infinitum IT
Power of integrated Security

Threat Spotlight: Lockbit Black 3.0 Ransomware

TABLE OF CONTENTS

Threat Spotlight: Lockbit Black 3.0 Ransomware

What's New on Lockbit Black 3.0

Lockbit Ransomware has been one of the most notorious groups since 2019, and they have a wide range of attack scopes, including critical infrastructures like hospital systems. According to Cyber Threat Intelligence members of Infinitum IT, the LockBit Ransomware group made several updates on the publication site and the Ransomware itself.

Figure 1 Lockbit 3.0 has launched its Bug Bounty program paying for web security exploits and more.

This update on the publication site of Lockbit 3.0, such as the Bug Bounty program, aims for more affiliation. Most notably, they wanted affiliate members to share critical internal data with the Ransomware group members, this can cause an increase in insider threats amongst organizations.

The major updates for Lockbit Black 3.0 Ransomware are:

- Anti Analysis technique to hide themselves against various AV vendors.
- Lockbit Black 3.0, requires an “access token” to be supplied as a parameter upon execution which is similar to BlackCat Ransomware.
- It has a command line argument feature.
- Much more evasive then Lockbit 2.0
- New Anti Debugging feature.
- Main code base is very similar to BlackMatter/Darkside Ransomware.
- Disabling the Windows Defender and Event Log Tampering.

New ransom note and wallpaper after the execution of Lockbit Black 3.0:

HLJkNskOq.README.txt

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak
site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner
your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljqxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwgxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljqxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwgxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically
motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system
administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest
services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a
decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's
Twitter https://twitter.com/hashtag/lockbit?f=live
```

Figure 2 Ransom note

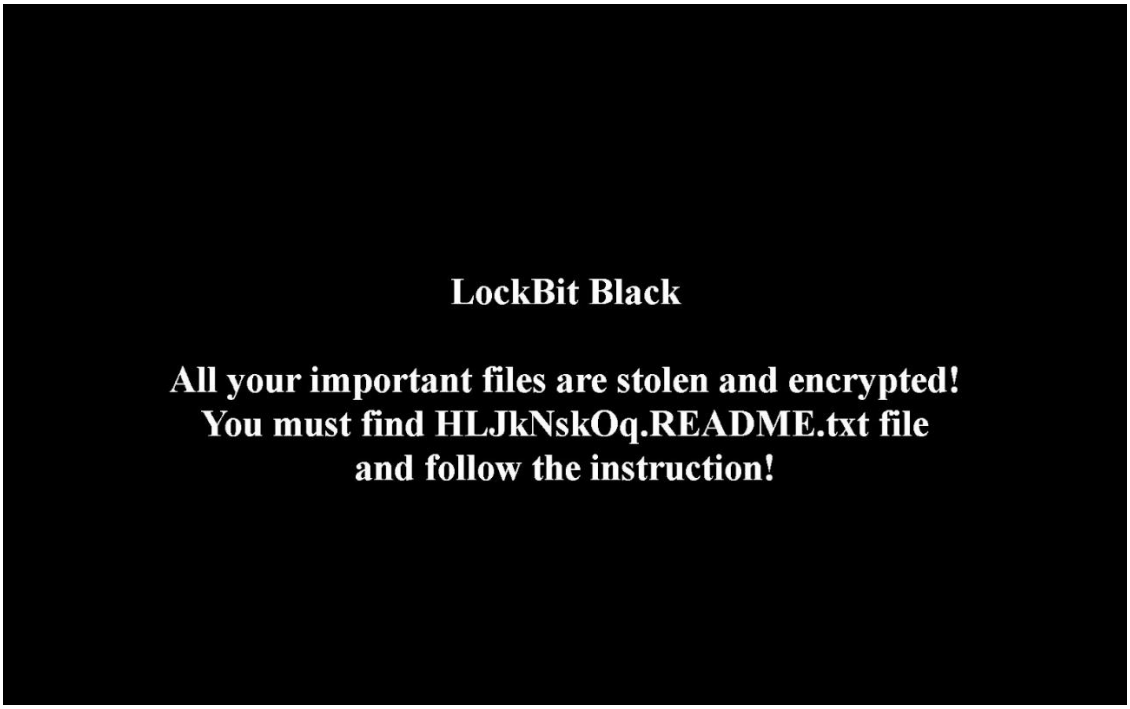
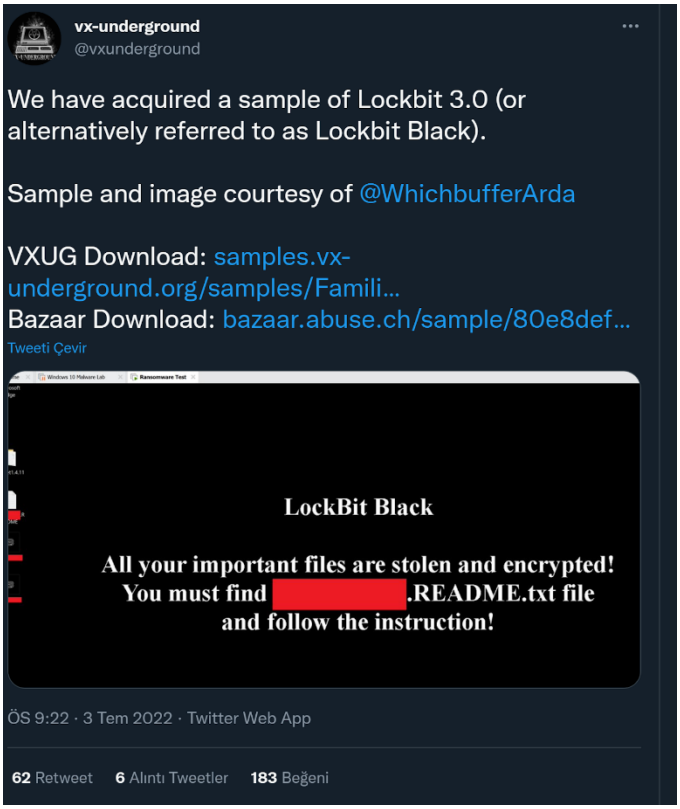


Figure 3 Changed wallpaper image.

First Sample Publication

The first-ever publication was done on July 3, 2022, by Arda Büyükkaya, the Malware Research Team Leader of Infinitum IT. The malware sample has been obtained from an Anonymous source (J. L) who suffered from Lockbit Ransomware attack in a real-life Incident.



https://twitter.com/vxunderground/status/1543661557883740161

After the first publication, “access token” of Lockbit 3.0 Ransomware has been shared with the public to help Malware Analysts from all over the world.

https://twitter.com/WhichbufferArda/status/1543669679637553158

Insides From Real Life Incident Response

To obtain the first-ever Lockbit 3.0 Ransomware sample, Cyber Threat Intelligence team members in Infinitum IT successfully contacted one of Lockbit victim and gathered necessary data to analyze during an Incident Response process. We believed this data could help other companies protect themselves against Lockbit and other Ransomware groups.

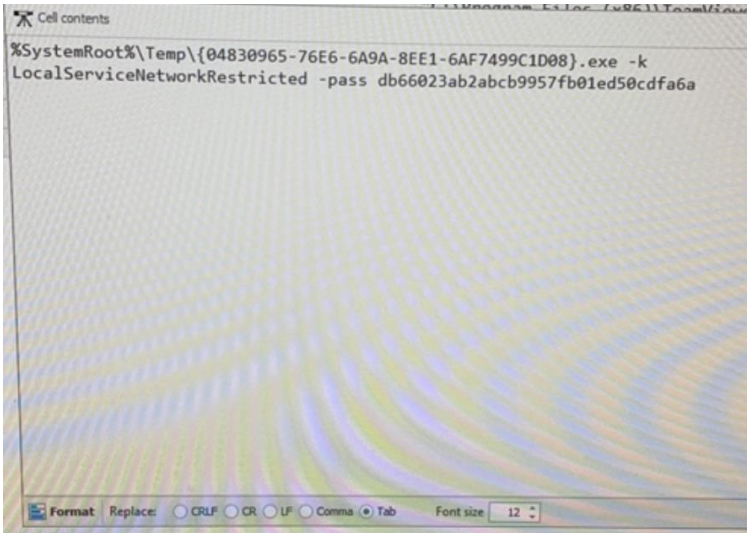


Figure 4 The first execution of Lockbit 3.0 Ransomware, supplied with "access token" (-pass).

Initial Access Point

According to the data obtained from the victim, Lockbit affiliate members used the BlueKeep (CVE-2019–0708) vulnerability and valid stolen credentials of a Local Admin user to gain access to the victim network via abusing the publicly facing Remote Desktop Protocol (RDP) on a Windows 7 installed device.

This Initial Access gives the attacker Local Administrator rights on the victim network, which could lead to mass infection of Lockbit 3.0 Ransomware.

Microsoft Operating Systems BlueKeep Vulnerability

Original release date: June 17, 2019

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this Activity Alert to provide information on a vulnerability, known as "BlueKeep," that exists in the following Microsoft Windows Operating Systems (OSs), including both 32- and 64-bit versions, as well as all Service Pack versions:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

An attacker can exploit this vulnerability to take control of an affected system.

https://www.cisa.gov/uscert/ncas/alerts/AA19-168A

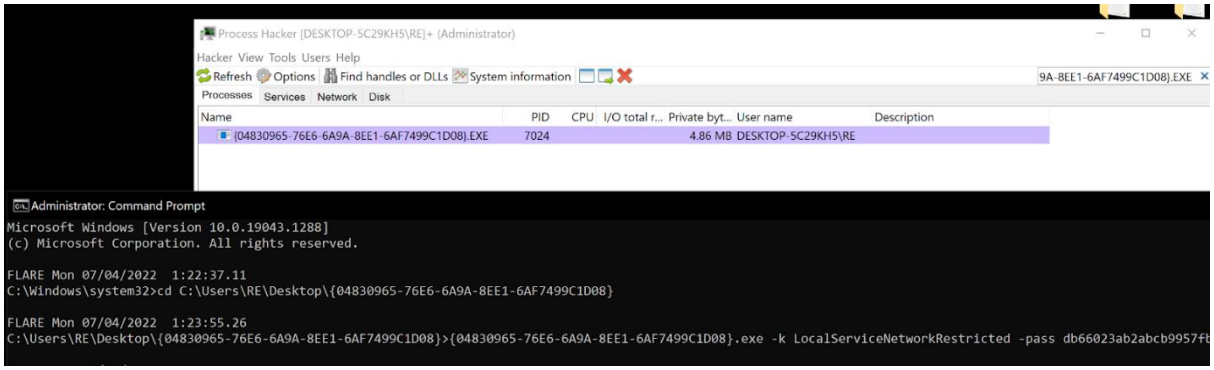
Technical Analysis of Lockbit 3.0 Ransomware

Execution Process

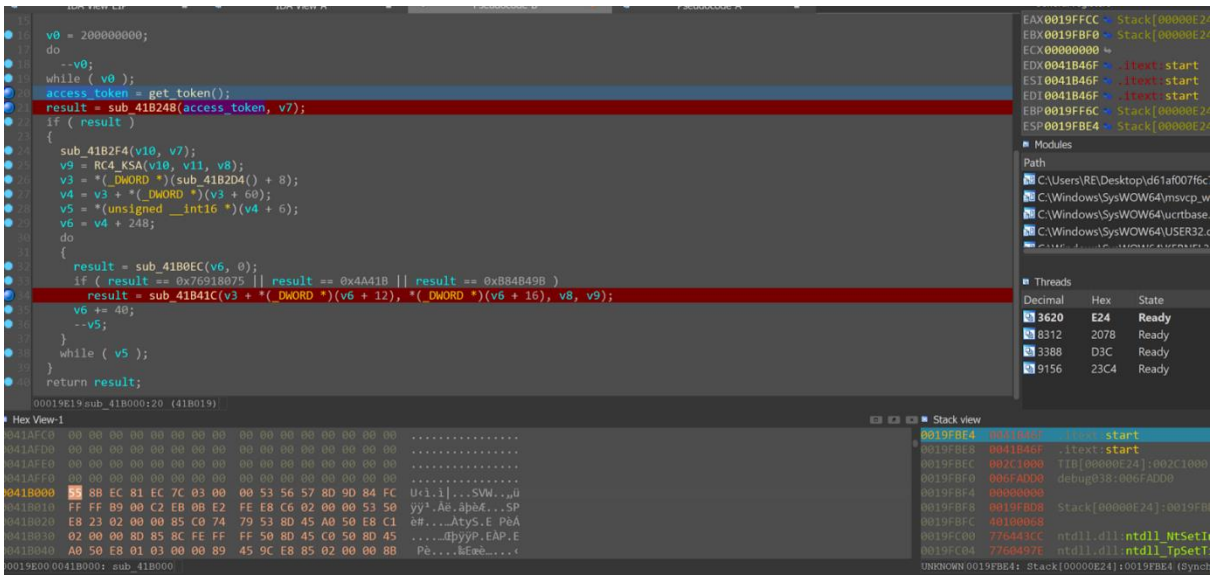
The first execution of Lockbit 3.0 Ransomware done by a “access token”:

- <Ransomware.exe> -k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a

This code protection mechanism encrypts the Lockbit 3.0 Ransomware code and help to evade malware detection. To execute the Ransomware successfully it needs a **parameter (-pass), this key will decrypt the source code of the Lockbit 3.0 and execute it on victim device.**



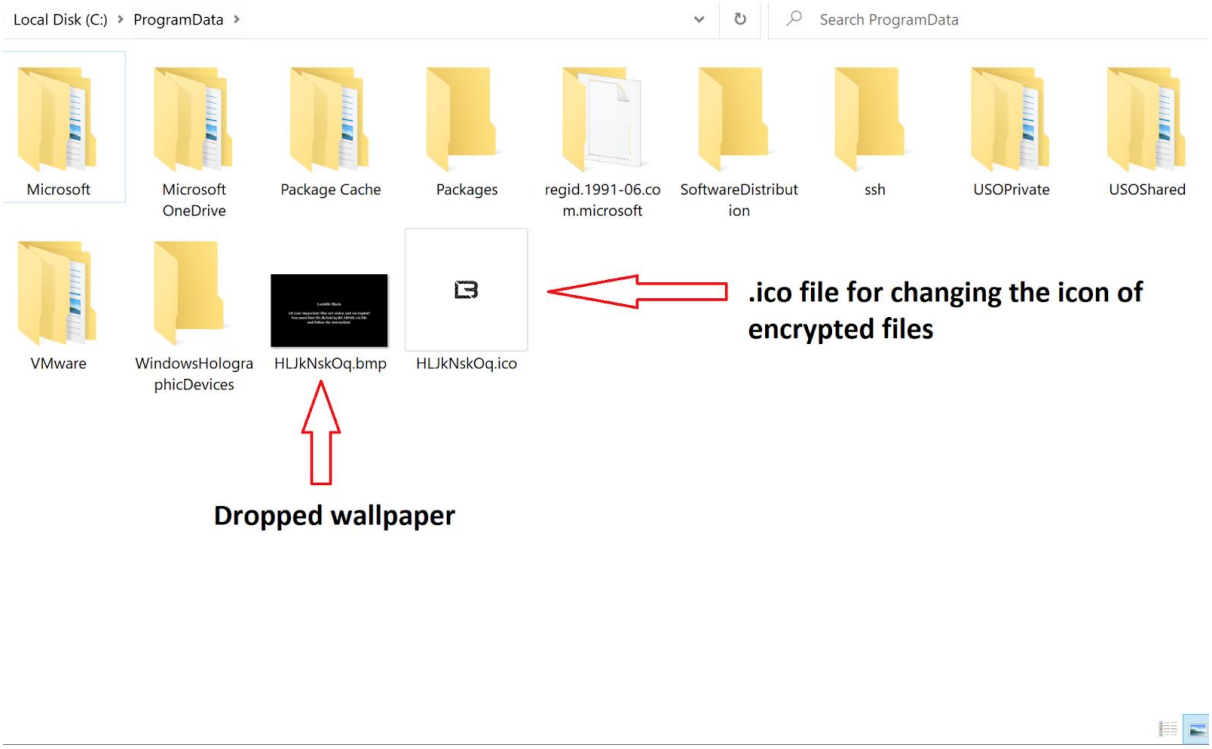
When Lockbit 3.0 started on the victim device, **sub_41B000** function is responsible for decryption of Ransomware code via decryption key supplied from the execution parameters.



sub_41B000 function

Ransom note wallpaper and .ico file written into C:\ProgramData\:

The icon (.ico) file being used to change icons of every encrypted files on the victim device and also every encrypted file renamed by random characters.



WriteFile Operation for the creation of README.txt and icon file

Below Procmon data showed us the WriteFile operations done by Lockbit 3.0 after the execution.

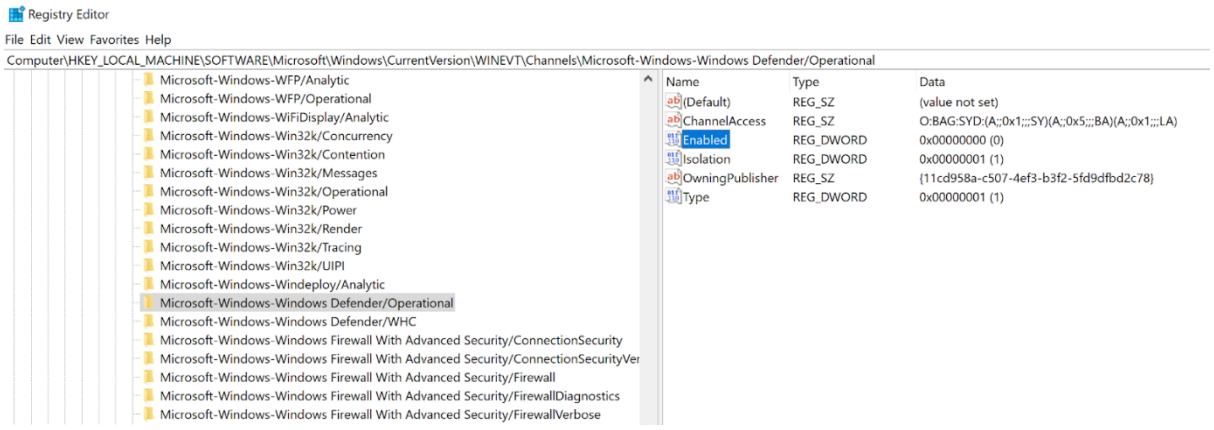
Process Name	PID	Operation	Path	Result
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	CreateFile	C:\ProgramData\HLJkNskOq.ico	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	WriteFile	C:\ProgramData\HLJkNskOq.ico	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegOpenKey	HKCU\Software\Classes\.HLJkNskOq	NAME NOT FOUND
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCreateKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegSetInfoKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegOpenKey	HKCU\Software\Classes\.HLJkNskOq	NAME NOT FOUND
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegSetValue	HKCR\.HLJkNskOq\(Default)	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCloseKey	HKCR\.HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegOpenKey	HKCU\Software\Classes\HLJkNskOq\DefaultIcon	NAME NOT FOUND
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCreateKey	HKCR\HLJkNskOq\DefaultIcon	NAME NOT FOUND
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCreateKey	HKCR\HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegSetInfoKey	HKCR\HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCreateKey	HKCR\HLJkNskOq\DefaultIcon	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCloseKey	HKCR\HLJkNskOq	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\HLJkNskOq\DefaultIcon	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\HLJkNskOq\DefaultIcon	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegOpenKey	HKCU\Software\Classes\HLJkNskOq\DefaultIcon	NAME NOT FOUND
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegQueryKey	HKCR\HLJkNskOq\DefaultIcon	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegSetValue	HKCR\HLJkNskOq\DefaultIcon\(Default)	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	RegCloseKey	HKCR\HLJkNskOq\DefaultIcon	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	CloseFile	C:\ProgramData\HLJkNskOq.ico	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	CreateFile	C:\HLJkNskOq.README.txt	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	WriteFile	C:\HLJkNskOq.README.txt	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384	WriteFile	C:\HLJkNskOq.README.txt	SUCCESS

Killing Windows Defender and tempering Windows Event Log

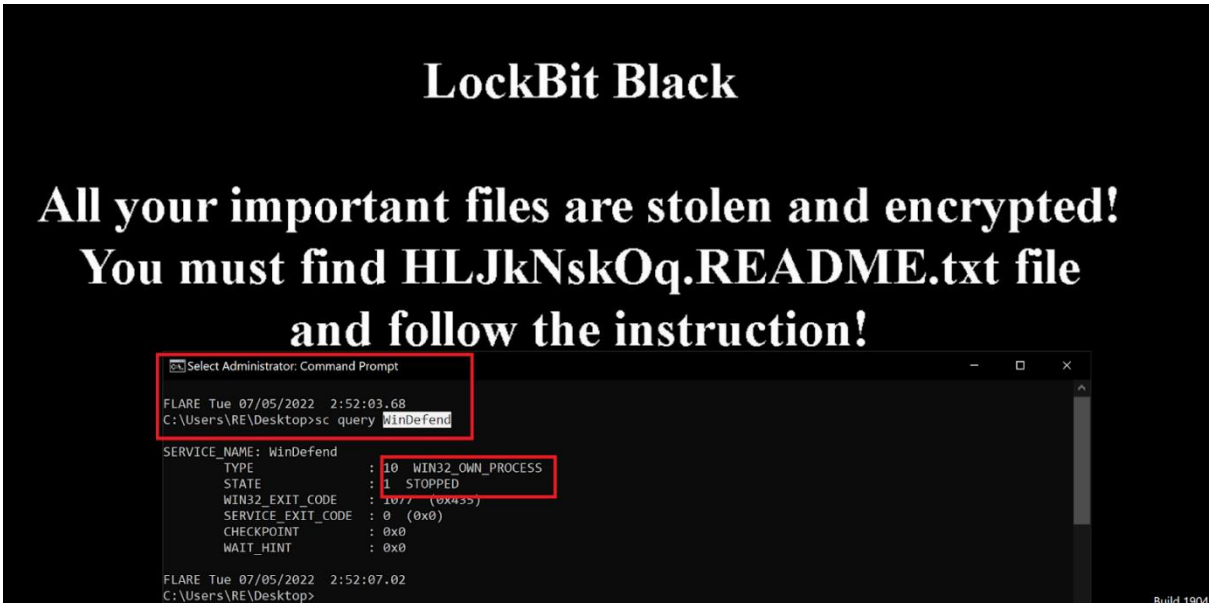
Ransomware developers wanted to disable the default security product of the victim device, in Lockbit 3.0 Ransomware we found that; it changes the bellowed registry keys to disable all Windows Event Log Messages.

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\<Log Name>**

After the registry key change, **Enabled key set to 0** and new Security Descriptor **(O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)** add it to temper the Event Logs.

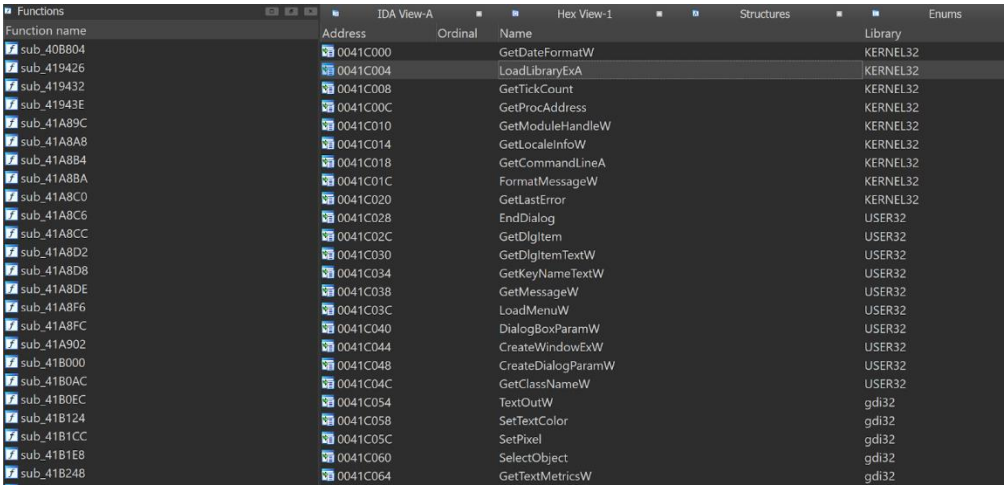


After the execution of Lockbit 3.0 (Lockbit Black), it stopped the Windows Defender Service as shown in image below.



Hiding the Windows APIs (import tables) for increasing the evasiveness

When we looked at the original sample of Lockbit 3.0 at IDA (Disassembly tool), sample have few function and Windows APIs, but in reality Lockbit 3.0 Ransomware developers hiding the function calls and Windows APIs by using **Stack String Obfuscation** and simple XOR Encryption.



This way Lockbit 3.0 Ransomware will load all of the Windows APIs during the execution time , which is increases the evasiveness, so in order to see the hidden API calls we can execute the sample and see the results under a Debugger or we can use HashDB on IDA to resolve the APIs .

After the decryption/unpacking of Ransomware code via -pass parameter ,Win32 APIs dynamically resolved by function **sub_407C5C** that receives as input an obfuscated string that is XORed with the key **0x4506DFCA**, so to decrypt the Win32 API name to be resolved.

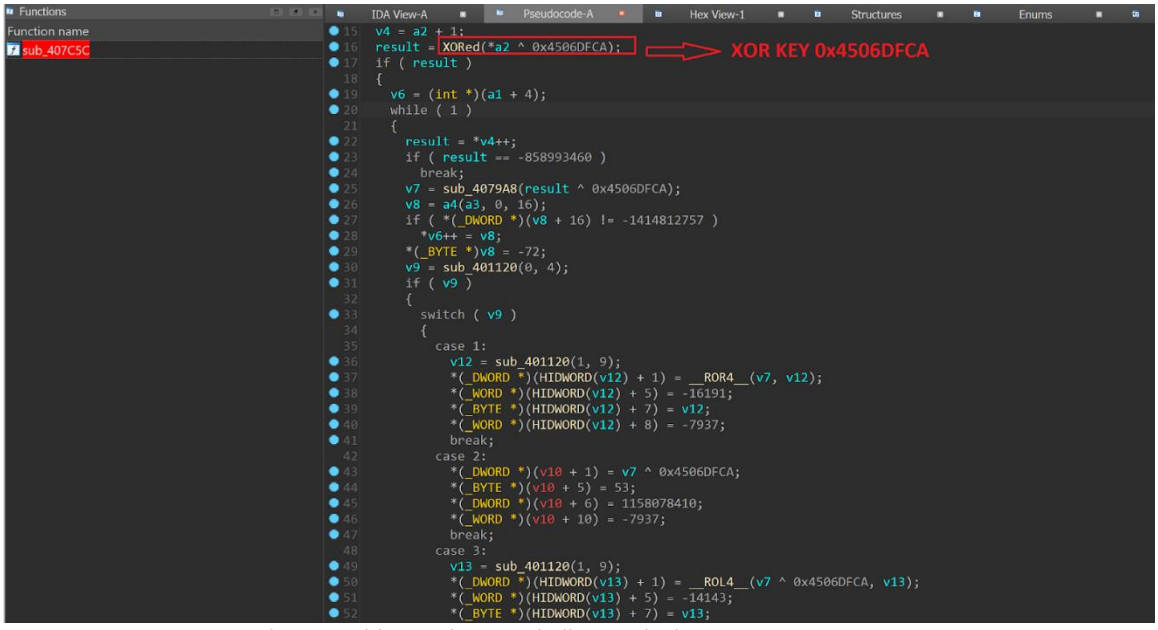
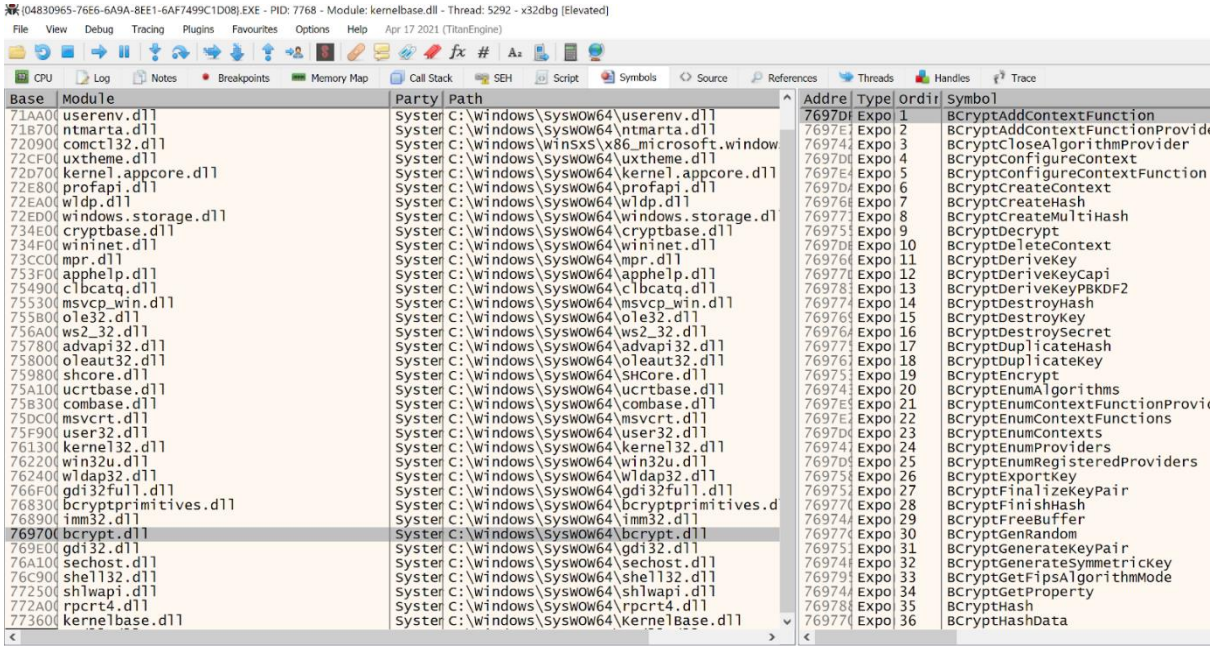
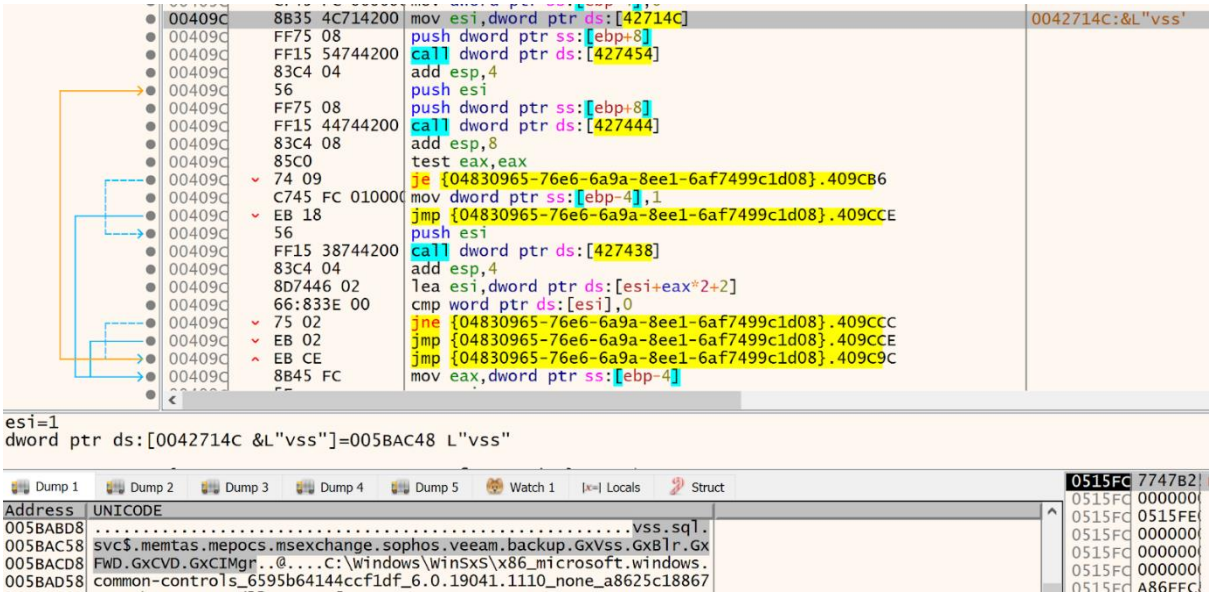


Figure 5 This part is very similar to BlackMatter Ransomware.

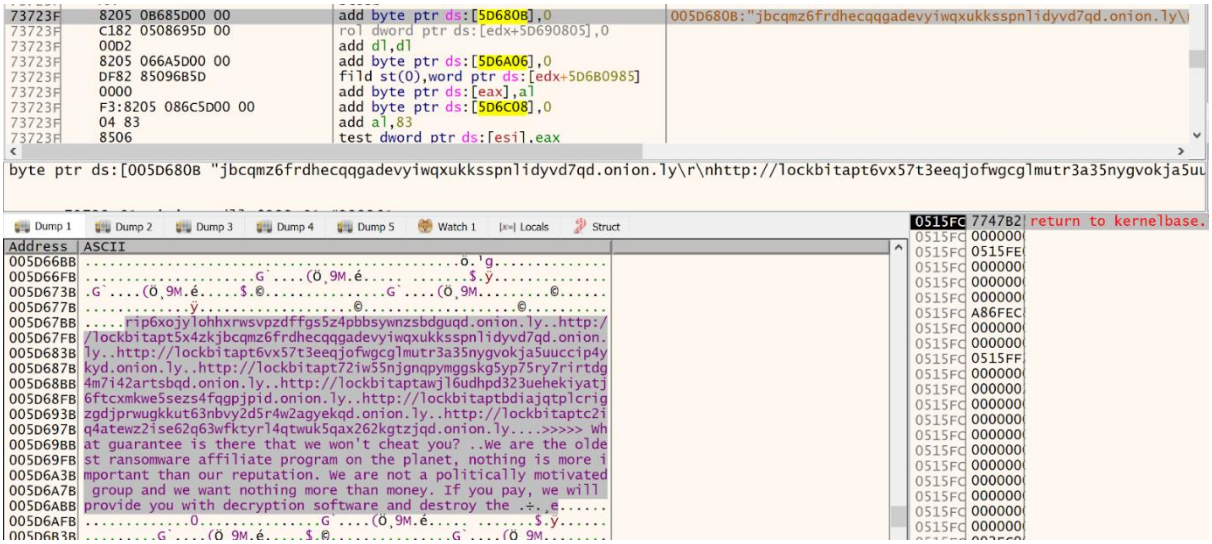
Now we can see the all loaded Windows APIs successfully under debugging screen, **including the bcrypt.dll which is being used during file encryption process by Lockbit 3.0**



While performing the Debugging, we can identify the **Windows Service blacklist**, this String data used by Lockbit 3.0 Ransomware to kill a specific named Service from victim device before the encryption starts, for example if I execute Lockbit 3.0 on Sophos installed device, first it will kill a Service named Sophos (AV vendor) to evade the detection. We also observed similar behavior on Lockbit 2.0

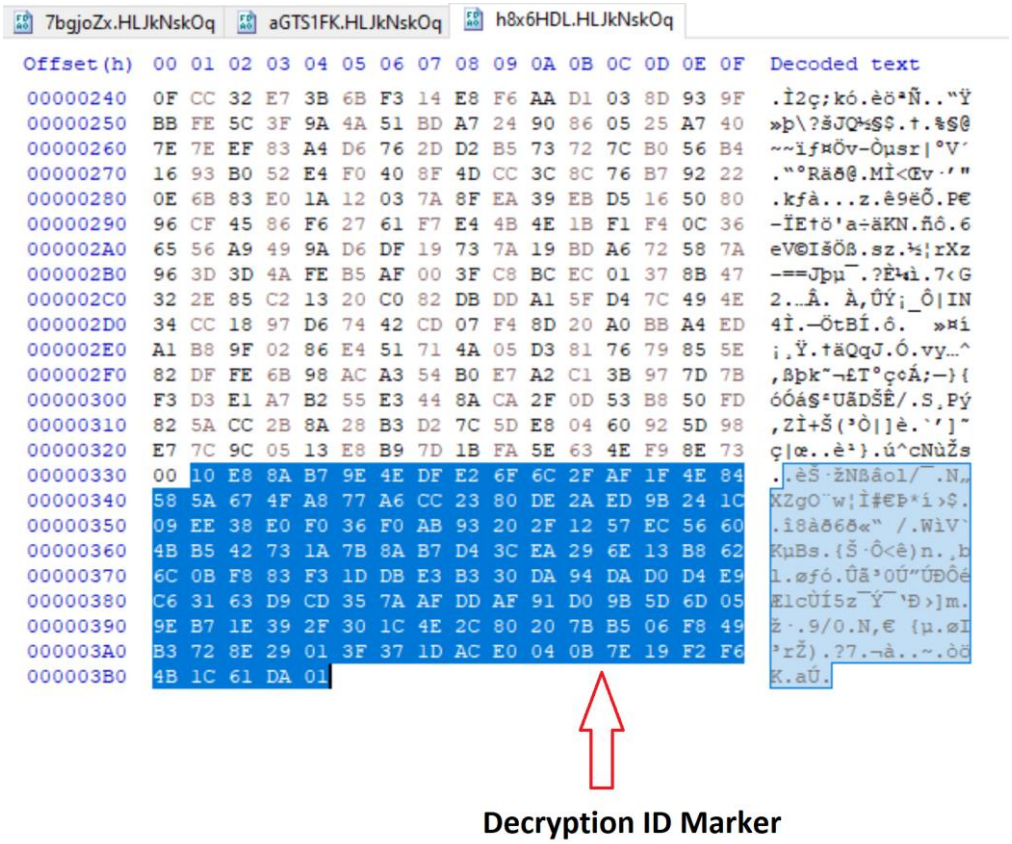


Normally the ransom note itself is also stored as encrypted, which means it can only be opened by a given “access token”, this way they can evade AV detection. After the execution we can see the ransom note on a memory dump.(Full ransom note can be seen here)



Encrypted file structure

Each encrypted file has a same marker at the end of the file, this marker has been used during the decryption process and this is the reason why Lockbit affiliates wanted an example of encrypted file after a negotiation process.



Mitigation and Prevention

- Maintain offline backups of data, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, and have irretrievable data.

- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between and access to various subnetworks and by restricting adversary lateral movement.

- Require multi-factor authentication for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.

- Keep all operating systems and software up to date. Prioritize patching known exploited vulnerabilities. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.

- Remove unnecessary access to administrative shares, especially ADMIN$ and C$

- Block public facing Remote Desktop Protocol (RDP). If remote access to RDP or terminal services is required, it should only be made accessible through a secure Virtual Private Network (VPN) connection (with Multi-Factor Authentication) to the corporate network or through a zero-trust remote access gateway.

- Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.

- Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.

- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.

- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows.
  Threat actors use PowerShell to deploy ransomware and hide their malicious activities.

LockBit 3.0 Tactics, Techniques and Procedures

TA0001 Initial Access	
T1190 Exploit Public-Facing Applications	Vulnerabilities such as BlueKeep (CVE-2019-0708) have been observed being utilized as footholds into the environment.
T1133 External Remote Services	Affiliates have been seen brute forcing exposed RDP services and compromising accounts with weak passwords.

TA0005 Defense Evasion	
T1562.001 Impair Defenses: Disable or Modify Tools	Windows Defender, other anti-malware solutions and monitoring tools are disabled.
T1070 Indicator Removal on Host	Indicators, such as logs in Windows Event Logs or malicious files, are removed after the execution of Lockbit 3.0
T1027 Obfuscated Files or Information	Lockbit 3.0 Ransomware using Stack String Obfuscation.

TA0040 Impact	
T1486 Data Encrypted for Impact	LockBit 3.0 Ransomware, encrypting devices and demanding a ransom.
T1489 Service Stop	During the defense evasion phase, anti-malware and monitoring software is disabled.

TA0010 Exfiltration	
T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	Affiliates can exfiltrate valuable data from victim device via RClone or Stealbit (Data Exfiltration tool)

Indicators of Compromise

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

Tor Browser Links for chat:
http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
http://lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion

Lockbit 3.0 Ransomware samples

SHA 256 - 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce

SHA 256 - a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e

SHA 256 - d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee

Sigma Rules

https://yaraify.abuse.ch/yarahub/rule/RANSOM_Lockbit_Black_Packer/
https://yaraify.abuse.ch/yarahub/rule/LockbitBlack_Loader/

infinitum IT
Power of integrated Security

Threat Spotlight: Lockbit Black 3.0 Ransomware