



**2023**

# **SECURITY REPORT**

## **Ransomware Attack LetsDefend Case**

 [github.com/Abdibimantara](https://github.com/Abdibimantara)

 [abdibimantara.github.io](https://abdibimantara.github.io)

 [abdibimantara91@gmail.com](mailto:abdibimantara91@gmail.com)

# Daftar Isi

<b>Executive Summary .....</b>	<b>2</b>
<b>Latar Belakang .....</b>	<b>2</b>
<b>Lab Environment .....</b>	<b>3</b>
<b>Analysis Incident .....</b>	<b>3</b>
<b>Celah Keamanan .....</b>	<b>9</b>
<b>Rekomendasi .....</b>	<b>9</b>
<b>IOC Ransomware Attack .....</b>	<b>9</b>
<b>Reference.....</b>	<b>10</b>

## Executive Summary

Berdasarkan informasi yang didapatkan oleh tim SOC, terdapat adanya aktivitas Malware yang terdeteksi pada lingkungan kerja disuatu perusahaan klien. Malware tersebut termasuk jenis Ransomware yang dibuktikan dengan adanya notepad intruksi ancaman serta semua file telah terenripsi dalam bentuk .2s6lc. Ransomware tersebut berasal dari grup Sodinokibi. Diketahui bahwa user yang melakukan proses download file tersebut adalah “charles” dan malicious file tersebut juga disebar dari ip internal. Technique yang digunakan attacker adalah T1574 dengan tactics Persistence, Privilege Escalation, Defense Evasion.

## Latar Belakang

Berdasarkan informasi yang tim SOC dapatkan, terdapat indikasi adanya aktivitas malware yang terdeteksi pada lingkungan kerja disuatu perusahaan klien kami. Malware yang terdeteksi tersebut dicurigai termasuk dalam kategori ransomware, dibuktikan dengan terdapat suatu file catatan yang melampirkan pesan berisi intruksi penebusan yang dibuat oleh attacker. Insiden tersebut diketahui terdeteksi pertama kali pada 22 Mei 2021, jam 21:34. Berikut adalah detail dari host yang terindikasi telah terjangkit malware ransomware

- Machine Name : WIN-2DET5DP0NPT
- Host Name : WIN-2DET5DP0NPT
- Processor Identity : Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
- Total Physical Memory : 3 Gigabytes
- Uptime : 00:30:13
- Operating Systems : Windows 7 Home Basic 7601 Service Pack 1
- Patch Level : Service Pack 1
- OS Build : 7601
- Operating systems Bitness : 32-bit
- Registered Owner : Windows User
- Registered Organization : Not Available

- Domain : WORKGROUP
- Logged in User : Charles
- Logged on User : WIN-2DET5DP0NPT\charles,WORKGROUP\WIN-2DET5DP0NPT\$

## Lab Environment

Selama proses analisis, Kami menggunakan sistem operasi windows 11 pro sebagai environment utama. Hal ini dikarenakan dalam proses analisis tersebut, kami menggunakan bantuan dari tool Redline Fireeye. Redline merupakan security tools endpoint gratis dari FireEye, memberikan kemampuan investigasi host kepada pengguna untuk menemukan tanda-tanda aktivitas anomlai melalui analisis memori dan file serta pengembangan profil penilaian ancaman. Redline juga dapat membantu untuk mengumpulkan, menganalisis, dan memfilter data endpoint serta melakukan analisis IOC dan tinjauan hit. Selain itu, pengguna FireEye's Endpoint Security (HX) dapat membuka koleksi triase langsung di Redline untuk analisis mendalam, yang memungkinkan pengguna menetapkan garis waktu dan cakupan insiden. Untuk saat ini, aplikasi redline hanya berjalan di sistem operasi Windows saja.

## Analysis Incident

Kami memulai dengan membuka suatu log file yang kami dapatkan dari tim SOC. File tersebut Bernama AnalysisSession1 dan segera kami buka menggunakan tools Redline Fireeye. Setelah membuka data tersebut kami memulai dengan mencari tahu mengenai proses apa saja yang sedang berjalan dalam mesin tersebut.

Process Name	PID	Path	Arguments
NOTEPAD.EXE	1416	C:\Windows\system32	"C:\Windows\system32\notepad.exe" C:\Users\charles\Desktop\2s6lc-readme.txt
cmd.exe	932	C:\Windows\System32	"C:\Windows\System32\cmd.exe" /C "C:\Users\charles\Documents\Analysis\Helper.bat"
cmd.exe	1388	C:\Windows\System32	C:\Windows\System32\cmd.exe /c C:\Users\charles\AppData\Local\Temp\MsMpEng.exe
MsmPng.exe	2824	C:\Users\charles\AppData\Local\Temp	C:\Users\charles\AppData\Local\Temp\MsMpEng.exe
svchost.exe	1064	C:\Windows\system32	C:\Windows\system32\svchost.exe -k LocalService
System	4		
smss.exe	276	\SystemRoot\System32	\SystemRoot\System32\smss.exe
winlogon.exe	468	C:\Windows\system32	winlogon.exe
SearchProtocolHost.exe	484	C:\Windows\system32	"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFitPipeMssGthrPipe6_Global\UsGthrCtrlFitPipeMss
csrss.exe	420	C:\Windows\system32	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On Sub

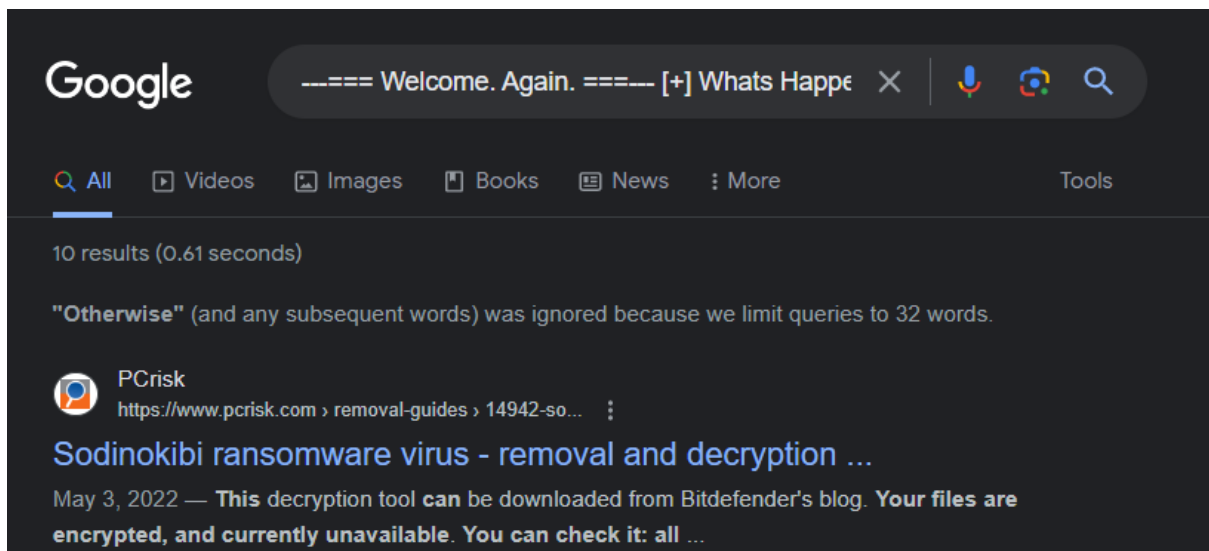
Dari gambar diatas, kami menemukan setidaknya 4 proses yang mencurigakan. Dimana pada proses pertama terdapat aplikasi Notepad yang berjalan dan sedang membuka file "2s6lc-readme.txt". File tersebut menggunakan nama yang mencurigakan sehingga kami berasumsi, bahwa notepad tersebut adalah catatan yang ditinggalkan oleh attacker untuk memberikan intruksi kepada korban.

```

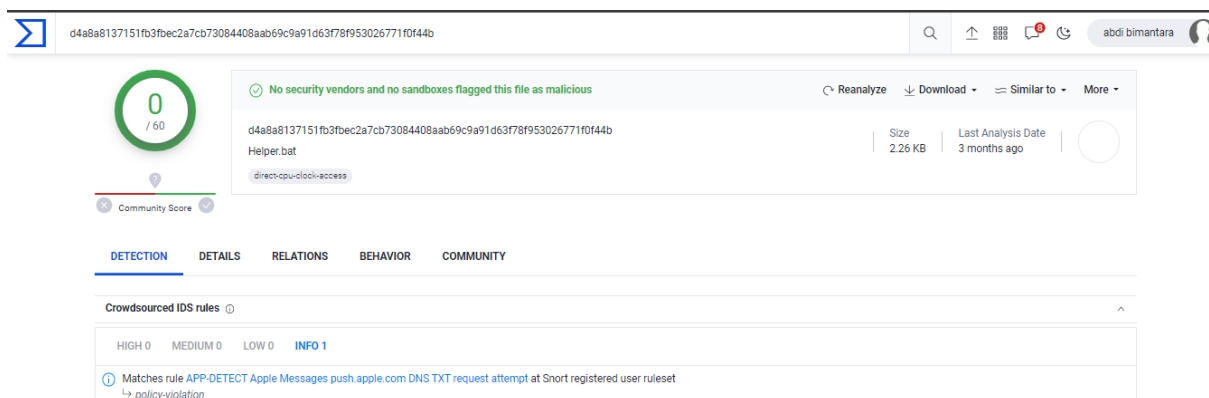
---=== Welcome. Again. ===---
[+] Whats Happen? [+]
Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 2s6lc.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
[+] What guarantees? [+]
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.
[+] How to get access on website? [+]
You have two ways:
1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: http://aplebz47wgazapdqks6vrcv6zcnjppkxbxbr6wketf56nf6aq2nmyoyd.onion/50E8F507062AC1AC
2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decoder.re/50E8F507062AC1AC
Warning: secondary website can be blocked, thats why first variant much better and more available.
When you open our website, put the following data in the input form:
upQFSOmQ88GOa7MrU26zaIXnUP4ayP8F51DEa7Gmnv7T4YB1ADncg+JF7/W2MR0
/aDnF5CmC0B7n0R2AadC7ITEFnn1tnil70rEImbCRAm4TDnrdkCiu1z0BKUYD

```

Dilihat dari pesan yang ditinggalkan oleh attacker tersebut, terdapat instruksi untuk membukakan url dengan domain Onion. Attacker pun menceritakan bahwa file yang terdapat di pc tersebut sudah di encrypt dengan extension file 2s6lc. Setelah kami googling untuk mencari tahu ransomware tersebut berasal dari grup mana, dan kami mendapatkan informasi yaitu Sodinokibi.

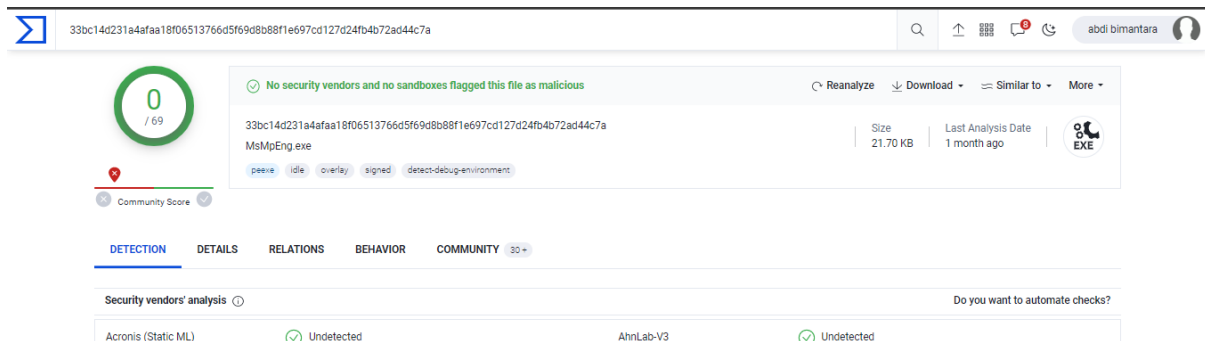


File selanjutnya adalah “Helper.bat” yang berjalan pada program CMD. Sebelumnya kami mencurigai bahwa file tersebut adalah malicious, namun saat kami melakukan pengecekan lebih lanjut file tersebut terlihat cukup bersih.



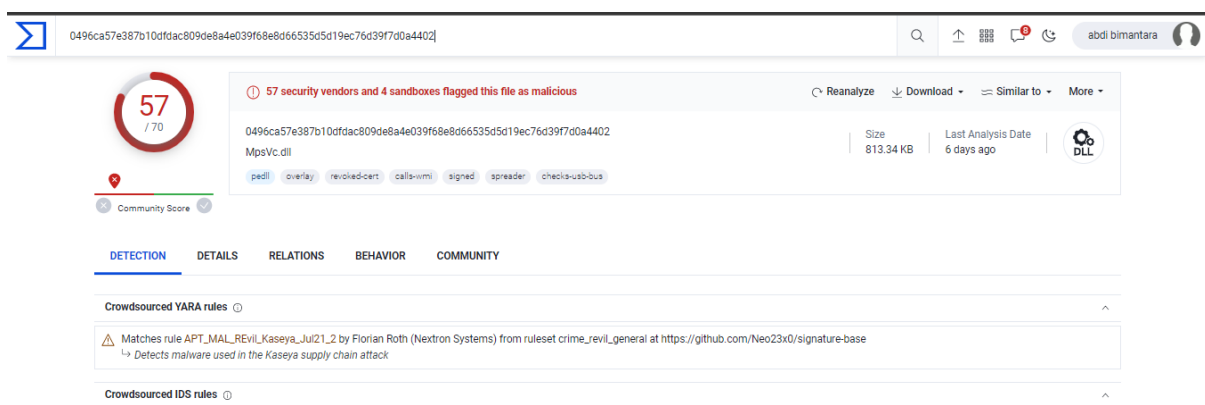
Selanjutnya kami mencari tahu mengenai proses “MsMpEng.exe” yang dipanggil dari direktori AppData\local\Temp menggunakan program “CMD.exe”. Hal ini sungguh membuat kami curiga, sehingga kami mencari tahu “MsMpEng.exe” apa sebenarnya. “MsMpEng.exe” merupakan proses inti dari Windows Defender, solusi antivirus asli. Namun Disini setelah kami mencari tahu lebih detail, kami melihat bahwa “MsMpEng.exe” cukup bersih. Namun disini kecurigaan kami masih ada diakrenakan proses “MsMpEng.exe” yang sebenarnya adalah bersal dari direktori C:\Program Files\Microsoft Security Client\.





Kami disini mencurigai bahwa Attacker menggunakan Technique T1574 (Hijack Execution Flow: DLL Side-Loading) dalam menjalankan proses “MsMpEng.exe”. Dimana attacker menggunakan file Executable (.exe) yang telah dikenal oleh sistem operasi sehingga dapat mengelabui untuk memuat file DLL bersi malicious code sebenarnya. Proses yang dijalankan oleh "MsMpEng.exe" akan mencoba mencari file dll yang diperlukan, Dimana file DLL tersebut dapat didownload secara automate dan dapat berjalan di belakang proses.












Disini kami berusaha mencari tahu file .dll apa saja yang diimport/diperlukan pada proses "MsMpEng.exe". Setelah mencari lebih detail, kami menemukan adanya file “Kernel32.dd” dan “mpsvc.dll”. Disini kami mencoba untuk menganalisis apakah benar kedua file tersebut adalah file malware sesungguhnya.



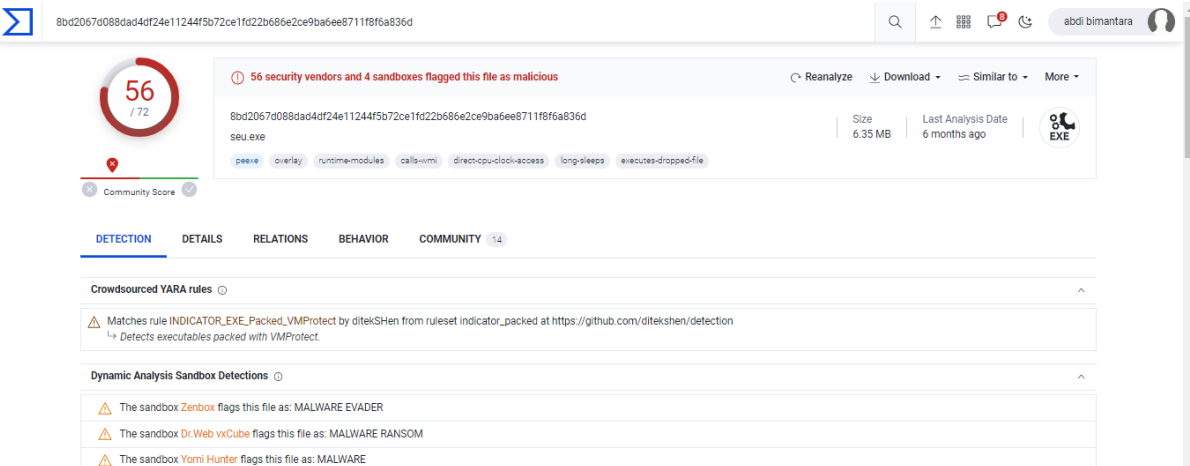
Dan benar saja, file “mpsvc.dll” adalah benar file malware sesungguhnya. Hal ini dibuktikan dengan sebnaya 57 security vendor memberikan tanda sebagai malware terhadap file ini.

Diketahui file “mpsvc.dll” ini masuk pertama kali di mesin korban adalah pada tanggal 2021-05-22 21:28:02Z.

Disini kami mencoba mencari pintu pertama dimana pertama kali user Charles terkena malware. Setelah mencari lebih detail, tepatnya dibagian timeline kami mendapatkan informasi mengenai pintu masuk dari malware tersebut.

	2021-05-22 21:27:18Z	File/Created	Path: C:\Users\charles\AppData\Local\Temp\7cf0f755-7ab3-411b-8abb...	MD5: d41d8cd98f00b204e980...
	2021-05-22 21:27:23Z	File/Created	Path: C:\Users\charles\Downloads\lsass.exe	MD5: bd3c693ecd17dcd9e60b...
	2021-05-22 21:27:48Z	File/Created	Path: C:\Windows\Prefetch\RUNDLL32.EXE-DFC47ECD.pf	MD5: 531ea39f243afec164d40...
	2021-05-22 21:28:02Z	File/Created	Path: C:\Users\charles\AppData\Local\Temp\MpsVc.dll	MD5: 040818b1b3c9b1bf8245...
	2021-05-22 21:28:02Z	File/Created	Path: C:\Users\charles\AppData\Local\Temp\MsMpEng.exe	MD5: 8cc83221870dd07144e6...
	2021-05-22 21:28:02Z	File/Created	Path: C:\Windows\Prefetch\LSASS.EXE-12A718BF.pf	MD5: 6740317f935112853ba7...
	2021-05-22 21:28:03Z	File/Created	Path: C:\\$Recycle.Bin\5-1-5-21-587826007-1492176363-1536112407-1...	MD5: 1f66812d9227f353312c2...
	2021-05-22 21:28:04Z	File/Created	Path: C:\Users\charles\2s6lc-readme.txt	MD5: 1f66812d9227f353312c2...
	2021-05-22 21:28:04Z	File/Created	Path: C:\Users\charles\Contacts\2s6lc-readme.txt	MD5: 1f66812d9227f353312c2...
	2021-05-22 21:28:04Z	File/Created	Path: C:\Users\charles\Desktop\2s6lc-readme.txt	MD5: 1f66812d9227f353312c2...
	2021-05-22 21:28:04Z	File/Created	Path: C:\Users\charles\Documents\2s6lc-readme.txt	MD5: 1f66812d9227f353312c2...




Terlihat bahawa user charels diketahui melakukan proses download file “lsass.exe” dan dilanjutkan dnegan menjalankan proses “mpsvc.dll” dan “MpEng.exe”. file “lsass.exe” kami curigai sebagai malware downloader, dibuktikan dengan hasil pengecekan pada virustotal.



The screenshot shows the VirusTotal analysis page for a file. The file is identified as 'seu.exe' with a size of 6.35 MB and a last analysis date of 6 months ago. The community score is 56/72, with a warning that 56 security vendors and 4 sandboxes flagged the file as malicious. The analysis includes several tabs: DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. Under the DETECTION tab, it shows that the file matches a rule named 'INDICATOR\_EXE\_Packed\_VMPProtect' and is detected by several sandboxes as malware. The sandboxes listed are Zenbox (MALWARE EVADER), Dr.Web vxCube (MALWARE RANSOM), and Yomi Hunter (MALWARE).



Lalu kami mendapatkan mengenai link download yang dibuka oleh user Charles sehingga menyebabkan terdownloadnya malware tersebut. Terlihat bawah user charler mendownload file tersebut menggunakan browser chrome dengan version 89.0.4.

Enter string to find here... 				Reg Ex	In All Fields	Clear Column Filters	Prev	Next
	Download Type	Source URL	Target Directory	File Name				
	Manual	http://192.168.75.129:8111/Documents/lsass	C:\Users\charles\Downloads	lsass				

### File Download Information

**Type:** Manual  
**Source URL:** http://192.168.75.129:8111/Documents/lsass  
**Target Directory:** C:\Users\charles\Downloads  
**Filename:** lsass  
**Temporary Path:** Not Available  
**File Size:** 6.353 Megabytes  
**Bytes Downloaded:** 6.353 Megabytes  
**State:** Finished  
**MIME Type:** Not Available  
**Referrer:** Not Available  
**Can Auto Resume:** Not Available  
**Cache Flags:** Not Available  
**Cache Hits:** 0  
**Full HTTP Header:** Not Available

### Download Timestamps

**Download Started:** 2021-05-22 21:27:23Z  
**Download Finished:** 2021-05-22 21:27:24Z  
**Last Modified:** Not Available  
**Last Accessed:** Not Available  
**Last Checked:** Not Available

### Browser

**Browser Name:** Chrome  
**Browser Version:** 89.0.4389.114  
**Profile:** Default  
**Username:** charles

## Celah Keamanan

1. User chales termasuk dalam grup Administrator. Sehingga dapat dengan mudah mendownload serta menjalankan suatu aplikasi yang berbahaya
2. Antivirus yang tidak update sehingga tidak berhasil dalam mendeteksi adanya malicious file.
3. Menggunakan sistem operasin yang terlalu lama, sehingga sangat rentan. Diketahui bahwa sistem operasi yang digunakan adalah windows 7 sp 1.
4. Diketahui bahwa malicious file tersebut didownload dari ip internal klien, sehingga ada kemungkinan ada pc atau host lain yang telah tercompromise sehingga dapat menyebarkan malicious file tersebut. Disini juga user charler harus di chek apakah benar tidak disengaja atau benar bahwa akun tersebut juga sudah tercompromise ataupun ini adalah insider threat.

## Rekomendasi

1. Segera lakukan isolasi device dengan cara menonaktifkan perangkat tersebut dari jaringan internet dan USB yang terhubung ke perangkat lain
2. Uninstall malicious file yang ada di host terinfeksi tersebut
3. Segera update sistem operasi yang ada pada host tersebut
4. Segera lakukan proses instalasi antivirus terupdate dan segera lakukan scanning total
5. Lakukan pembatasan akun yang memiliki priviledge “administrator” di lingkungan kerja tersebut

## IOC Ransomware Attack

Grup Ransomware	Sodinokibi
Malicious file Name 1	mpsvc.dll
Hash malicious file 1	3fae8f94296001c32eab62cd7d82e0fd
Malicious file Name 2	lsass.exe
Hash malicious file 2	bd3c693ecd17dcd9e60b08ab963121de
IP Internal	192(.)168(.)75.(129)

Malware Website	<a href="http://aplebzu47wgazapdqks6vrcv6zcnjppkxbxr6wketf56nf6aq2nmyoyd(.)onion/50E8F507062AC1AC">http://aplebzu47wgazapdqks6vrcv6zcnjppkxbxr6wketf56nf6aq2nmyoyd(.)onion/50E8F507062AC1AC</a>
-----------------	---

## Reference

<https://attack.mitre.org/techniques/T1574/002/>

<https://cybergladius.com/letsdefends-dfir-challenge-ransomware-attack-walk-through/>

<https://www.linkedin.com/pulse/letsdefend-ransomware-attack-write-up-armin-toric/>

<https://www.pcrisk.com/removal-guides/14942-sodinokibi-ransomware>