



Threat Spotlight: Lockbit Black 3.0 Ransomware

TABLE OF CONTENTS

What’s New on Lockbit Black 3.0 3

First Sample Publication 5

Insides From Real Life Incident Response 6

 Initial Access Point..... 6

Technical Analysis of Lockbit Black 3.0..... 7

Mitigation and Prevention 11

LockBit 3.0 Tactics, Techniques and Procedures 12

Indicators of Compromise..... 13

Lockbit 3.0 Ransomware samples 14

Sigma Rules 14

Threat Spotlight: Lockbit Black 3.0 Ransomware

What's New on Lockbit Black 3.0

Lockbit Ransomware is one of the most notorious groups since 2019, they have a wide range of attack scope including critical infrastructures like [hospital systems](#). According to Cyber Threat Intelligence members of Ininitum IT, the LockBit Ransomware group made an interesting updates on the publication site and the Ransomware itself

The screenshot shows a webpage header with the Lockbit 3.0 logo on the left, a red banner with the text "LEAKED DATA" in the center, and a red hamburger menu icon on the right. Below the header is a large white box with a red dashed border. Inside this box, the text "WEB SECURITY" is displayed in large black letters, followed by "BUG BOUNTY" in white letters on a red rectangular background. Below this, the text "Bug Bounty Program" is centered. Underneath is a small orange "#". At the bottom of the box, a paragraph reads: "We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from \$1000 to \$1 million."

Lockbit 3.0 has launched their own Bug Bounty program paying for web security exploits, and more.

This update on the publication site such as the Bug Bounty program, is aiming for more affiliation but most importantly sharing critical internal data to the Ransomware group members this can cause the increase of insiders Threats.

The main updates for Lockbit Black 3.0 Ransomware are:

- Anti Analysis technique to hide against AV vendors.
- Lockbit Black 3.0 requires an “access token” to be supplied as a parameter upon execution; it's similar to BlackCat.
- It has a command line argument feature.
- Much more evasive and faster than older versions of Lockbit.
- New Anti Debugging feature.
- The main code base is very similar to BlackMatter/Darkside Ransomware.
- Disabling the Windows Defender and tempering the Windows Event Logs.

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

```

HLJKNsKQq.README.txt
1  --- LockBit 3.0 the world's fastest and most stable ransomware from 2019---
2
3  >>>> Your data is stolen and encrypted.
4  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
5  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
6  your company will be safe.
7
8  Tor Browser Links:
9  http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
10 http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv413azl3gy6pyd.onion
11 http://lockbitapt34kvrp6xojylohhrxwsvpzdffgs5z4pbbsywnzsbduqd.onion
12 http://lockbitapt5x4zkjbcqmz6frdhecgqgadevyiwqkukksspnldiyvd7qd.onion
13 http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
14 http://lockbitapt72iw55njngnqymgskg5yp75ry7rirtgd4m7i42artsbqd.onion
15 http://lockbitaptawj16udhpd323uehekiyatj6ftcxmkwe5sezs4fqqppjid.onion
16 http://lockbitaptbdiajqtplcrlgzgdjprwugkkut63nbvy2d5z4w2agyekqd.onion
17 http://lockbitaptc2iq4atewz2lse62q63wfktyrl4qtwk5qax262kgtzjqd.onion
18
19 Links for normal browser:
20 http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
21 http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv413azl3gy6pyd.onion.ly
22 http://lockbitapt34kvrp6xojylohhrxwsvpzdffgs5z4pbbsywnzsbduqd.onion.ly
23 http://lockbitapt5x4zkjbcqmz6frdhecgqgadevyiwqkukksspnldiyvd7qd.onion.ly
24 http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
25 http://lockbitapt72iw55njngnqymgskg5yp75ry7rirtgd4m7i42artsbqd.onion.ly
26 http://lockbitaptawj16udhpd323uehekiyatj6ftcxmkwe5sezs4fqqppjid.onion.ly
27 http://lockbitaptbdiajqtplcrlgzgdjprwugkkut63nbvy2d5z4w2agyekqd.onion.ly
28 http://lockbitaptc2iq4atewz2lse62q63wfktyrl4qtwk5qax262kgtzjqd.onion.ly
29
30 >>>> What guarantee is there that we won't cheat you?
31 We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically
32 motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data.
33 After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system
34 administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest
35 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
36 decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Elon Musk's
37 Twitter https://twitter.com/hashtag/lockbit?f=live
38
39

```

Figure 1 Ransom note.

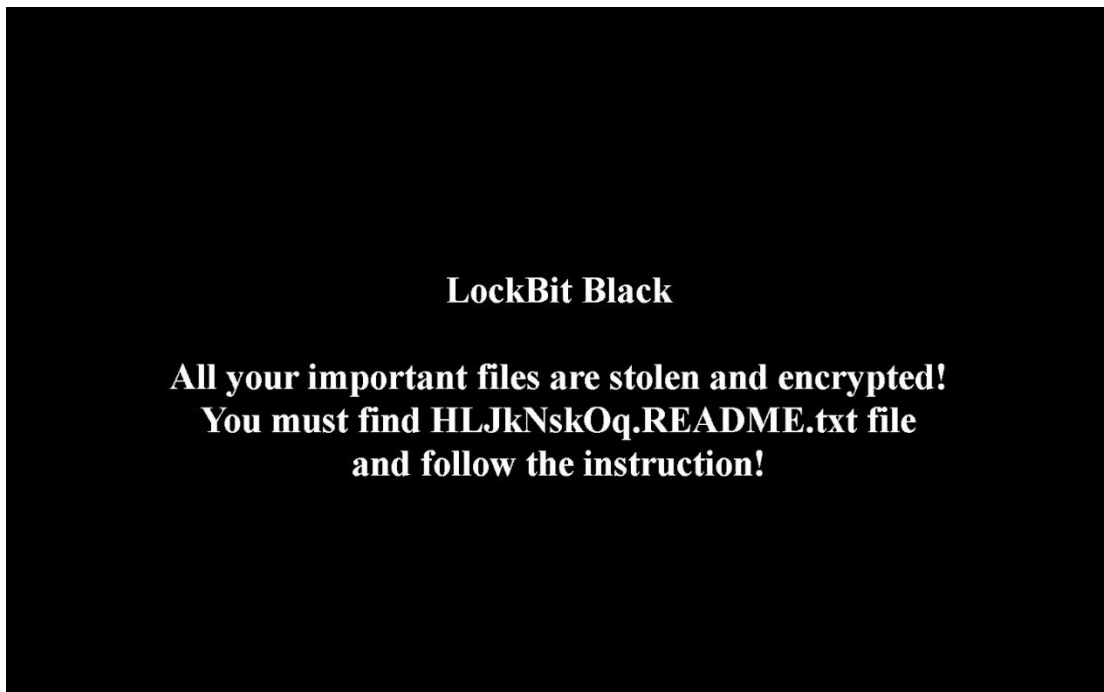
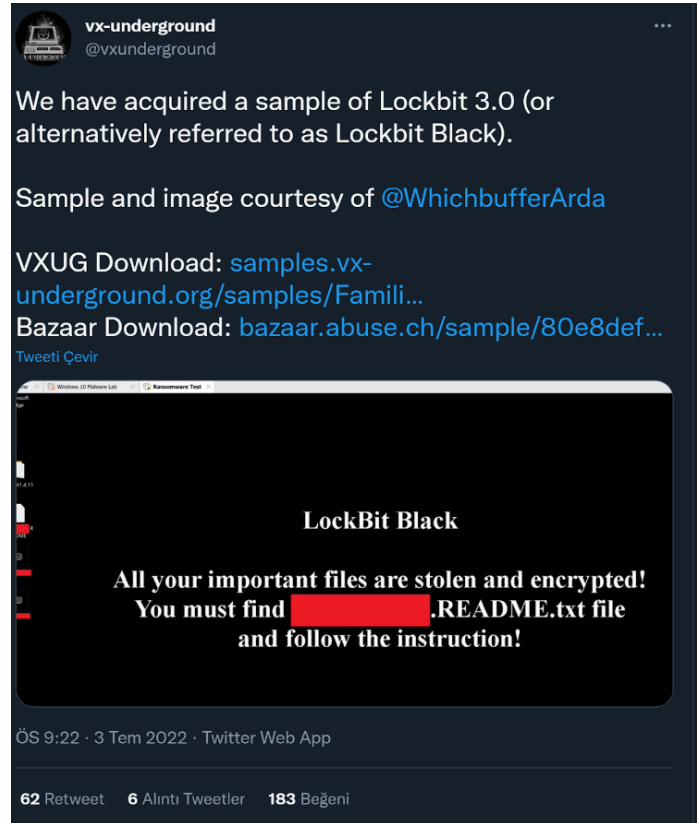


Figure 2 Changed wallpaper image.

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 who suffers from Lockbit Ransomware attack in a real-life Incident.



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

Minutes after the first publication the “access token” of Lockbit Blackcat 3.0 has been shared with the public for helping Malware Analyst from all over the world.



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

Insides From Real Life Incident Response

In order to obtain the first ever Lockbit 3.0 Ransomware sample, the Cyber Threat Intelligence team members in Infinitum IT, contacted with one of the Lockbit Ransomware victim and gather all of the necessary data to analyze during an Incident Response process, overall this data could help other companies to protect it self against Lockbit and other Ransomware groups.

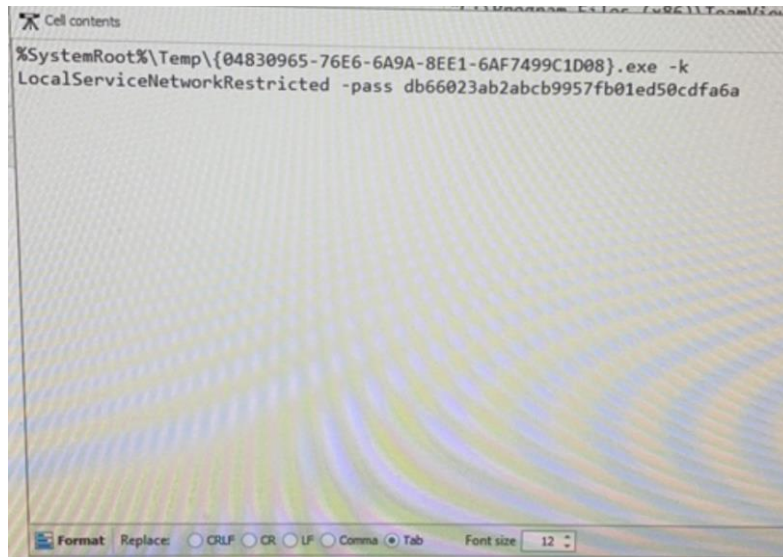


Figure 3 The first execution of Lockbit 3.0 Ransomware, supplied with "access token" (-pass).

Initial Access Point

According to the data obtained from the victim; Lockbit affiliate members used the BlueKeep (CVE-2019-0708) vulnerability and valid 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 an 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



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

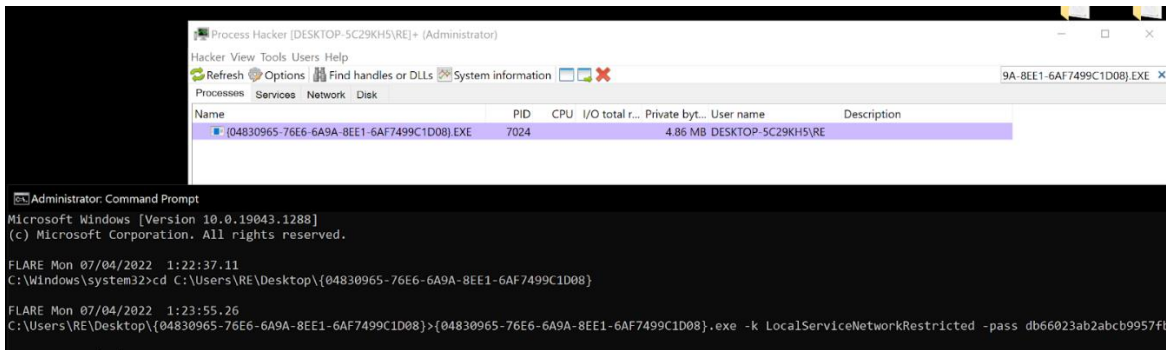
An attacker can exploit this vulnerability to take control of an affected system.

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

Technical Analysis of Lockbit Black 3.0

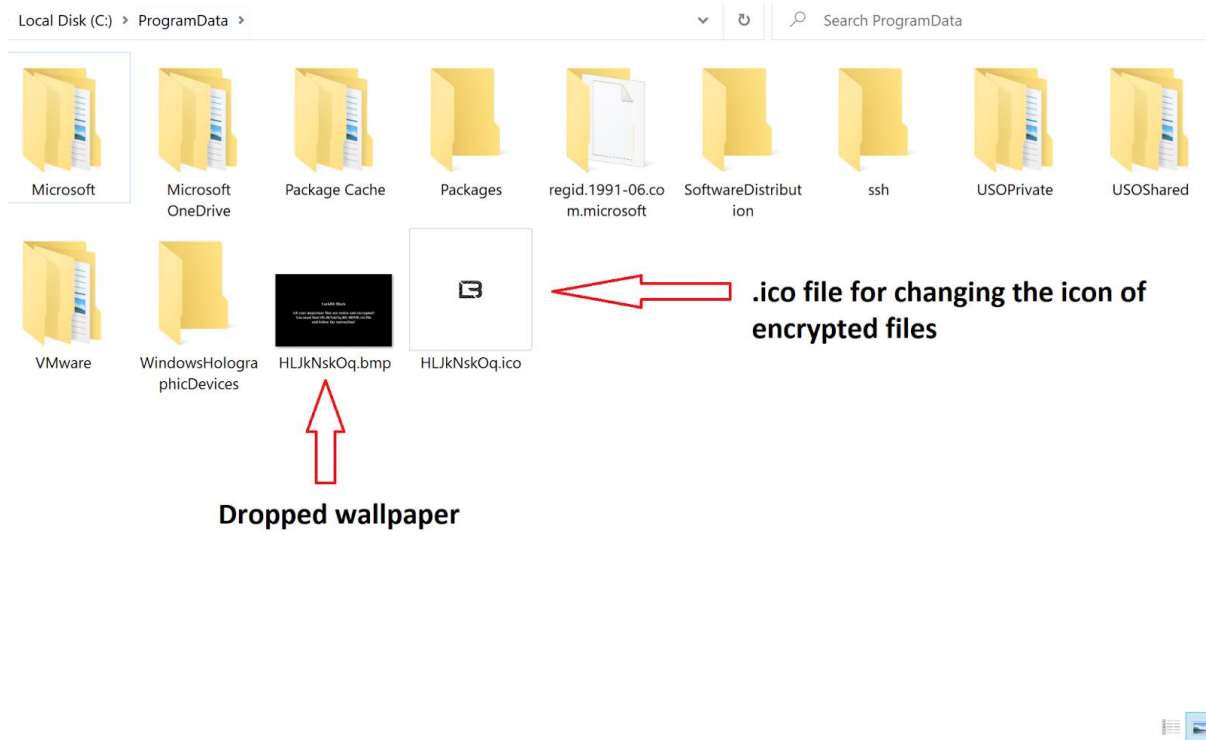
After the first execution of Lockbit 3.0 Ransomware with beloved “access token”:

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



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

The written .ico file name is the victim ID with 9 characters of data, this data is static and it's being used during the decryption process, also every encrypted file name has been changed to a random name attended by Lockbit 3.0. That .ico file is being used for changing encrypted file icons.

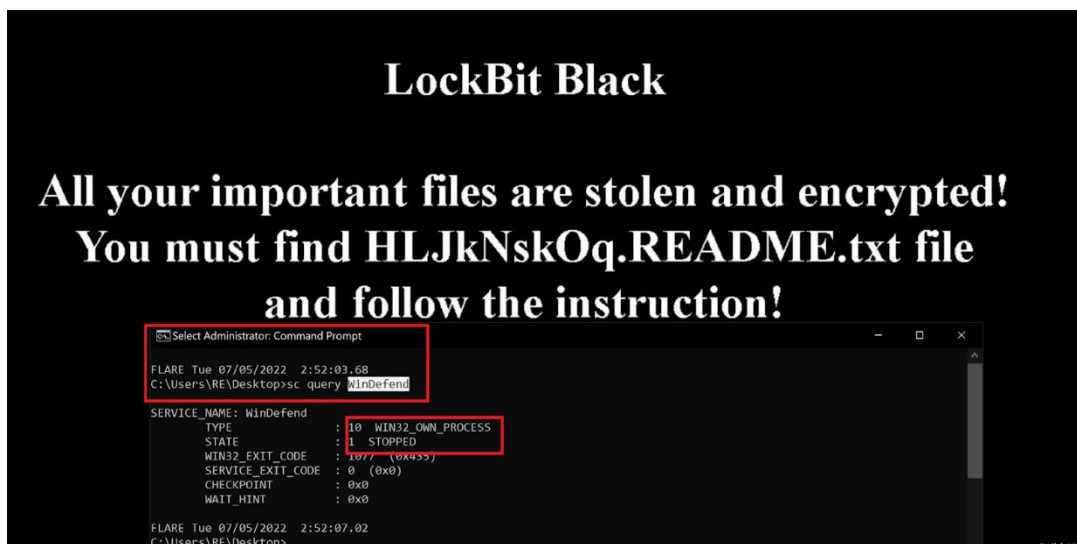


WriteFile Operation for the creation of README.txt and icon file

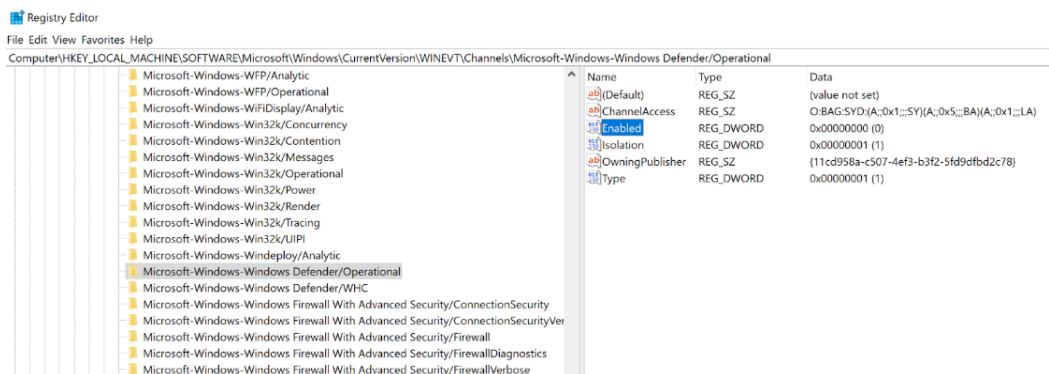
| Process Name | PID | Operation | Path | Result |
|--|------|---------------|---|----------------|
| {04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe | 3384 | CreateFile | C:\ProgramData\HLJkNskOq.ico | SUCCESS |
| {04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe | 3384 | WriteFile | C:\ProgramData\HLJkNskOq.ico | 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 the Windows Defender and tempering Windows Event Log

Oftentimes Ransomware developers want to disable the default security feature of the victim device, in Lockbit Black 3.0 Ransomware we found that it changes the registry keys to disable all Windows Event Log Messages and kill the Microsoft Defender Process/Service.

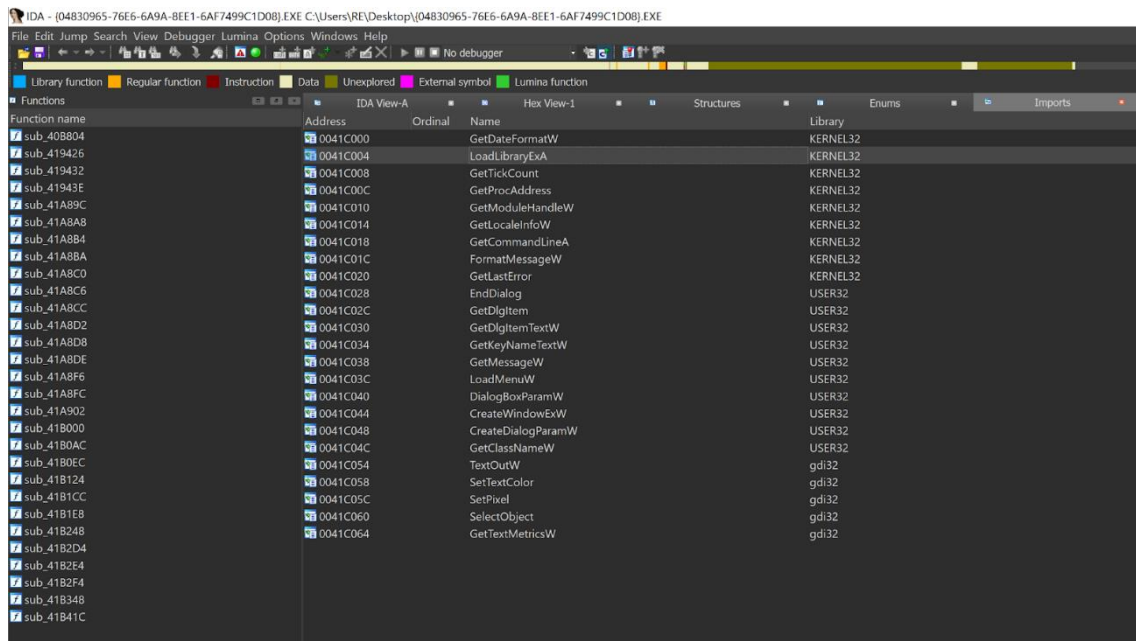


After the registry key change, **Enabled** key set to **0** and new Security Descriptor **(O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)** add it to temper the Event Logs.



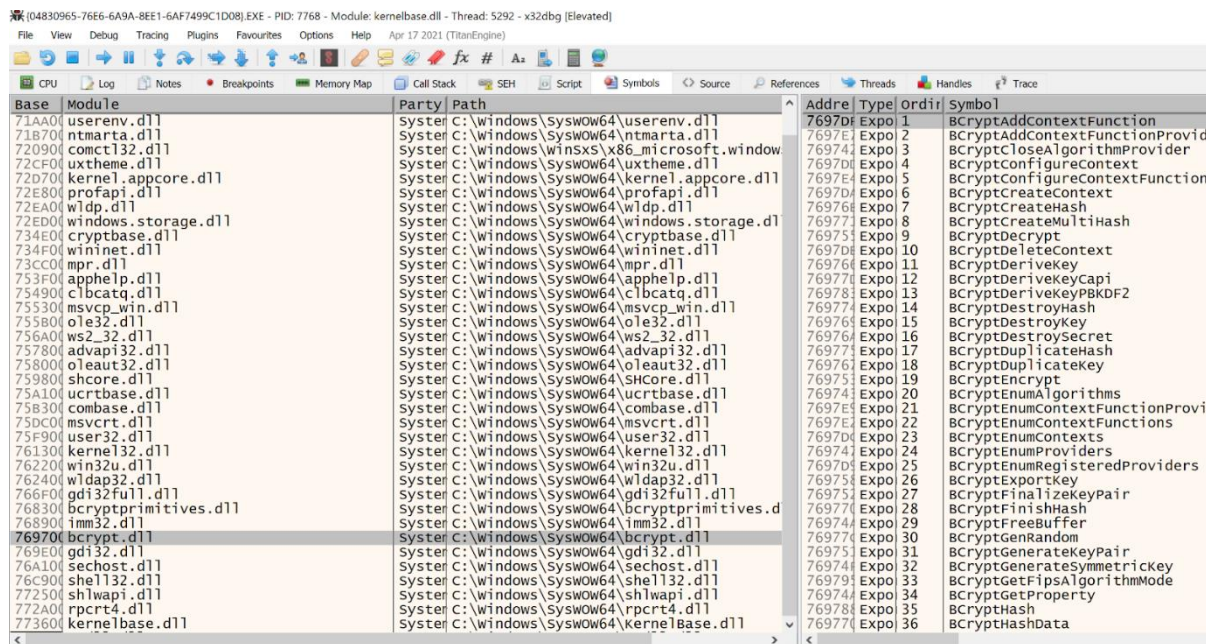
Hiding the Windows APIs (import tables) for increasing the evasiveness

When we look at the original sample at IDA (Disassembly tool), we can see that Lockbit 3.0 sample have very few function and Windows APIs but the reality is since the Lockbit 2.0, the Ransomware developers hiding the function calls and Windows APIs by using [Stack String Obfuscation](#) and simple XOR Encryption.



This way Lockbit 3.0 can load all of the Windows APIs during the execution time which increases the evasiveness, so in order to see the hidden API calls we can execute the sample and see the results under Debugger or we can use [HashDB](#) on IDA.

Now we can see the all loaded Windows APIs successfully, including the bcrypt.dll



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

Normally the ransom note itself is also stored as hidden, which means it can only be opened by a given “access token”, this way they can evade detection more, after the execution we can clearly 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.

```

7bgoZx.HLJkNskOq  aGTS1FK.HLJkNskOq  h8x6HDL.HLJkNskOq
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000240 0F CC 32 E7 3B 6B F3 14 E8 F6 AA D1 03 8D 93 9F .İ2ç;kó.èó*Ñ.."Ý
00000250 BB FE 5C 3F 9A 4A 51 BD A7 24 90 86 05 25 A7 40 »p\`šJQ~$$.+.&$e
00000260 7E 7E EF 83 A4 D6 76 2D D2 B5 73 72 7C B0 56 B4 ~~if#0v-0usr|°V`
00000270 16 93 B0 52 E4 F0 40 8F 4D CC 3C 8C 76 B7 92 22 ."°Rãøø.Mí<@v`"
00000280 0E 6B 83 E0 1A 12 03 7A 8F EA 39 EB D5 16 50 80 .kfa...z.ë9ëö.PE
00000290 96 CF 45 86 F6 27 61 F7 E4 4B 4E 1B F1 F4 0C 36 -İE+ò'a+àKN.ñó.6
000002A0 65 56 A9 49 9A D6 DF 19 73 7A 19 BD A6 72 58 7A eV@İšÖš.sz.~;rXz
000002B0 96 3D 3D 4A FE B5 AF 00 3F C8 BC EC 01 37 8B 47 ==Jpu`.?E+ti.7<G
000002C0 32 2E 85 C2 13 20 C0 82 DB DD A1 5F D4 7C 49 4E 2...Ă. Ă,ŮŸ;_Ŏ|IN
000002D0 34 CC 18 97 D6 74 42 CD 07 F4 8D 20 A0 BB A4 ED 4İ.-ŎtBİ.ö. »#i
000002E0 A1 B8 9F 02 86 E4 51 71 4A 05 D3 81 76 79 85 5E ;,Ÿ.+aQqŸ.Ŏ.vy...^
000002F0 82 DF FE 6B 98 AC A3 54 B0 E7 A2 C1 3B 97 7D 7B ,Bpk~-eT°çcĂ;-){
00000300 F3 D3 E1 A7 B2 55 E3 44 8A CA 2F 0D 53 B8 50 FD óóás°UãDšÉ/.S.Pý
00000310 82 5A CC 2B 8A 28 B3 D2 7C 5D E8 04 60 92 5D 98 ,Zİ+š(°Ŏ|)è..'']~
00000320 E7 7C 9C 05 13 E8 B9 7D 1B FA 5E 63 4E F9 8E 73 ç|œ..è°}.ú^cNùšs
00000330 00 10 E8 8A B7 9E 4E DF E2 6F 6C 2F AF 1F 4E 84 .eš-žNšãol/.N.
00000340 58 5A 67 4F A8 77 A6 CC 23 80 DE 2A ED 9B 24 1C XZgO°w;İ#E#i>$.
00000350 09 EE 38 E0 F0 36 F0 AB 93 20 2F 12 57 EC 56 60 .İšãøøøœ" /WiV`
00000360 4B B5 42 73 1A 7B 8A B7 D4 3C EA 29 6E 13 B8 62 KuBs.(š-Ŏ<è)n..b
00000370 6C 0B F8 83 F3 1D DB E3 B3 30 DA 94 DA D0 D4 E9 l.eřó.Ůã°ŮŮ"ŮBŎé
00000380 C6 31 63 D9 CD 35 7A AF DD AF 91 D0 9B 5D 6D 05 ElcŮİšz-Ÿ`Ů>}m.
00000390 9E B7 1E 39 2F 30 1C 4E 2C 80 20 7B B5 06 F8 49 È.9/0.N,€ (u.œİ
000003A0 B3 72 8E 29 01 3F 37 1D AC E0 04 0B 7E 19 F2 F6 *rž).?7.-ã...-òö
000003B0 4B 1C 61 DA 01 K.aŮ.
    
```



Decryption ID Marker

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\$
- Do not set your RDP to be publicly facing.



DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal

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://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion>
<http://lockbitapt34kvrp6xojylohxrwsvpzdffgs5z4pbbsywnzsbduqd.onion>
<http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukkssplidyvd7qd.onion>
<http://lockbitapt6vx57t3eejqofwgcglmutr3a35nygvokja5uuccip4kyd.onion>
<http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirdg4m7i42artsbqd.onion>
<http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqjpid.onion>
<http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion>
<http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion>

Links for normal browser:

<http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly>
<http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion.ly>
<http://lockbitapt34kvrp6xojylohxrwsvpzdffgs5z4pbbsywnzsbduqd.onion.ly>
<http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukkssplidyvd7qd.onion.ly>
<http://lockbitapt6vx57t3eejqofwgcglmutr3a35nygvokja5uuccip4kyd.onion.ly>
<http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirdg4m7i42artsbqd.onion.ly>
<http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqjpid.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://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtk5xflw3draxk6gwqd.onion>
<http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion>
<http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion>
<http://lockbitsupuhsw4izvoucoxsbnokmgq6durg7kfcg6u33zfvq3oyd.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/



Threat Spotlight: Lockbit Black 3.0 Ransomware