Report

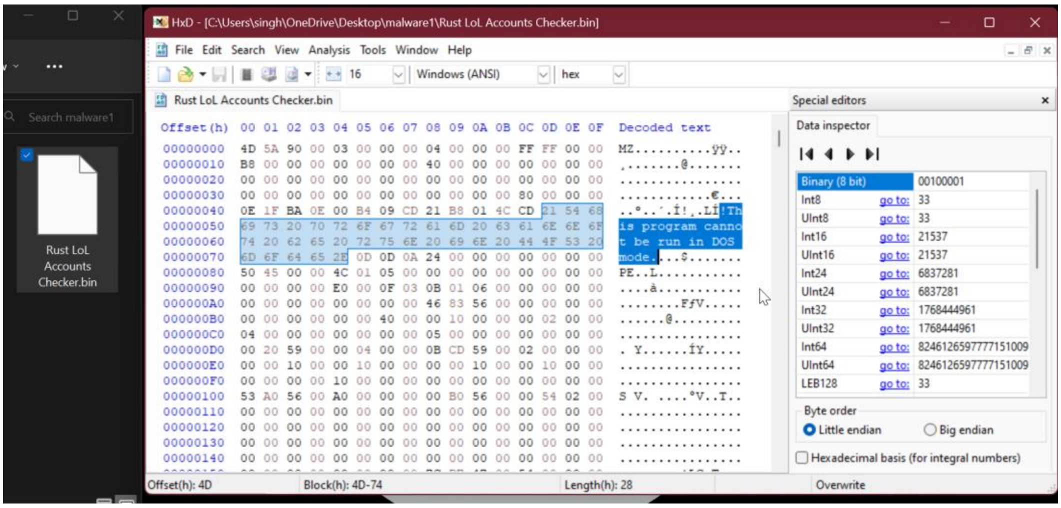
In this example, a suspicious file was analysed. The sample was taken from any.run named ‘Rust LoL Accounts Checker.bin’.

Basic Information

- Name: Rust LoL Accounts Checker
- Type: Bin File (.bin)
- SHA256 Hash: 4bc5ade40ab56113ce9709c0da15416628e089e838864a6756ceca90b8ffaf5b
- SHA1 Hash: 3927ded7ffee7ab8f400d00bcb3b5479ffa3abfb
- MD5 Hash: bded213b6ad8b501a9a8769498c06858
- Size: 5.56 MB

Static Analysis

[1] Upon analysing the file in a Hex editor (HxD) it became known that it is an executable file and shouldn’t be executed in an unsecure environment unless trusted completely.



HxD - [C:\Users\singh\OneDrive\Desktop\malware1\Rust LoL Accounts Checker.bin]

16 | Windows (ANSI) | hex

Rust LoL Accounts Checker.bin

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  ............€...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  50 45 00 00 4C 01 05 00 00 00 00 00 00 00 00 00  PE..L...........
00000090  00 00 00 00 E0 00 0F 03 0B 01 06 00 00 00 00 00  ....à...........
000000A0  00 00 00 00 00 00 00 00 46 83 56 00 00 00 00 00  ........FƒV.....
000000B0  00 00 00 00 00 00 40 00 00 10 00 00 00 02 00 00  ......@.........
000000C0  04 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00  ................
000000D0  00 20 59 00 00 04 00 00 0B CD 59 00 02 00 00 00  . Y......ÍY.....
000000E0  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
000000F0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  53 A0 56 00 A0 00 00 00 00 B0 56 00 00 54 02 00  S V. ....°V..T..
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Binary (8 bit)		00100001
Int8	go to:	33
UInt8	go to:	33
Int16	go to:	21537
UInt16	go to:	21537
Int24	go to:	6837281
UInt24	go to:	6837281
Int32	go to:	1768444961
UInt32	go to:	1768444961
Int64	go to:	8246126597777151009
UInt64	go to:	8246126597777151009
LEB128	go to:	33

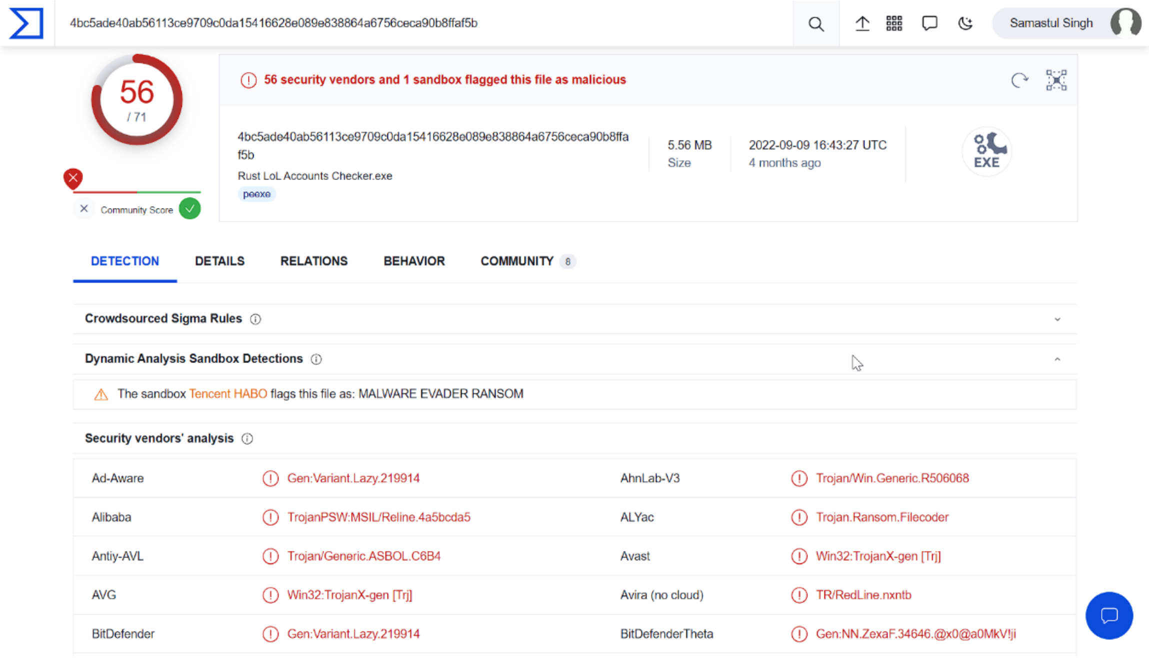
Byte order
● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Offset(h): 4D | Block(h): 4D-74 | Length(h): 28 | Overwrite

[2] The first red flag was when Windows Defender quarantined the file while attempting to retrieve its hash values using the cmd command "get-filehash." The command "certutil -hashfile" was later used to retrieve the hashes.

[3] According to the analysis report by VirusTotal the detection rate of the sample is 56/71. Another tool metadefender also marked the file as suspicious.



56 security vendors and 1 sandbox flagged this file as malicious

4bc5ade40ab56113ce9709c0da15416628e089e838864a6756ceca90b8ffa f5b
Rust LoL Accounts Checker.exe
peexe

5.56 MB
Size

2022-09-09 16:43:27 UTC
4 months ago

Crowdsourced Sigma Rules

Dynamic Analysis Sandbox Detections

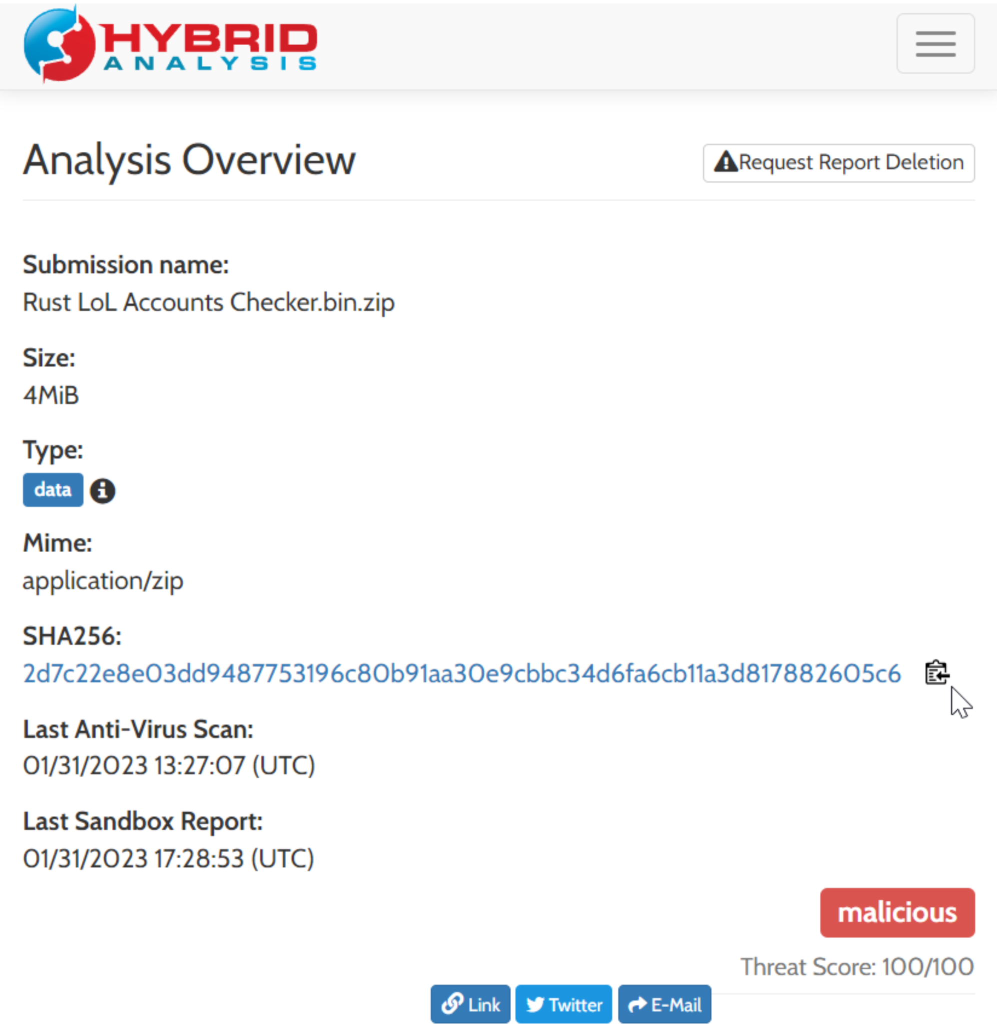
⚠ The sandbox Tencent HABO flags this file as: MALWARE EVADER RANSOM

Security vendors' analysis

Ad-Aware	Gen:Variant.Lazy.219914	AhnLab-V3	Trojan/Win.Generic.R506068
Alibaba	TrojanPSW:MSIL/Reline.4a5bcda5	ALYac	Trojan.Ransom.Filecoder
Antiy-AVL	Trojan/Generic.ASBOL.C6B4	Avast	Win32:TrojanX-gen [Trj]
AVG	Win32:TrojanX-gen [Trj]	Avira (no cloud)	TR/RedLine.nxntb
BitDefender	Gen:Variant.Lazy.219914	BitDefenderTheta	Gen:NN.ZexaF.34646.@x0@a0MkV!ji

Dynamic Analysis

[4] For further analysis the file was executed in some sandbox environments, starting with hybrid analysis which gave the file a threat score of 100/100 and marked is as 'malicious.



Analysis Overview

Submission name:
Rust LoL Accounts Checker.bin.zip

Size:
4MiB

Type:
data

Mime:
application/zip

SHA256:
2d7c22e8e03dd9487753196c80b91aa30e9cbbc34d6fa6cb11a3d817882605c6

Last Anti-Virus Scan:
01/31/2023 13:27:07 (UTC)

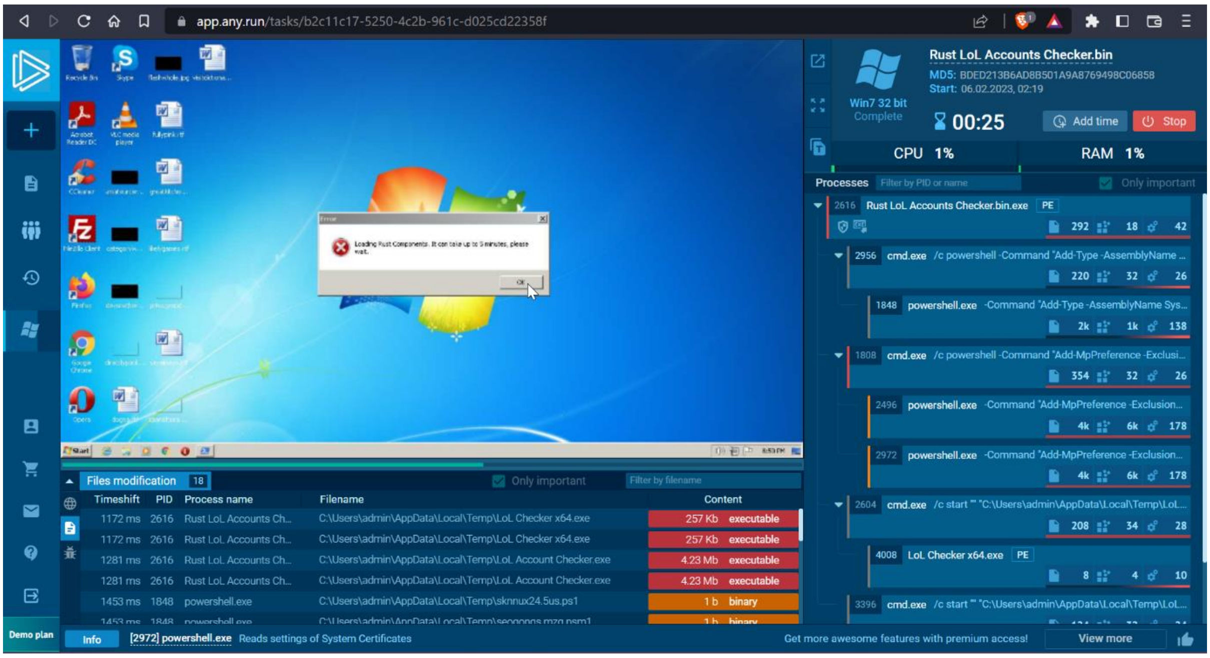
Last Sandbox Report:
01/31/2023 17:28:53 (UTC)

malicious

Threat Score: 100/100

[5] The file was also run in Any.Run sandbox, where it was tagged as ransomware, malware and trojan with its *hash values (MD5, SHA1 & SHA256)* as the main IOCs, while other indicators include *adding the process to start up, dropping executable file, task containing several apps running* and *integrity level elevation.*

[6] The file started many executable programs on its own. The file didn't make any connections over http or https, the only web artefact collected is the link to contact them.



app.any.run/tasks/b2c11c17-5250-4c2b-961c-d025cd22358f

Error

Loading Rust Components. It can take up to 5 minutes, please wait.

OK

Rust LoL Accounts Checker.bin
MD5: BDED213B6AD8B501A9A8769498C06858
Start: 06.02.2023, 02:19
Win7 32 bit
Complete
00:25
CPU 1%
RAM 1%

Processes

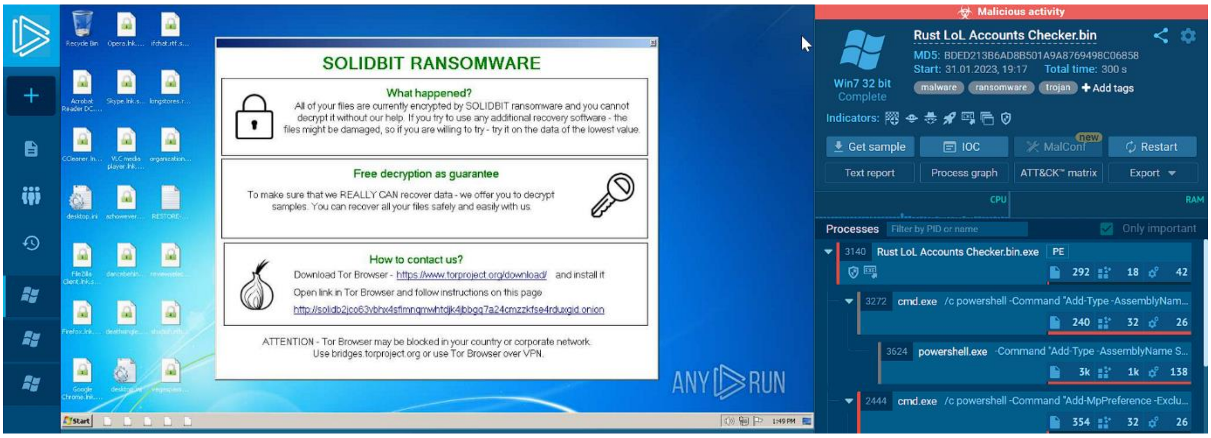
```
2616 Rust LoL Accounts Checker.bin.exe PE                                   292  18  42
  2956 cmd.exe /c powershell -Command "Add-Type -AssemblyName ...            220  32  26
    1848 powershell.exe -Command "Add-Type -AssemblyName Sys...               2k  1k 138
  1808 cmd.exe /c powershell -Command "Add-MpPreference -Exclusi...          354  32  26
    2496 powershell.exe -Command "Add-MpPreference -Exclusion...              4k  6k 178
    2972 powershell.exe -Command "Add-MpPreference -Exclusion...              4k  6k 178
  2604 cmd.exe /c start "" "C:\Users\admin\AppData\Local\Temp\LoL...         208  34  28
    4008 LoL Checker x64.exe PE                                                 8   4  10
  3396 cmd.exe /c start "" "C:\Users\admin\AppData\Local\Temp\LoL...
```

Files modification 18

Timeshift	PID	Process name	Filename	Content
1172 ms	2616	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Checker x64.exe	257 Kb executable
1172 ms	2616	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Checker x64.exe	257 Kb executable
1281 ms	2616	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Account Checker.exe	4.23 Mb executable
1281 ms	2616	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Account Checker.exe	4.23 Mb executable
1453 ms	1848	powershell.exe	C:\Users\admin\AppData\Local\Temp\sknnux24.5us.ps1	1 b binary
1453 ms	1848	powershell.exe	C:\Users\admin\AppData\Local\Temp\seogongs.mzq.psm1	1 b binary

Info [2972] powershell.exe Reads settings of System Certificates

[7] The file wasn't initially observed to cause any harm in the foreground until more time was spent running the sandbox. Following around three minutes of operation, the file revealed itself to be "solidbit ransomware," encrypting all files in the sandbox environment and requesting to be contacted via a URL through the TOR browser in order to successfully unlock the contents.



SOLIDBIT RANSOMWARE

What happened?

All of your files are currently encrypted by SOLIDBIT ransomware and you cannot decrypt it without our help. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

Free decryption as guarantee

To make sure that we REALLY CAN recover data - we offer you to decrypt samples. You can recover all your files safely and easily with us.

How to contact us?

Download Tor Browser - https://www.torproject.org/download/ and install it

Open link in Tor Browser and follow instructions on this page

http://solidb2jco63vbhx4sfimnqmwhtdjk4jbbgq7a24cmzzkfse4rduxgid.onion

ATTENTION - Tor Browser may be blocked in your country or corporate network. Use bridges.torproject.org or use Tor Browser over VPN.

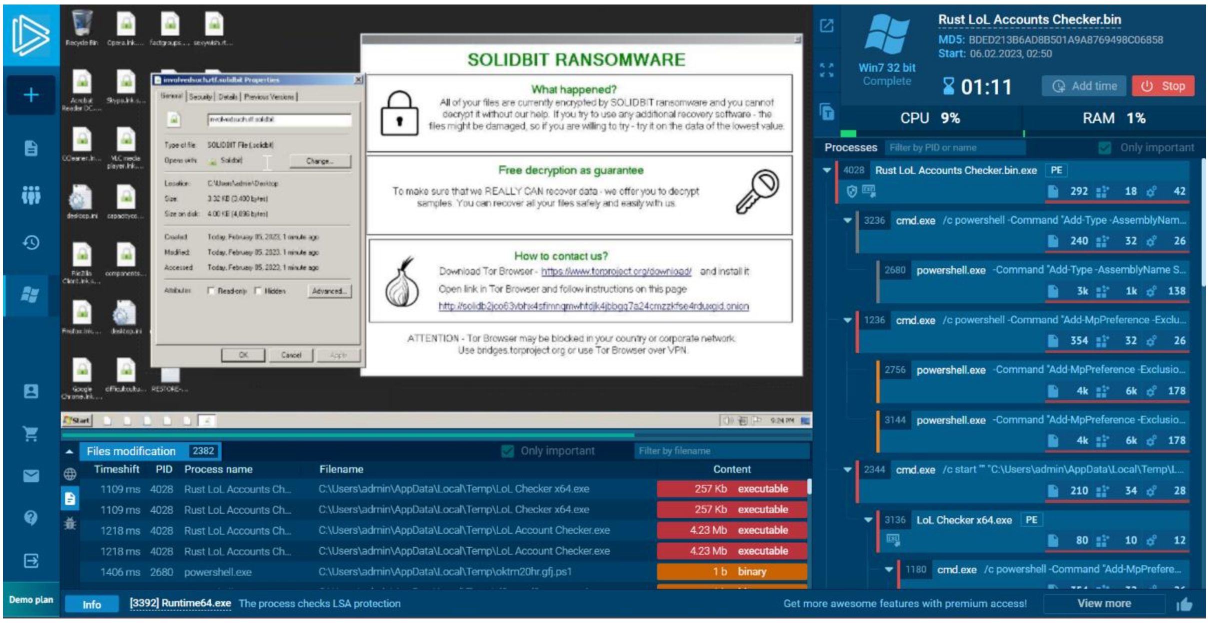
Malicious activity

Rust LoL Accounts Checker.bin
MD5: BDED213B6AD8B501A9A8769498C06858
Start: 31.01.2023, 19:17 Total time: 300 s
malware ransomware trojan
Win7 32 bit
Complete

Processes

```
3140 Rust LoL Accounts Checker.bin.exe PE                                   292  18  42
  3272 cmd.exe /c powershell -Command "Add-Type -AssemblyNam...             240  32  26
    3624 powershell.exe -Command "Add-Type -AssemblyName S...                3k  1k 138
  2444 cmd.exe /c powershell -Command "Add-MpPreference -Exclu...           354  32  26
```

[8] Lastly, all of the files already present in the sandbox were encrypted with the ".solidbit" extension, and attempting to access them just redirected to the ransomware page.



SOLIDBIT RANSOMWARE

What happened?

All of your files are currently encrypted by SOLIDBIT ransomware and you cannot decrypt it without our help. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

Free decryption as guarantee

To make sure that we REALLY CAN recover data - we offer you to decrypt samples. You can recover all your files safely and easily with us.

How to contact us?

Download Tor Browser - https://www.torproject.org/download/ and install it

Open link in Tor Browser and follow instructions on this page

http://solidb2jco63vbhx4sfimnqmwhtdjk4jbbgq7a24cmzzkfse4rduxgid.onion

ATTENTION - Tor Browser may be blocked in your country or corporate network. Use bridges.torproject.org or use Tor Browser over VPN.

involvedsuch.rtf.solidbit Properties

General | Security | Details | Previous Versions

involvedsuch.rtf.solidbit

Type of file:	SOLIDBIT File (.solidbit)
Opens with:	Solidbit
Location:	C:\Users\admin\Desktop
Size:	3.32 KB (3,400 bytes)
Size on disk:	4.00 KB (4,096 bytes)
Created:	Today, February 05, 2023, 1 minute ago
Modified:	Today, February 05, 2023, 1 minute ago
Accessed:	Today, February 05, 2023, 1 minute ago
Attributes:	□ Read-only □ Hidden

Rust LoL Accounts Checker.bin
MD5: BDED213B6AD8B501A9A8769498C06858
Start: 06.02.2023, 02:50

Win7 32 bit
Complete

01:11

CPU 9%
RAM 1%

PID	Process	Command	Files	Registry	Modules
4028	Rust LoL Accounts Checker.bin.exe PE		292	18	42
3236	cmd.exe	/c powershell -Command "Add-Type -AssemblyNam...	240	32	26
2680	powershell.exe	-Command "Add-Type -AssemblyName S...	3k	1k	138
1236	cmd.exe	/c powershell -Command "Add-MpPreference -Exclu...	354	32	26
2756	powershell.exe	-Command "Add-MpPreference -Exclusio...	4k	6k	178
3144	powershell.exe	-Command "Add-MpPreference -Exclusio...	4k	6k	178
2344	cmd.exe	/c start "" "C:\Users\admin\AppData\Local\Temp\L...	210	34	28
3136	LoL Checker x64.exe PE		80	10	12
1180	cmd.exe	/c powershell -Command "Add-MpPrefere...			

Files modification 2382

Timeshift	PID	Process name	Filename	Content
1109 ms	4028	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Checker x64.exe	257 Kb executable
1109 ms	4028	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Checker x64.exe	257 Kb executable
1218 ms	4028	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Account Checker.exe	4.23 Mb executable
1218 ms	4028	Rust LoL Accounts Ch...	C:\Users\admin\AppData\Local\Temp\LoL Account Checker.exe	4.23 Mb executable
1406 ms	2680	powershell.exe	C:\Users\admin\AppData\Local\Temp\oktm20hr.gfj.ps1	1 b binary

Info [3392] Runtime64.exe The process checks LSA protection