)	GetCurrentThreadId	x	0x0000EBE2	0x0000EBE2	526 (0x206)	execution	T1057   Process Discovery	implicit	-	KERNEL32.dll	
vinustotal (status > error)	AddAtomW	x	0x0000EC04	0x0000EC04	5 (0x005)	data-exchange	-	implicit	-	KERNEL32.dll	
dos-header (size > 64 bytes)	CreateFileW	-	0x0000EBD4	0x0000EBD4	194 (0x0C2)	file	-	implicit	-	KERNEL32.dll	
dos-stub (size > 168 bytes)	InitFileW	-	0x0000EBE8	0x0000EBE8	1547 (0x060B)	-	-	implicit	-	KERNEL32.dll	
rich-header (tooling > Visual Studio 2015)	SetErrorMode	-	0x0000EC10	0x0000EC10	1263 (0x04EF)	-	-	implicit	-	KERNEL32.dll	
file-header (executable > 32-bit)	MessageBoxW	-	0x0000EC2E	0x0000EC2E	589 (0x24D)	-	-	implicit	-	USER32.dll	
optional-header (subsystem > GUI)											
directories (count > 3)											
sections (flag > name)											
libraries (count > 2)											
imports (flag > 6)											
exports (n/a)											
thread-local-storage (n/a)											
.NET (n/a)											
resources (n/a)											
strings (count > 2301)											
debug (n/a)											
manifest (n/a)											
version (n/a)											
certificate (n/a)											
overlay (n/a)											

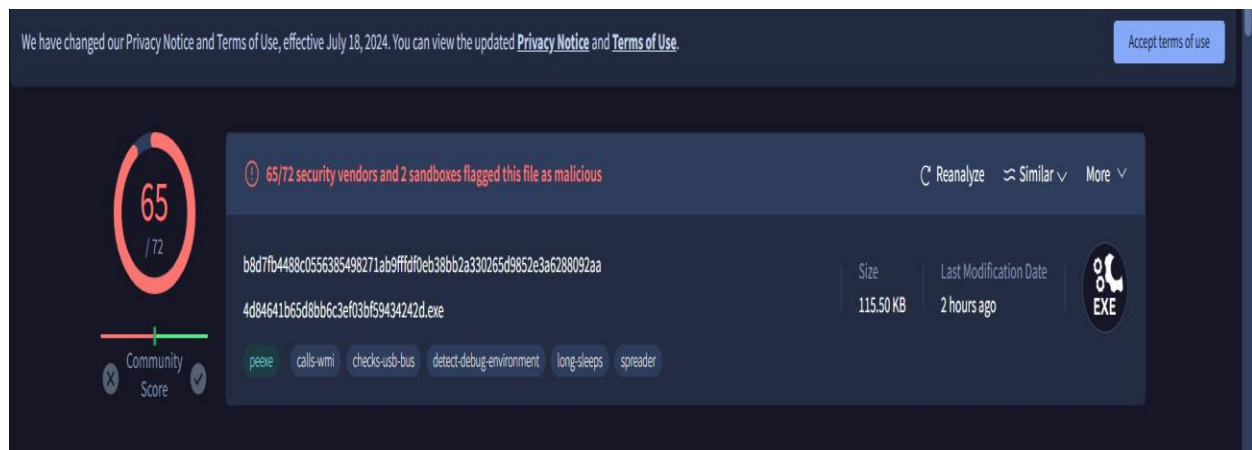
## 4 Sections Found (Uncommon Section .7tdlvx was found)

property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name		.text	.rdata	.data	.7tdlvx
footprint > sha256	BEAF117EABE4BF008C327A...	ACB019C32148240035E1C1...	C4DA552A3E08BE9400331F...	FE18830DCA35FE427E5167F...	583EAF5EEE96A63944AA4BE...
entropy	6.534	7.768	7.463	5.652	5.680
file-ratio (99.13%)	37.66 %	9.96 %	6.49 %	43.29 %	1.73 %
raw-address (begin)	0x00000400	0x0000B200	0x0000E000	0x0000FE00	0x0001C600
raw-address (end)	0x0000B200	0x0000E000	0x0000FE00	0x0001C600	0x0001CE00
raw-size (117248 bytes)	0x0000AE00 (44544 bytes)	0x00002E00 (11776 bytes)	0x00001E00 (7680 bytes)	0x0000C800 (51200 bytes)	0x00000800 (2048 bytes)
virtual-address	0x00001000	0x0000C000	0x0000F000	0x00012000	0x0001F000
virtual-size (116672 bytes)	0x0000AD44 (44356 bytes)	0x00002C48 (11336 bytes)	0x00002018 (8216 bytes)	0x0000C800 (51200 bytes)	0x0000061C (1564 bytes)
characteristics	0x60000020	0x40000040	0xC0000040	0xC0000040	0x42000040
write	-	-	x	x	-
execute	x	-	-	-	-
share	-	-	-	-	-
self-modifying	-	-	-	-	-
virtual	-	-	-	-	-
items					
directory > import	-	0x0000EB78	-	-	-
directory > relocation	-	-	-	-	0x0001F000
directory > import-address	-	0x0000C000	-	-	-
base-of-code	0x00001000	-	-	-	-
base-of-data	-	0x0000C000	-	-	-
entry-point	0x00003ED1	-	-	-	-

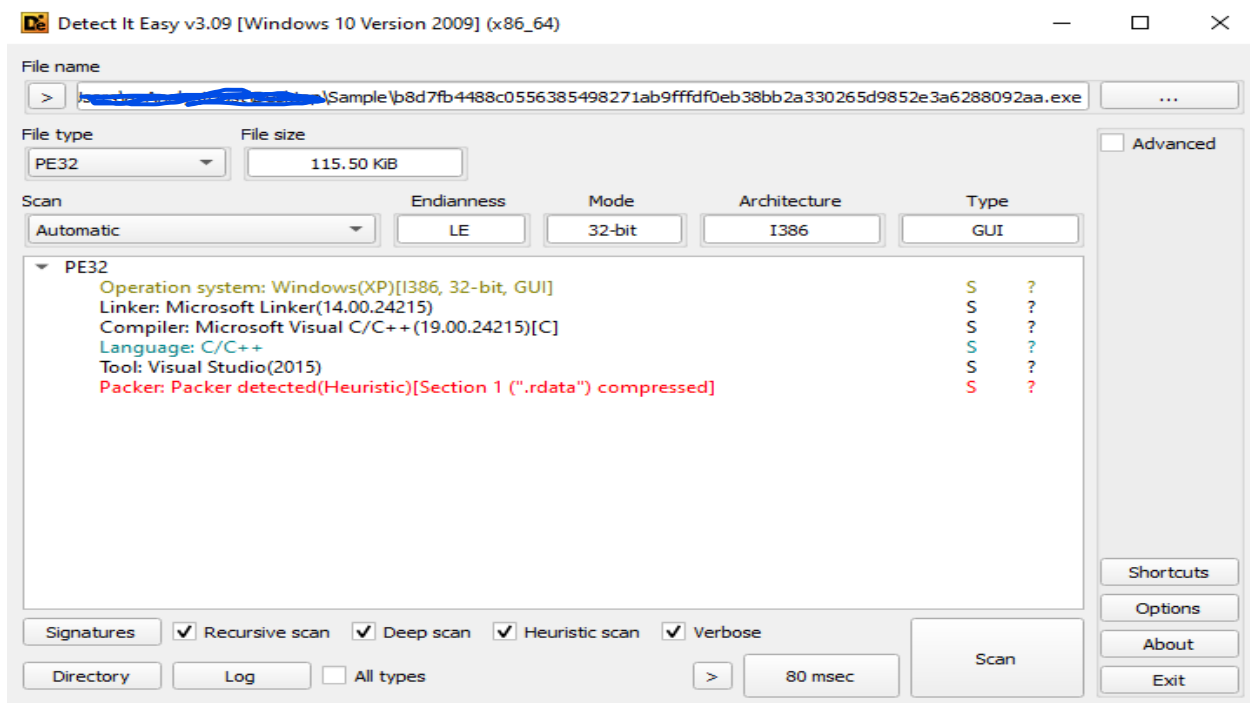
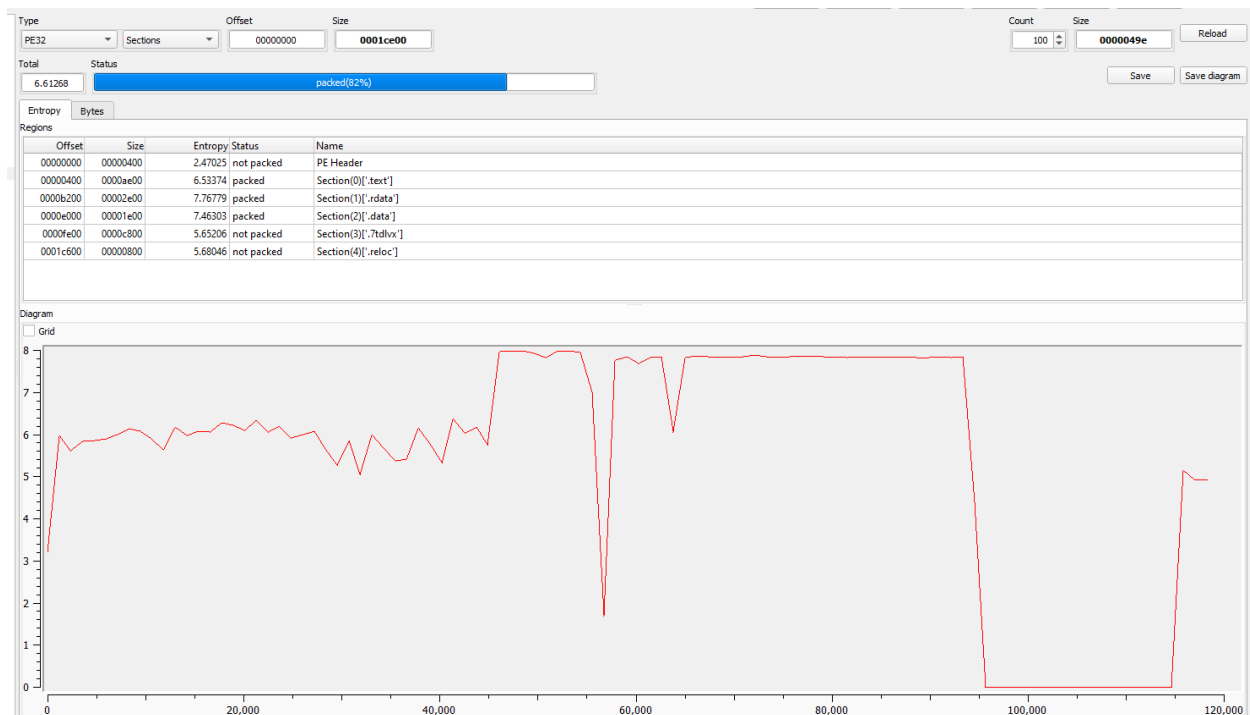
## Suspicious PE File Strings texts found (Using BinText)

- kremez and hszrd f\*\*koff.txt
- USER32.dll
- KERNEL32.dll
- SetErrorMode
- AddAtomW
- GetCurrentThreadId
- CreateFileW
- polish prostitute

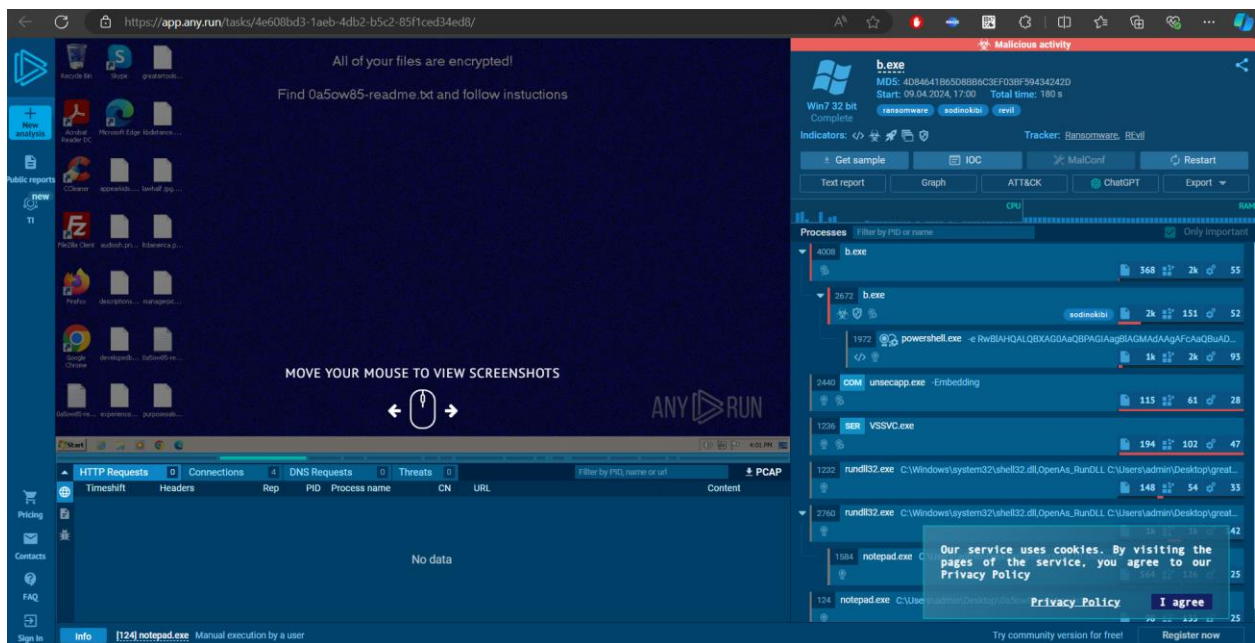
**VirusTotal** ([VirusTotal - File - b8d7fb4488c0556385498271ab9ffdf0eb38bb2a330265d9852e3a6288092aa](#))



Used "Detect It Easy" to identify if file is packet (**82% PACKED**)



**AnyRun Sandbox** ([Analysis b.exe \(MD5: 4D84641B65D8BB6C3EF03BF59434242D\)](#) Malicious activity - Interactive analysis ANY.RUN)



## IP Connections (AnyRun Sandbox – VirusTotal)

IP Traffic											
UDP	192.168.0.71:138										
TCP	20.99.132.105:443										
UDP	192.168.0.45:138										
UDP	a83f:8110:0:0:629b:2800:0:0:53										
TCP	20.99.184.37:443										
TCP	192.229.211.108:80										
TCP	20.99.186.246:443										
UDP	192.168.0.6:138										
TCP	23.215.102.40:443										
UDP	192.168.0.76:138										
UDP	a83f:8110:0:2800:100:200:106:0:53										
TCP	20.99.133.109:443										
UDP	192.168.0.48:138										
TCP	23.216.147.76:443										
UDP	192.168.0.18:138										
UDP	192.168.0.47:138										
TCP	23.216.147.64:443										

Filter by PID, domain, name or ip											
HTTP Requests	0	Connections	4	DNS Requests	0	Threats	0				
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
BEFORE	UDP	?	–	–	?	224.0.0.252	5355	–	–	↑ 48 b	↓ –
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	–	–	↑ 2.93 Kb	↓ –
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑ 1.46 Kb	↓ –
1848 ms	UDP	?	1080	svchost.exe	?	224.0.0.252	5355	–	–	↑ 48 b	↓ –

Processes		Filter by PID or name	Only important			
4008	b.exe		368	2k	55	
2672	b.exe	sodinokibi	2k	151	52	
1972	powershell.exe	-e RwBIAHQALQBXAG0AaQBPAGIAagBIAGMAdAAgAFcAaQBuAD...	1k	2k	93	
2440	COM unsecapp.exe	-Embedding	115	61	28	
1236	SER VSSVC.exe		194	102	47	
1232	rundll32.exe	C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\admin\Desktop\great...	148	54	33	
2760	rundll32.exe	C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\admin\Desktop\great...				

## b.exe process behaviors

**Advanced details of process** [2672] b.exe C:\Users\admin\AppData\Local\Temp\b.exe

**Main information**

- Code signing: 0
- Process startup: 0
- Parent: 0
- Modified time: 302
- Registry changes: 7
- Systemization: 14
- HTTP requests: 0
- Connections: 0
- Network threats: 0
- Modules: 0
- Debug: 0

**Threat Verdict**

**100** Malicious

The score is an approximate value calculated by our Risk algorithm based on process and user actions.

**Process information**

Username: admin  
PID: 2672  
PID: 1232  
Start: 7:34

**File information**

Command line: %Users\admin\AppData\Local\Temp\b.exe

**Timeline of the process**

0 x 7:34 s 45:36 s

**Danger 3**

- Stop the executable file immediately after the start
- T1886 Data Encrypted for Impact (2)
- Removes file file randomness
- Executable network note is found
- SODINOKIBI has been detected (YARA)

**Warning 3**

- T1886 Data Encrypted for Impact (1)
- Creates files for ransomware instruction
- Base64-encrypted command line is found
- T1888-MSI Process (2)
- BASE64 encoded PowerShell command has been detected
- Starts POWERSHELL.EXE for commands execution

**Other 5**

- Creates files in a temporary directory
- Dropped object may contain TDR URLs
- Creates files in the program directory

**Advanced details of process** [2672] b.exe C:\Users\admin\AppData\Local\Temp\b.exe

**Main information**

- Code signing: 0
- Process startup: 0
- Parent: 0
- Modified time: 302
- Registry changes: 7
- Systemization: 14
- HTTP requests: 0
- Connections: 0
- Network threats: 0
- Modules: 0
- Debug: 0

**Threat Verdict**

**100** Malicious

The score is an approximate value calculated by our Risk algorithm based on process and user actions.

**Process information**

Username: admin  
PID: 2672  
PID: 1232  
Start: 7:34

**File information**

Command line: %Users\admin\AppData\Local\Temp\b.exe

**Timeline of the process**

0 x 7:34 s 45:36 s

**Danger 3**


- Stop the executable file immediately after the start
- T1886 Data Encrypted for Impact (2)
- Removes file file randomness
- Executable network note is found
- SODINOKIBI has been detected (YARA)

**Warning 3**

- T1886 Data Encrypted for Impact (1)
- Creates files for ransomware instruction
- Base64-encrypted command line is found
- T1888-MSI Process (1)
- BASE64 encoded PowerShell command has been detected
- Starts POWERSHELL.EXE for commands execution

**Other 5**

- Creates files in a temporary directory
- Dropped object may contain TDR URLs
- Creates files in the program directory



ANALYZE MALWARE

> Huge database of samples and IOCs  
 > Unlimited submissions

> Custom VM setup  
 > Interactive approach

Sign up, it's free

MALICIOUS	SUSPICIOUS	INFO
Drops the executable file immediately after the start <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> <li>• b.exe (PID: 2672)</li> </ul>	Reads the Internet Settings <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> </ul>	Reads the computer name <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> <li>• b.exe (PID: 2672)</li> </ul>
Sodinokibi ransom note is found <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Reads security settings of Internet Explorer <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> </ul>	Checks supported languages <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> <li>• b.exe (PID: 2672)</li> </ul>
SODINOKIBI has been detected (YARA) <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Application launched itself <ul style="list-style-type: none"> <li>• b.exe (PID: 4008)</li> </ul>	Reads product name <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>
Renames files like ransomware <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Starts POWERSHELL.EXE for commands execution <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Reads Environment values <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>
	Executes as Windows Service <ul style="list-style-type: none"> <li>• VSSVC.exe (PID: 1236)</li> </ul>	Reads the machine GUID from the registry <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>
	BASE64 encoded PowerShell command has been detected <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Creates files in the program directory <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>
	Base64-obfuscated command line is found <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Dropped object may contain TOR URL's <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>
	Creates files like ransomware instruction <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>	Manual execution by a user <ul style="list-style-type: none"> <li>• rundll32.exe (PID: 1232)</li> <li>• notepad.exe (PID: 124)</li> <li>• rundll32.exe (PID: 2760)</li> </ul>
		Create files in a temporary directory <ul style="list-style-type: none"> <li>• b.exe (PID: 2672)</li> </ul>

## Some Files OPENED by Malware

- C:\Documents and Settings\root\

- C:\Python27\
- C:\WINDOWS\system32\
- C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83\comctl32.dll
- C:\documents and settings\administrator\

#### **Some Files Written by Malware locations**

- C:\0\4rgi37-readme.txt
- C:\4rgi37-readme.txt
- C:\DiskD\4rgi37-readme.txt
- C:\DiskX\4rgi37-readme.txt
- C:\Documents and Settings\4rgi37-readme.txt
- C:\Documents and Settings\Administrator\
- C:\Documents and Settings\All Users\
- C:\Documents and Settings\Default User\
- C:\Documents and Settings\NetworkService\
- C:\Documents and Settings\root\
- C:\Python27\
- C:\\$SysReset\Logs\

#### **Some Deletion of files at**

- %USERPROFILE%\AppData\Local\
- C:\BOOTNXT
- C:\ProgramData\Microsoft\Windows\
- C:\Windows\System32\spp\store\2.0\cache\cache.dat

#### **Some Dropped Files by malware locations**

- %USERPROFILE%\AccountPictures\
- %USERPROFILE%\AppData\Local\Microsoft\CLR\_v4.0\UsageLogs\powershell.exe.log
- %USERPROFILE%\AppData\Local\Temp\
- %USERPROFILE%\Contacts\
- %USERPROFILE%\Desktop\
- %USERPROFILE%\Documents\
- %USERPROFILE%\Pictures\
- %USERPROFILE%\Videos\
- C:\Program Files (x86)\Microsoft SQL Server\
- C:\ProgramData\Microsoft\Windows\WER\Temp\
- C:\Recovery\WindowsRE\



## Recommendations

1. Use sandboxes, search with the hash of the malware
2. If malware does not exist on sandboxes, you will need to test malware on safe isolated virtual machines and use tools like:
  - **TRID** (Identify file type)
  - **Pestudio** (Observe PE file format)
  - **BinText** (Extract strings from PE file)
  - **DIE** (Detect if file is packed)
  - **Process explorer** (Observe process activity)
  - **Autoruns** (Identify Auto-starting Locations)
  - **Procdot** (Visualize timeline of activities)
  - **Procmon** (Observe file system interaction)
  - **Regshot** (Analyze registry changes)
  - **FakeNetNG** (Create fake servers)
3. Look if any task scheduler exists from the malware and delete them to prevent respawn of some malware functionalities
4. Disable network to prevent connection from the malware to other domains
5. Look for path that the malware accessed to modify or insert files, you may need to delete whole directories
6. Do the same for registry key modifications