



Threat Spotlight: Lockbit Black 3.0 Ransomware

### **TABLE OF CONTENTS**

3
5
6
6
7
11
12
13
14
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 <u>hospital systems</u>. According to Cyber Threat Intelligence members of Infinitum IT, the LockBit Ransomware group made an interesting updates on the publication site and the Ransomware itself



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:

HLJ	NekOq.README.ist 🗹
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
	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.
5	
6	Tor Browser Links:
7	http://lockbitapt2d73krlbewgv27tguljgxr33xbwwsp6rkyieto7u4ncead.onion
8	http://lockbitapt2yfbt7lchxejug47kmgvggxvvjpgkmevv413az13gy6pyd.onion
	http://lockbitapt34kyrip6xojylohhxrwsypzdffgs5z4pbbsywnzsbdgugd.onion
	http://lockbitapt5x4zkjbcamz6frdhecgggadevyiwgxukksspnlidyvd7gd.onion
	http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
	http://lockbitapt72iw55njgngpymggskq5yp75ry7rirtdg4m7i42artsbgd.onion
	http://lockbitaptawil6udhpd323uehekivatj6ftcxmkwe5sezs4fqqppid.onion
	http://lockbitaptbdiajgtplcrigzgdiprwugkkut63nbvy2d5r4w2agyekgd.onion
	http://lockbitaptc2ig4atewz2ise62g63wfktvrl4gtwuk5gax262kgtzigd.onion
16	
17	Links for normal browser:
18	http://lockbitapt2d73krlbewgv27tguljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
19	http://lockbitapt2yfbt7lchxejug47kmgyggxvyjpgkmevv413az13gy6pyd.onion.ly
	http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdgugd.onion.ly
	http://lockbitapt5x4zkjbcgmz6frdhecgggadevyiwgxukksspnlidyvd7gd.onion.ly
	http://lockbitapt6vx57t3eegjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
23	http://lockbitapt72iw55njgngpymggskg5yp75ry7rirtdg4m7i42artsbgd.onion.ly
24	http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fggpjpid.onion.ly
25	http://lockbitaptbdiajgtplcrigzgdjprwugkkut63nbvv2d5r4w2agvekgd.onion.ly
26	http://lockbitaptc2iq4atewz2ise62q63wfktyr14qtwuk5qax262kqtzjqd.onion.ly
27	
	>>>>> What guarantee is there that we won't cheat you?
29	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







# **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.



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.





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 authorities

### **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



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 authorities

# **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

Process Hacker [DESKTOP-5C29KH5\RE]+ (Administrato	ur)			– 🗆 ×
Hacker View Tools Users Help				
😴 Refresh 🗇 Options   🕌 Find handles or DLLs 💯 System	informati	ion 🗔 🔜 💥		9A-8EE1-6AF7499C1D08}.EXE
Processes Services Network Disk				
Name	PID	CPU I/O total r Private byt User name	Description	
(04830965-76E6-6A9A-8EE1-6AF7499C1D08).EXE	7024	4.86 MB DESKTOP-5C29KH5\F	RE	
्य Administrator: Command Prompt				
ন্ত্রAdministrator.Command Prompt icrosoft Windows [Version 10.0.19043.1288] c) Microsoft Corporation. All rights reserved.				
licrosoft Windows [Version 10.0.19043.1288]	-6AF749	990(1008}		

### 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\.HLJkNskOg	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384 RegQueryKey	HKCR\.HLJkNskOg	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\.HLJkNskOg	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384 RegSetValue	HKCR\.HLJkNskOq\(Default)	SUCCESS
{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe	3384 RegCloseKey	HKCR\.HLJkNskOg	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\HLJkNskOg	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\HLJkNskOg\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\HLJkNskOg\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 **(0:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)** add it to temper the Event Logs.



8

#### 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 <u>Stack String</u> <u>Obfuscation</u> and simple XOR Encryption.

Functions     EDA View-A     Hex View-1     Structures     Enums     Function name       Address     Ordinal     Name     Library     Library       sub.408804     10.0041(C00     GetDateFormatW     KERNEL32       sub.419426     10.0041(C00     GetTateFormatW     KERNEL32       sub.419426     10.0041(C00     GetTateFormatW     KERNEL32       sub.419426     10.0041(C00     GetTateFormatW     KERNEL32       sub.419426     10.0041(C00     GetTateFormatW     KERNEL32       sub.414826     10.0041(C010     GetModuleHandleW     KERNEL32       sub.414884     10.0041(C010     GetLocaleInforW     KERNEL32       sub.414880     10.0041(C018     GetLocaleInforW     KERNEL32       sub.414860     10.0041(C018     GetLocaleInforW     KERNEL32       sub.414860     10.0041(C02     GetLastFror     KERNEL32       sub.414860     10.0041(C02     GetLogBane     USFR32       sub.414860     10.0041(C02     GetLogBane     USFR32       sub.414860     10.0041(C030     GetLogBane     USFR32       sub.414860     10.0041(C030     GetLogBane     USFR32       sub.414860     10.0041(C030     GetLogBane     USFR32       sub.414800     10.0041(C030     GetLogBane	Ordinal         Name         Library           0041C000         GetDateFormatW         KERNE132           0041C004         LoadLibraryExA         KERNE132           0041C005         GetTickCount         KERNE132           0041C006         GetTickCount         KERNE132           0041C010         GetHooduleHandleW         KERNE132           0041C010         GetLocaleInfoW         KERNE132           0041C011         GetLocaleInfoW         KERNE132           0041C012         GetLocaleInfoW         KERNE132           0041C013         GetLocaleInfoW         KERNE132           0041C014         GetLocaleInfoW         KERNE132           0041C020         GetLastError         KERNE132           0041C020         GetLotError         KERNE132           0041C020         GetLotError         KERNE132           0041C020         GetLotError         KERNE132           0041C030         GetDigItemTextW         USER32           0041C031         GetKeyNameTextW         USER32           0041C032         LoadMenuW         USER32           0041C033         GetKeyNameTextW         USER32           0041C040         DialogBorParamW         USER32 <t< th=""><th>Library function Regular function</th><th>Instruction 📃 Data 📕 L</th><th>Jnexplored Ext</th><th>ernal symbol</th><th>Lumina function</th><th></th><th></th><th></th><th></th><th></th><th></th></t<>	Library function Regular function	Instruction 📃 Data 📕 L	Jnexplored Ext	ernal symbol	Lumina function						
Sub_408804         III 0041(000         GetDateFormatW         KERNEL32           sub_419426         III 0041(0004         LoadlibrayExA         KERNEL32           sub_419426         III 0041(0008         GetTateKCount         KERNEL32           sub_419432         III 0041(0002         GetModule+andleW         KERNEL32           sub_41489C         III 0041(0010         GetModule+andleW         KERNEL32           sub_414881         III 0041(0110         GetModule+andleW         KERNEL32           sub_414884         III 0041(0116         GetCommandLineA         KERNEL32           sub_414884         III 0041(020         GetLorentaleW         KERNEL32           sub_414886         III 0041(020         GetLorentale         KERNEL32           sub_414886         III 0041(020         GetLorentalesageW         KERNEL32           sub_414886         III 0041(020         GetMeyNameTextW         USER32	0041C000         GetDateFormatW         KERNEL32           0041C003         GetTickCount         KERNEL32           0041C003         GetProcAddress         KERNEL32           0041C001         GetProcAddress         KERNEL32           0041C003         GetProcAddress         KERNEL32           0041C010         GetModuleHandleW         KERNEL32           0041C011         GetCommandLineA         KERNEL32           0041C013         GetCommandLineA         KERNEL32           0041C016         FormatMessageW         KERNEL32           0041C020         GetLastError         KERNEL32           0041C020         GetLastError         KERNEL32           0041C020         GetLastError         KERNEL32           0041C021         GetMgItemTextW         USER32           0041C030         GetUgItemTextW         USER32           0041C031         GetKeyNameTextW         USER32           0041C032         LoadMenuW         USER32           0041C033         GetLessageW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateWindowSW         USER32           0041C042         GetClastnameW         USER32	Functions		IDA View-A		Hex View-1	Structures		Enums	5	Imports	
Sub_419426         To 0441C004         LaadLibraryExA         KERNEL32           sub_419432         To 0441C004         GetTickCount         KERNEL32           sub_419432         To 0441C006         GetTickCount         KERNEL32           sub_419432         To 041C000         GetModuleHandleW         KERNEL32           sub_414884         To 041C010         GetModuleHandleW         KERNEL32           sub_414884         To 041C018         GetLocaleInfoW         KERNEL32           sub_414884         To 041C018         GetLocaleInfoW         KERNEL32           sub_414884         To 041C018         GetLocaleInfoW         KERNEL32           sub_414884         To 041C020         GetLocaleInfoW         KERNEL32           sub_414866         To 041C020         GetLocaleInfoW         KERNEL32           sub_414866         To 041C020         GetDigitem         USER32           sub_414806         To 041C020         GetDigitem TextW         USER32           sub_414808         To 041C030         GetMessageW         USER32           sub_414806         To 041C030         GetMessageW         USER32           sub_414806         To 041C030         GetMessageW         USER32           sub_414806         To 041C040	0041C004         LoadLibraryEvA         KERNEL32           0041C008         GetTickCount         KERNEL32           0041C000         GetTickCount         KERNEL32           0041C001         GetModuleHandleW         KERNEL32           0041C002         GetModuleHandleW         KERNEL32           0041C001         GetModuleHandleW         KERNEL32           0041C002         GetLocaleInfoW         KERNEL32           0041C016         GetLocaleInfoW         KERNEL32           0041C020         GetLastError         KERNEL32           0041C020         GetLastError         KERNEL32           0041C024         GetBlgtem         USER32           0041C035         GetKeyNameTextW         USER32           0041C034         GetKeyNameTextW         USER32           0041C035         GetMessageW         USER32           0041C034         GetKeyNameTextW         USER32           0041C035         GetMessageW         USER32           0041C040         DialogBoaParamW         USER32           0041C041         CreateWindowEvW         USER32           0041C042         GetLasWindowEvW         USER32           0041C043         CreateWindowEvW         USER32		Address	Ord	nal Name			Library				
ub. 419426         ID 00410004         LoadLibraryEvA         KERNEL32           ub. 419432         ID 00410000         GetTrickCount         KERNEL32           ub. 419434         ID 00410000         GetWordAdress         KERNEL32           ub. 414947         ID 00410010         GetWordAdress         KERNEL32           ub. 414986         ID 00410010         GetWordAdress         KERNEL32           ub. 414987         ID 00410010         GetWordAdress         KERNEL32           ub. 414884         ID 00410010         FormatMessageW         KERNEL32           ub. 414884         ID 00410010         GetCommandLineA         KERNEL32           ub. 414884         ID 00410020         GetLastFror         KERNEL32           ub. 414860         ID 00410208         GetDigIterm TextW         USER32           ub. 414861         ID 00410304         GetDigIterm TextW         USER32           ub. 414802         ID 00410304         GetMossageW         USER32           ub. 414808         ID 00410304         GetMossageW         USER32           ub. 414808         ID 00410304         GetMossageW         USER32           ub. 414806         ID 00410304         CreateDialogBorParamW         USER32           ub. 414807 <tdi< td=""><td>0041C004         LoadLibraryEsA         KERNE132           0041C002         GetTricCount         KERNE132           0041C002         GetTricCount         KERNE132           0041C001         GetModuleHandleW         KERNE132           0041C002         GetModuleHandleW         KERNE132           0041C001         GetModuleHandleW         KERNE132           0041C002         GetLocaleInfoW         KERNE132           0041C002         GetLastError         KERNE132           0041C020         GetLastError         KERNE132           0041C020         GetLigtem         USER32           0041C024         GetMogameTextW         USER32           0041C033         GetMogameTextW         USER32           0041C034         GetMessageW         USER32           0041C035         LandMenuW         USER32           0041C040         DialogBorParamW         USER32           0041C041         CreateWindowErW         USER32           0041C042         GetLasVineW         USER32           0041C043         CreateDialogParamW         USER32           0041C044         GetLasVineW         USER32           0041C045         TextOutW         USER32           0041C0</td><td>ub_40B804</td><td><b>10041</b></td><td>000</td><td>GetDa</td><td>teFormatW</td><td></td><td>KERNEL32</td><td></td><td></td><td></td><td></td></tdi<>	0041C004         LoadLibraryEsA         KERNE132           0041C002         GetTricCount         KERNE132           0041C002         GetTricCount         KERNE132           0041C001         GetModuleHandleW         KERNE132           0041C002         GetModuleHandleW         KERNE132           0041C001         GetModuleHandleW         KERNE132           0041C002         GetLocaleInfoW         KERNE132           0041C002         GetLastError         KERNE132           0041C020         GetLastError         KERNE132           0041C020         GetLigtem         USER32           0041C024         GetMogameTextW         USER32           0041C033         GetMogameTextW         USER32           0041C034         GetMessageW         USER32           0041C035         LandMenuW         USER32           0041C040         DialogBorParamW         USER32           0041C041         CreateWindowErW         USER32           0041C042         GetLasVineW         USER32           0041C043         CreateDialogParamW         USER32           0041C044         GetLasVineW         USER32           0041C045         TextOutW         USER32           0041C0	ub_40B804	<b>10041</b>	000	GetDa	teFormatW		KERNEL32				
sub.419432         GotAlCOOB         GetTickCount         KERNEL32           sub.41943E         Gr0AlCOOC         GetProcAddress         KERNEL32           sub.41943E         Gr0AlCOOC         GetProcAddress         KERNEL32           sub.41484C         Gr0AlCOOC         GetProcAddress         KERNEL32           sub.41488A         Gr0AlCOOL         GetLocaleInfoW         KERNEL32           sub.41488A         Gr0AlCOOL         GetLocaleInfoW         KERNEL32           sub.4148AA         Gr0AlCOOL         GetLoszleInfoW         KERNEL32           sub.4148AC         Gr0AlCOOL         GrdAlssageW         KERNEL32           sub.4148AC         Gr0AlCO2B         GetLoszleTror         KERNEL32           sub.4148CO         Gr0AlCO2B         GetLoszleTror         KERNEL32           sub.4148CO         Gr0AlCO2B         GetLoszleTror         KERNEL32           sub.4148CO         Gr0AlCO2B         GetLoszleTror         KERNEL32           sub.4148D2         Gr0AlCO2B         GetLoszleTror         KERNEL32           sub.4148D2         Gr0AlCO2B         GetLoszleTror         USER32           sub.4148D2         Gr0AlCO2B         GetLoszleTror         USER32           sub.4148D2         Gr0AlCO3B         GetL	0041C008         GetTickCount         KERNEL32           0041C010         GetProcAddress         KERNEL32           0041C010         GetProcAddress         KERNEL32           0041C010         GetProcAddress         KERNEL32           0041C011         GetLocaleInfoW         KERNEL32           0041C014         GetLocaleInfoW         KERNEL32           0041C010         FormatMessageW         KERNEL32           0041C020         GetLastError         KERNEL32           0041C030         GetDigIterm         USER32           0041C031         GetKeyAmeTextW         USER32           0041C032         LoadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateVindowSW         USER32           0041C042         GetClassNameW         USER32 <td< td=""><td>sub_419426</td><td>00410</td><td>2004</td><td></td><td></td><td></td><td>KERNEL32</td><td></td><td></td><td></td><td></td></td<>	sub_419426	00410	2004				KERNEL32				
Sub_41A89C         Dividuality         KERNEL32           sub_41A84         10041C010         GettocallerhofW         KERNEL32           sub_41A84         10041C014         GettocallerhofW         KERNEL32           sub_41A84         10041C018         GettocallerhofW         KERNEL32           sub_41A84         10041C01C         FormaldLineA         KERNEL32           sub_41A84         10041C01C         FormatMessageW         KERNEL32           sub_41A8C0         10041C020         GettastError         KERNEL32           sub_41A8C0         10041C020         GettastError         KERNEL32           sub_41A8C0         10041C020         GettastError         USER32           sub_41A8C0         10041C020         GettastError         USER32           sub_41A8C0         10041C020         GettastError         USER32           sub_41A8C1         10041C020         GettogethameTextW         USER32           sub_41A8C2         10041C034         GettogetharmExtW         USER32           sub_41A8C6         10041C040         DialogBorMarmW         USER32           sub_41A902         10041C044         CreateMindowExW         USER32           sub_41806         10041C044         CreateMindowExW         USER32 </td <td>0041C010         GetModuleHandleW         KERNEL32           0041C014         GetLocalInfoW         KERNEL32           0041C018         GetLocalInfoW         KERNEL32           0041C010         FormatMessageW         KERNEL32           0041C012         FormatMessageW         KERNEL32           0041C020         GetLastError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         VSER32           0041C020         GetMolatem         VSER32           0041C021         GetKeyNameTextW         VSER32           0041C033         GetMolatemTextW         VSER32           0041C040         DialogBowParamW         VSER32           0041C041         CreateDialogParamW         VSER32           0041C042         GetClastameW         VSER32           0041C043         CreateDialogParamW         VSER32           0041C044         GetClastameW         VSER32           0041C045         SerTocLor         Get32           0041C054         SerTocLor         Get32           0041C055</td> <td>sub_419432</td> <td>00410</td> <td>2008</td> <td></td> <td></td> <td></td> <td>KERNEL32</td> <td></td> <td></td> <td></td> <td></td>	0041C010         GetModuleHandleW         KERNEL32           0041C014         GetLocalInfoW         KERNEL32           0041C018         GetLocalInfoW         KERNEL32           0041C010         FormatMessageW         KERNEL32           0041C012         FormatMessageW         KERNEL32           0041C020         GetLastError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         KERNEL32           0041C020         GetDatError         VSER32           0041C020         GetMolatem         VSER32           0041C021         GetKeyNameTextW         VSER32           0041C033         GetMolatemTextW         VSER32           0041C040         DialogBowParamW         VSER32           0041C041         CreateDialogParamW         VSER32           0041C042         GetClastameW         VSER32           0041C043         CreateDialogParamW         VSER32           0041C044         GetClastameW         VSER32           0041C045         SerTocLor         Get32           0041C054         SerTocLor         Get32           0041C055	sub_419432	00410	2008				KERNEL32				
NDL_41ABAB         III OUT(014)         GetLocalInfoW         KENNEL32           Vub_41ABAA         III OUT(014)         GetLocalInfoW         KENNEL32           Vub_41ABAA         III OUT(016)         GetLocalInfoW         KENNEL32           Vub_41ABAA         III OUT(017)         Format/NessageW         KENNEL32           Vub_41ABAA         III OUT(016)         Format/NessageW         KENNEL32           Vub_41ABAC         III OUT(020)         GetLastError         KENNEL32           Vub_41ABAC         III OUT(020)         GetUpIgtem         USER32           Vub_41ABD2         III OUT(020)         GetUpIgtem         USER32           Vub_41ABD2         III OUT(020)         GetUpIgtemTextW         USER32           Vub_41ABD2         III OUT(020)         GetUpIgtemTextW         USER32           Vub_41ABD2         III OUT(020)         GetMessageW         USER32           Vub_41ABD4         III OUT(020)         GetMessageW         USER32           Vub_41ABD5         III OUT(04)         GetMessageW         USER32           Vub_41ABD6         III OUT(04)         GetMessageW         USER32           Vub_41ABD2         IIII OUT(04)         GetTextDevindowEW         USER32           Vub_41BD6         IIIIIIIII	0041C014         GetLc.aleInfoW         KERNEL32           0041C018         GetCommandLineA         KERNEL32           0041C010         FormatMessageW         KERNEL32           0041C012         GetLastError         KERNEL32           0041C012         GetLastError         KERNEL32           0041C020         GetLastError         KERNEL32           0041C030         GetDigItemTextW         USER32           0041C031         GetKeyNameTextW         USER32           0041C032         LondMenuW         USER32           0041C033         GetKeySageW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateWindowScW         USER32           0041C042         GetClassNameW         USER32           0041C043         CreateWindowScW         USER32           0041C044         CreateWindowScW         USER32           0041C045         SetToxUntW         USER32           004	sub_41943E	00410	200C	GetPro	ocAddress		KERNEL32				
ub_41A884         in Out1C018         GetCommandLineA         KENNEL32           ub_41A8A         in Out1C018         GetCommandLineA         KENNEL32           ub_41A8A         in Out1C0102         FormatMessageW         KENNEL32           ub_41A8C6         in Out1C020         GetLastFror         USER82           ub_41A8D2         in Out1C030         GetDlgttemTextW         USER82           ub_41A8D8         in Out1C030         GetMostemTextW         USER82           ub_41A8D8         in Out1C030         GetMostemTextW         USER82           ub_41A8D6         in Out1C030         GetMostemErextW         USER82           ub_41A8D6         in Out1C040         DialogBonParamW         USER82           ub_41A8D6         in Out1C040         CreateDialogParamW         USER82           ub_418000         in Out1C044         CreateDialogParamW         USER82           ub_418000         in Out1C054         TextOutW         USER82           ub_418000         in Out1C054	Odd1C018         GetCommandLineA         KERNEL32           00d1C010         FormatMessageW         KERNEL32           00d1C020         GetLastError         KERNEL32           00d1C020         GetLastError         KERNEL32           00d1C020         GetLastError         KERNEL32           00d1C020         GetLoffer         USER32           00d1C020         GetLofferm         USER32           00d1C030         GetLoffermTextW         USER32           00d1C031         GetKeyNameTextW         USER32           00d1C032         LadMenuW         USER32           00d1C041         CreateMessageW         USER32           00d1C042         LastMenuW         USER32           00d1C043         GetColsparamW         USER32           00d1C044         CreateWindowExW         USER32           00d1C045         GetColsparamW         USER32           00d1C045         GetColsparamW         USER32           00d1C045         SerTextColor         gdi32           00d1C055         SerTextColor         gdi32           00d1C056         SelectObject         gdi32	sub_41A89C	00410	2010	GetMo	oduleHandleW		KERNEL32				
sub_41A88A         0.041C01C         Format/MessageW         KERNEL32           sub_41A8C0         0.041C01C         Format/MessageW         KERNEL32           sub_41A8C0         0.041C020         GetLastError         KERNEL32           sub_41A8C0         0.041C020         GetLastError         KERNEL32           sub_41A8C0         0.041C020         GetLastError         USER32           sub_41A8C0         0.041C026         GetDjgtemTextW         USER32           sub_41A8D2         0.041C030         GetDjgtemTextW         USER32           sub_41A8D6         0.041C034         GetKeyNameTextW         USER32           sub_41A8F6         0.041C038         GetMessageW         USER32           sub_41A8F6         0.041C034         GetKeyNameTextW         USER32           sub_41A8F6         0.041C040         DialogBoxParamW         USER32           sub_41892         0.041C044         CreateDialogParamW         USER32           sub_41890         0.041C045         GetLestAmeW         USER32           sub_41892         0.041C045         GetLestAmeW         USER32           sub_41804         0.041C045         GetLestAmeW         USER32           sub_418104         0.041C058         SetTextColor	Odd1C01C         FormatMessageW         KERNEL32           0041C020         GetLastFror         KERNEL32           0041C020         GetLastFror         KERNEL32           0041C020         GetLastFror         KERNEL32           0041C020         GetLastFror         KERNEL32           0041C020         GetDlgItem         USER32           0041C030         GetDlgItemTextW         USER32           0041C033         GetKessageW         USER32           0041C034         CatAdvessageW         USER32           0041C03C         LaadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateVinidovEdW         USER32           0041C042         GetLastNameW         USER32           0041C043         CreateDialogParamW         USER32           0041C044         CreateDialogParamW         USER32           0041C045         TextOutW         USER32           0041C046         GetClassNameW         USER32           0041C058         SeTextColor         gdi32           0041C054         SetPoixel         gdi32           0041C056         SelectObject         gdi32	sub_41A8A8	00410	2014	GetLo	caleInfoW		KERNEL32				
sub_41A8C0         in 041 CO20         GetLastFor         KERNEL32           sub_41A8C6         in 041 CO20         GetDlgItem         USER32           sub_41A8D2         in 041 CO20         GetDlgItemTextW         USER32           sub_41A8D8         in 041 CO30         GetMeyNamEizxWW         USER32           sub_41A8D6         in 041 CO38         GetMeyNamEizxWW         USER32           sub_41A8F6         in 041 CO38         GetMeyNamEizxWW         USER32           sub_41A8F6         in 041 CO40         DialogBoxParamW         USER32           sub_41A8F6         in 041 CO44         CreateDialogParamW         USER32           sub_41800         in 041 CO44         CreateDialogParamW         USER32           sub_41802         in 041 CO454         TextOrtW         gdi32           sub_41802         in 041 CO454         SetTextColor         gdi32           sub_418124         in 041 CO55         SetTextColor         gdi32           sub_418124         in 041 CO50 <td< td=""><td>0041C020         GetLastError         KERNEL32           0041C020         BetDiglatem         USER32           0041C023         GetDiglatem         USER32           0041C024         GetDiglatemTextW         USER32           0041C033         GetKeyNameTextW         USER32           0041C034         GetKeyNameTextW         USER32           0041C035         LoadMenuW         USER32           0041C036         LoadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateWindowSW         USER32           0041C042         GetClassNameW         USER32           0041C043         GetClassNameW         USER32           0041C044         GetClassNameW         USER32           0041C054         TotOutW         USER32           0041C054         SeTiewtColor         gdi32           0041C055         SetTiextColor         gdi32           0041C056         SetEctObject         gdi32</td><td>sub_41A8B4</td><td>00410</td><td>2018</td><td>GetCo</td><td>mmandLineA</td><td></td><td>KERNEL32</td><td></td><td></td><td></td><td></td></td<>	0041C020         GetLastError         KERNEL32           0041C020         BetDiglatem         USER32           0041C023         GetDiglatem         USER32           0041C024         GetDiglatemTextW         USER32           0041C033         GetKeyNameTextW         USER32           0041C034         GetKeyNameTextW         USER32           0041C035         LoadMenuW         USER32           0041C036         LoadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C041         CreateWindowSW         USER32           0041C042         GetClassNameW         USER32           0041C043         GetClassNameW         USER32           0041C044         GetClassNameW         USER32           0041C054         TotOutW         USER32           0041C054         SeTiewtColor         gdi32           0041C055         SetTiextColor         gdi32           0041C056         SetEctObject         gdi32	sub_41A8B4	00410	2018	GetCo	mmandLineA		KERNEL32				
Sub_41A8CO         GetLastError         KERNEL32           Sub_41A8CO         GO041C028         EndDialog         USER32           Sub_41A8CC         GO041C028         EndDialog         USER32           Sub_41A8CC         GO041C028         GetDlgHemTerrW         USER32           Sub_41A8D2         GO041C030         GetDlgHemTerrW         USER32           Sub_41A8D2         GO041C034         GetKeyNamEextW         USER32           Sub_41A8D2         GO041C034         GetKeyNamEextW         USER32           Sub_41A8F6         GO041C036         CadtMeruW         USER32           Sub_41A8F6         GO041C036         CadtMeruW         USER32           Sub_41A8F6         GO041C036         CateXerNamEextW         USER32           Sub_41A962         GO041C040         DialogBoxPramW         USER32           Sub_41A902         GO041C044         CreateDialogParamW         USER32           Sub_41806C         GO041C054         TextOutW         gdi32           Sub_41806C         GO041C054         SetTextColor         gdi32           Sub_41806C         GO041C055         SetTextColor         gdi32           Sub_41806C         GO041C056         SetTextColor         gdi32           S	00041C020         GetLastError         KERNEL32           00041C020         GetLastError         USER32           00041C020         GetDlgItem         USER32           00041C020         GetDlgItemTextW         USER32           00041C030         GetDlgItemTextW         USER32           00041C031         GetKeyNameTextW         USER32           00041C033         GetKeyNameTextW         USER32           00041C034         GetKeyNameTextW         USER32           00041C035         LoadMenuW         USER32           00041C040         DialogBoxParamW         USER32           00041C041         CreateWindowEvW         USER32           00041C042         GetClassNameW         USER32           00041C043         GetClassNameW         USER32           00041C054         TotOutW         USER32           00041C054         SeTiextColor         gil32           00041C055         SetTextColor         gil32           00041C056         SetExtColor         gil32           0041C050         SelextObject         gil32	sub_41A8BA	00410	C01C	Forma	tMessageW		KERNEL32				
sub_41A8CC         0.041C02C         GetDightem         USER32           sub_41A8D2         0.041C030         GetDightemTextW         USER32           sub_41A8D2         0.041C034         GetKyMameTextW         USER32           sub_41A8D6         0.041C034         GetKyMameTextW         USER32           sub_41A8D6         0.041C038         GetKyMameTextW         USER32           sub_41A8F6         0.041C034         LadMenuW         USER32           sub_41A8F6         0.041C040         DialogBoxParamW         USER32           sub_4188F0         0.041C044         CreateVindowExW         USER32           sub_41802         0.041C044         CreateVindowExW         USER32           sub_41802         0.041C044         CreateVindowExW         USER32           sub_41802         0.041C045         GetClashameW         USER32           sub_41802         0.041C058         SetTextColor         gdi32           sub_418124         0.041C058         SetTextColor         gdi32           sub_418124         0.041C050         SelfextColor         gdi32           sub_418124         0.041C050         SelfextColor         gdi32           sub_418124         0.041C050         SelfextColor         gdi32	0041C02C         GetD/gltem         USER32           0041C030         GetD/gltemTextW         USER32           0041C034         GetD/gltemTextW         USER32           0041C034         GetMessageW         USER32           0041C034         LoadMenuW         USER32           0041C034         CetMessageW         USER32           0041C040         DialogBoxParamW         USER32           0041C044         CreateVindowExW         USER32           0041C045         GetClassNameW         USER32           0041C046         GetClassNameW         USER32           0041C054         TextOutW         USER32           0041C054         SetTextColor         gdi32           0041C055         SetTextColor         gdi32           0041C050         SelectObject         gdi32	sub_41A8C0	<b>10041</b>	2020	GetLas	stError		KERNEL32				
sib_41A8CC         GetDlgitem         USER32           sib_41A8DC         GotDlgitemTextW         USER32           sib_41A8DC         GotDlgitemTextW         USER32           sib_41A8DC         GotDlgitemTextW         USER32           sib_41A8DC         GotAlC034         GetReyNameTextW         USER32           sib_41A8DE         GotAlC038         GetReyNameTextW         USER32           sib_41A8F6         GotAlC03C         LadMeruW         USER32           sib_41A8FC         GotAlC03C         LadMeruW         USER32           sib_41A8FC         GotAlC040         DialogBorkFramW         USER32           sib_4188C         GotAlC048         CreateWindowExW         USER32           sib_4180C         GotAlC048         CreateWindowExW         USER32           sib_4180C         GotAlC048         CreateWindowExW         USER32           sib_4180C         GotAlC048         CreateWindowExW         USER32           sib_4180C         GotAlC058         SetTextColor         gdi32           sib_4181CA         GotAlC050         SetTextColor         gdi32           sib_4181CA         GotAlC060         SelectObject         gdi32           sib_418124         GotAlC060         SelectObject <td>00041C02C         GetDlgitem         USER32           00041C030         GetDlgitem TextW         USER32           00041C034         GetDlgitem TextW         USER32           00041C034         GetMessageW         USER32           00041C034         GetMessageW         USER32           00041C034         GetMessageW         USER32           00041C040         DialogBooParamW         USER32           00041C044         CreateVindowExW         USER32           00041C045         GetClassNameW         USER32           00041C046         GetClassNameW         USER32           00041C054         TextOutW         gdi32           00041C056         SelectObject         gdi32</td> <td>sub_41A8C6</td> <td>00410</td> <td>028</td> <td>EndDi</td> <td>alog</td> <td></td> <td>USER32</td> <td></td> <td></td> <td></td> <td></td>	00041C02C         GetDlgitem         USER32           00041C030         GetDlgitem TextW         USER32           00041C034         GetDlgitem TextW         USER32           00041C034         GetMessageW         USER32           00041C034         GetMessageW         USER32           00041C034         GetMessageW         USER32           00041C040         DialogBooParamW         USER32           00041C044         CreateVindowExW         USER32           00041C045         GetClassNameW         USER32           00041C046         GetClassNameW         USER32           00041C054         TextOutW         gdi32           00041C056         SelectObject         gdi32	sub_41A8C6	00410	028	EndDi	alog		USER32				
sub_41A8D8         0.041C03         Getegytamintaria         0.041C03           sub_41A8D8         0.041C034         Getegytamintaria         0.041C03           sub_41A8D6         0.041C038         GetMessageW         USER32           sub_41A8D6         0.041C03C         LoadMenuW         USER32           sub_41A8FC         0.041C04         DialogBoxParamW         USER32           sub_41A8FC         0.041C04         CreateWindowEvmW         USER32           sub_41802         0.041C048         CreateDialogParamW         USER32           sub_41804         0.041C044         GetegytamW         USER32           sub_41804         0.041C043         CreateDialogParamW         USER32           sub_41804         0.041C044         GetegytamW         USER32           sub_41804         0.041C054         GetegytamW         USER32           sub_41804         0.041C054         SetTextColor         gdi32           sub_41814         0.041C056         SetTextColor         gdi32           sub_418164         0.041C060         SelectObject         gdi32           sub_418124         0.041C060         SelectObject         gdi32           sub_418248         0.041C064         GetextMetricsW         gdi32 <td>Odd1C034         GetKeyNameTextW         USER32           Odd1C038         GetMessageW         USER32           Odd1C031         LoadMenuW         USER32           IOdd1C032         LoadMenuW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C042         GetCloskmaneW         USER32           IOdd1C054         ForteOutW         USER32           IOdd1C055         SerTextColor         gdi32           IOdd1C056         SelectObject         gdi32</td> <td>sub_41A8CC</td> <td><b>10041</b></td> <td>C02C</td> <td>GetDl</td> <td>altem</td> <td></td> <td>USER32</td> <td></td> <td></td> <td></td> <td></td>	Odd1C034         GetKeyNameTextW         USER32           Odd1C038         GetMessageW         USER32           Odd1C031         LoadMenuW         USER32           IOdd1C032         LoadMenuW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C034         CreateWindowExW         USER32           IOdd1C042         GetCloskmaneW         USER32           IOdd1C054         ForteOutW         USER32           IOdd1C055         SerTextColor         gdi32           IOdd1C056         SelectObject         gdi32	sub_41A8CC	<b>10041</b>	C02C	GetDl	altem		USER32				
Sub_41A8DE         Code (Co3         Code (Sub) function         Code (Sub) function           sub_41A8F6         C0 041 CO3         CodMerce         USER32           sub_41A8F6         C0 041 CO3         CodMerce         USER32           sub_41A8F6         C0 041 CO3         CodMerce         USER32           sub_41A8F6         C0 041 CO4         CreateDialogParamW         USER32           sub_41A902         C0 041 CO48         CreateDialogParamW         USER32           sub_41806         C0 041 CO44         CreateDialogParamW         USER32           sub_41802         C0 041 CO45         CreateDialogParamW         USER32           sub_418124         C0 041 CO54         TextOutW         gdi32           sub_418124         C0 041 CO55         SetTextColor         gdi32           sub_418124         C0 041 CO50         SelectObject         gdi32           sub_41824         C0 041 CO64         GetTextMetricsW         gdi32           sub_41824         C0 041 CO64 </td <td>0041C038         GetMessageW         USER32           0041C03C         LoadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C044         CreateWindowExW         USER32           0041C045         GreateDialogParamW         USER32           0041C046         GreateDialogParamW         USER32           0041C047         GreateDialogParamW         USER32           0041C048         FeatOutW         gdi32           0041C054         TextOutW         gdi32           0041C054         SetTextColor         gdi32           0041C050         SelectObject         gdi32</td> <td>sub_41A8D2</td> <td><b>21</b> 00410</td> <td>030</td> <td>GetDl</td> <td>altemTextW</td> <td></td> <td>USER32</td> <td></td> <td></td> <td></td> <td></td>	0041C038         GetMessageW         USER32           0041C03C         LoadMenuW         USER32           0041C040         DialogBoxParamW         USER32           0041C044         CreateWindowExW         USER32           0041C045         GreateDialogParamW         USER32           0041C046         GreateDialogParamW         USER32           0041C047         GreateDialogParamW         USER32           0041C048         FeatOutW         gdi32           0041C054         TextOutW         gdi32           0041C054         SetTextColor         gdi32           0041C050         SelectObject         gdi32	sub_41A8D2	<b>21</b> 00410	030	GetDl	altemTextW		USER32				
sub_41A8F6         in 041(C03C         LoadMeruW         USER32           sub_41A8FC         in 041(C04C)         DialogBoxParamW         USER32           sub_41A9D2         in 041(C04C)         CreateMindowExW         USER32           sub_41800         in 041(C04C)         CreateMindowExW         USER32           sub_4180C         in 041(C04C)         CreateMindowExW         USER32           sub_4180C         in 041(C054         TextOutW         gdl32           sub_41812A         in 041(C05C)         SetFextColor         gdl32           sub_41812A         in 041(C060)         SelectObject         gdl32           sub_41812B         in 041(C060)         SelectObject         gdl32           sub_41824B         in 0404(C064)         GetTextMetricsW         gdl32	J0041C03C         LoadMenuW         USER32           10041C04D         DialogBoxParamW         USER32           10041C04A         CreateWindowEwW         USER32           10041C04B         CreateVindowEwW         USER32           10041C04C         GetClassNameW         USER32           10041C04C         GetClassNameW         USER32           10041C05A         TextOutW         gil32           10041C05C         SetTextColor         gdi32           10041C05C         SetPixel         gdi32	sub_41A8D8	<b>10041</b>	2034	GetKe	yNameTextW		USER32				
sub_11A8FC         GOATCOM         DialogBoxParamW         USER32           sub_11A902         GOATCOM         CreateWindowEvW         USER32           sub_11A902         GOATCOM         CreateWindowEvW         USER32           sub_11B0AC         GOATCOM         GetateDialogParamW         USER32           sub_11B0AC         GOATCOM         GetClasMameW         USER32           sub_11B0AC         GOATCOM         GetClasMameW         USER32           sub_11B0AC         GOATCOSA         SetTextColor         gdi32           sub_11B1AC         GOATCOSA         SetTextColor         gdi32           sub_11B1A         GOATCOSO         SetTextColor         gdi32           sub_11B1A         GOATCOSO         SetTextColor         gdi32           sub_11B1A         GOATCOSO         SetTextColor         gdi32           sub_11B1A         GOATCOSO         SetCODject         gdi32           sub_11B2A         GOATCOSO         SetCODject         gdi32           sub_1182A         GOATCOSO         SetCODject         gdi32           sub_1182A         GOATCOSO         SetCODject         gdi32 <td>0041C040         DialogBoxParamW         USER32           10041C044         CreateWindowExW         USER32           10041C048         CreateWindowExW         USER32           10041C044         CreateWindowExW         USER32           10041C045         GetClassNameW         USER32           10041C054         TextOutW         gdi32           10041C055         SetTextColor         gdi32           10041C056         SelectObject         gdi32</td> <td>sub_41A8DE</td> <td><b>10041</b></td> <td>2038</td> <td>GetMe</td> <td>essageW</td> <td></td> <td>USER32</td> <td></td> <td></td> <td></td> <td></td>	0041C040         DialogBoxParamW         USER32           10041C044         CreateWindowExW         USER32           10041C048         CreateWindowExW         USER32           10041C044         CreateWindowExW         USER32           10041C045         GetClassNameW         USER32           10041C054         TextOutW         gdi32           10041C055         SetTextColor         gdi32           10041C056         SelectObject         gdi32	sub_41A8DE	<b>10041</b>	2038	GetMe	essageW		USER32				
sub_41A902         in Ox1CO4         CreateDialogParaMW         USER32           sub_41B00         in Ox1CO43         CreateDialogParaWW         USER32           sub_41B0AC         in Ox1CO43         CreateDialogParaWW         USER32           sub_41B0AC         in Ox1CO44         CerateDialogParaWW         USER32           sub_41B0AC         in Ox1CO45         CerateDialogParaWW         USER32           sub_41B1CC         in Ox1CO45         SetTextColor         gdi32           sub_41B1CC         in Ox1CO5C         SetTextColor         gdi32           sub_41B1E8         in Ox1CO5C         SetTextColor         gdi32           sub_41B1E8         in Ox1CO5C         SetTextColor         gdi32           sub_41B24         in Ox1CO5C         SetTextColor         gdi32           sub_41B24         in Ox1CO5C         SetTextColor         gdi32	0041C044         CreateWindowExW         USER32           0041C048         CreateDialogParamW         USER32           0041C04C         GetClassNameW         USER32           0041C045         TextOutW         gdi32           0041C054         TextOutW         gdi32           0041C055         SetTextColor         gdi32           0041C056         SelectObject         gdi32	sub_41A8F6	00410	C03C	LoadM	1enuW						
sub_41800         10 041 C048         CreateDialogParamW         USER32           sub_4180AC         10 041 C048         CreateDialogParamW         USER32           sub_4181AC         10 041 C044         CreateDialogParamW         USER32           sub_4181AC         10 041 C054         TextOutW         gdi32           sub_41812A         10 041 C058         SetFertColor         gdi32           sub_4181E6         10 041 C060         SelectObject         gdi32           sub_41812A         10 041 C060         SelectObject         gdi32           sub_4182A         10 041 C064         GetTextMetricsW         gdi32	0041C048         CreateDialogParamW         USER32           0041C04C         GetClassNameW         USER32           0041C054         ToxtOutW         gdi32           0041C058         SerTextColor         gdi32           0041C05C         SetPixel         gdi32           0041C050         SelectObject         gdi32		<b>100410</b>	2040	Dialog	BoxParamW		USER32				
sub_4180AC         GetLastBy meW         USER32           sub_4180AC         GetLastBy meW         USER32           sub_4180C         GetLastBy meW         gdi32           sub_41812         GotAlCOSE         SetTextColor         gdi32           sub_41812         GotAlCOSE         SetTextColor         gdi32           sub_41812         GotAlCOSE         SetTextColor         gdi32           sub_41812         GotAlCOSE         SetTextColor         gdi32           sub_418124         GotAlCOSE         SetTextColor         gdi32           sub_418248         GotAlCOGE         SelectObject         gdi32           sub_418244         GotAlCOGE         SelectObject         gdi32           sub_418244         GotAlCOGE         SelectObject         gdi32	Odd1C04C         GetClassNameW         USER32           0041C054         TextOutW         gdi32           0041C058         SetTextColor         gdi32           0041C050         SetTextColor         gdi32           0041C050         SetTextColor         gdi32           0041C050         SeletObject         gdi32		00410	2044	Create	WindowExW		USER32				
Sub_4180EC         Odd1C054         TextOutW         gd132           Sub_418124         G1 0041C058         SetTextColor         gd132           Sub_41812C         G1 0041C05C         SetTextColor         gd132           Sub_41812C         G1 0041C05C         SetTextColor         gd132           Sub_418126         G1 0041C05C         SetPriel         gd132           Sub_418126         G1 0041C060         SeloctObject         gd132           Sub_418248         G1 0041C064         GetTextMetricsW         gd132           Sub_4182D4         G1 0041C064         GetTextMetricsW         gd132	0041C054         TextOurtW         gdi32           10041C058         SetTextColor         gdi32           10041C05C         SetTextColor         gdi32           0041C050         SelectObject         gdi32           0041C050         SelectObject         gdi32	sub_41B000	<b>100410</b>	2048	Create	DialogParamW		USER32				
sub_418124         Covincion         guiz           sub_418124         ClovinCloss         SetTextColor         gdi32           sub_41816C         ClovinClose         SetTextColor         gdi32           sub_41816C         ClovinClose         SetTextColor         gdi32           sub_41816C         ClovinClose         SetTextColor         gdi32           sub_418248         ClovinClose         SetClobject         gdi32           sub_418204         GlovinClose         gdi32	0041C058         SetTextColor         gdi32           0041C05C         SetPixel         gdi32           0041C060         SelectObject         gdi32	sub_41B0AC	00410	C04C	GetCla	issNameW		USER32				
sub_4181CC         Gold CoSc         SetMedia         gdi32           sub_4181CC         Gold COSC         SetPice         gdi32           sub_4181C8         Gold COSO         SelectObject         gdi32           sub_418248         Gold CoSC         GetTextMetricsW         gdi32           sub_418204         GetTextMetricsW         gdi32	0041C05C SetPixel gdi32 10041C060 SelectObject gdi32		00410	2054	TextO	utW		gdi32				
sub_418204 gdi32 sub_418204 gdi32 sub_418204 gdi32 sub_418204	0041C060 SelectObject gdi32		00410	2058	SetTex	tColor		gdi32				
sub_418248 gdi32 sub_4182D4 gdi32			00410	C05C	SetPix	el		gdi32				
sub_4182D4 going	0041C064 GetTextMetricsW gdi32		00410	2060	Select	Object		gdi32				
			<b>10041</b>	2064	GetTex	dtMetricsW		gdi32				
sub 4182F4												
		sub_41B2E4										
sub_4182F4 sub_418348												

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 <u>HashDB</u> on IDA.

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

CPU Log Notes • Breakpoints • Memory Map	Support of the second seco
Base   Module	Party Path Addre Type Ordir Symbol
71AAO(userenv.dl) 71AAO(userenv.dl) 72090(comctl32.dl) 72090(comctl32.dl) 72260(uxtheme.dl) 72260(upofapi.dl) 72480(upofapi.dl) 72480(upofapi.dl) 72480(upofapi.dl) 72490(d) 73490(c) 73490(c) 73490(c) 73490(c) 73490(c) 75390(c) 75390(c) 75390(c) 75390(c) 7580(c)	SysterC:\windows\sysWWWG4\userenv.dll7697ptExp01BCryptAddContextFunctionSysterC:\windows\winSxS\x86_microsoft.window7697ptExp01BCryptAddContextFunctionProviSysterC:\windows\vinSxS\x86_microsoft.window7697ptExp01BCryptCloseAlgorithmProviderSysterC:\windows\vinSxS\x86_microsoft.window7697ptExp01BCryptCloseAlgorithmProviderSysterC:\windows\vinSxS\x86_microsoft.window7697ptExp01BCryptConfigureContextFunctionSysterC:\windows\sysWWG4\urportari.dll7697ptExp01BCryptConfigureContextFunctionSysterC:\windows\sysWWG4\urportari.dll7697ptExp01BCryptCreateMultHashSysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptDeriveKeySysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptEnumAlgorithmsSysterC:\windows\sysWWG4\urportari.dll7697ftExp01BCryptEnumAlgorithmsSysterC:\windows

minfinitum IT

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 authorities

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.

	00409C	8835 4C714200	mov esi, dword ptr ds: [42714C]	0042714C:&L"vss'
	00409C	FF75 08	push dword ptr ss:[ebp+8]	00+271+C.GE V33
	00409d	FF15 54744200		
	00409d	83C4 04	add esp.4	
	00409d	56	push esi	
	00409C	FF75 08	push dword ptr ss:[ebp+8]	
	00409C	FF15 44744200		
	00409C	83C4 08	add esp.8	
		850	test eax.eax	
	00409C	✓ 74 09	je {04830965-76e6-6a9a-8ee1-6af7499c1d08}.409CB6	
	004090		mov dword ptr ss:[ebp-4],1	
		✓ EB 18	jmp {04830965-76e6-6a9a-8ee1-6af7499c1d08}.409CCE	
	004090	56	push esi	
	00409C	FF15 38744200		
	00409d	83C4 04	add esp,4	
	00409d	8D7446 02	<pre>lea esi,dword ptr ds:[esi+eax*2+2]</pre>	
	00409d	66:833E 00	cmp word ptr ds:[esi],0	
		✓ 75 02	jne {04830965-76e6-6a9a-8ee1-6af7499c1d08}.409CCC	
	00409d	EB 02	jmp {04830965-76e6-6a9a-8ee1-6af7499c1d08}.409CCE	
	00409c	EB CE	jmp {04830965-76e6-6a9a-8ee1-6af7499c1d08}.409C9C	
	00409d	8B45 FC	mov eax,dword ptr ss:[ebp-4]	
•	< 100 d	r -		

esi=1

dword ptr ds:[0042714C &L"vss"]=005BAC48 L"vss"

I Dump 1	Uump 2	E Dump 3	🚛 Dump 4	🚛 Dump 5	👹 Watch 1	x=  Locals	🤌 St	truct		0515FC	
005BAC58 005BACD8	UNICODE svc\$.memta FWD.GxCVD. common-con	s.mepocs.m GxCIMgr@	nsexchange. aC:\Wir	.sophos.ve ndows\WinS	eam.backup xS\x86_mic	GXVss.G	(Blr.G)	ix -	^	0515FC 0515FC 0515FC 0515FC 0515FC	0515FE 0000000 0000000 0000000

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)

73723F	8205 0B685D00 00	add byte ptr ds: [5D680B],0	005D680B: "jbcgmz6frdhecgggadevyiwgxukksspnlidyvd7gd.onion.ly\
73723F	C182 0508695D 00	rol dword ptr ds:[edx+5D690805].0	
73723F	00D2	add dl,dl	
73723F	8205 066A5D00 00	add byte ptr ds: [5D6A06],0	
73723F	DF82 85096B5D	fild st(0), word ptr ds: [edx+5D6B0985]	
73723F	0000	add byte ptr ds:[eax].a]	
73723F	F3:8205 086C5D00 00	add byte ptr ds: [5D6C08],0	
73723F	04 83	add al.83	
73723F	8506	test dword ptr ds:[esi].eax	~ · · · · · · · · · · · · · · · · · · ·
<	0500	reese anora per astrestricax	>
byte ntr	ds: [005p680g "ibcomz6frdbe	caaaadeyyiwaxukksennlidyyd7ad onion	ly\r\nhttp://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uu
byce per	us. Loosboob Jbedinzorrane	eqquaevy maxakesspiritay var qui onton.	
		******	
🚛 Dump 1	🟭 Dump 2 🗱 Dump 3 🚛 Dump 4	🚛 Dump 5 👹 Watch 1 🛛 💷 Locals 🦻 Struct	0515FC 7747B2 return to kernelbase.
Address	ASCTT		0515FC 000000
005D66BB		ö.'a	0515FC 0515FE
005D66EB	G		0515Fd 000000
005D673B	G`(Ö 9M.é. \$.0	G`(Ö. 9M	0515Fd 000000
005D677B	Ÿ		0515Fd 000000
005D67BB	rip6xojvlohhxrwsvpzdffas5	z4pbbsywnzsbdgugd.onion.lyhttp:/	0515Fd A86FEC
		ggadevyiwgxukksspnlidyvd7gd.onion.	0515Fd 000000
005D683B	lv_http://lockbitapt6vx57t3ee	gjofwgcglmutr3a35nygvokja5uuccip4y	0515Fd 000000
005D687B	kyd onion ly http://lockbitar	t72iw55njgnqpymggskg5yp75ry7rirtdg	0515Fd 0515FF
		/lockbitaptawj16udhpd323uehekiyatj	0515Fd 000000
		lyhttp://lockbitaptbdiajqtplcrig	0515Fd 000000
00506938	zadiprwugkkut63nbyy2d5r4w2agye	kgd.onion.lyhttp://lockbitaptc2i	0515Fd 000000
		gax262kgtzjgd.onion.ly>>>> Wh	0515Fd 000000
		won't cheat you? We are the olde	0515Fd 000000
		m on the planet, nothing is more i	0515Fd 000000
		We are not a politically motivated	0515Fd 000000
		e than money. If you pay, we will	0515Fd 000000
005DGAPB	provide you with decryption so	oftware and destroy the .÷.,e	0515Fd 000000
OOSDGABB	o o o o o o o o o o o o o o o o o o o	i (ö, 9M.é \$.ÿ	0515Fd 000000
		G (Ö 9M	0515Fd 000000



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 authorities

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.

B 7bgjoZx.HL	JkNs	kOq	FP	aG	TS1FI	K.HL.	JkNs	kOq	FD	h8x	6HD	L.HL	JkNs	kOq			
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF	Decoded text
00000240	OF	CC	32	E7	3B	6B	F3	14	E8	F6	AA	Dl	03	8D	93	9F	.12ç;kó.èöªÑ"Ÿ
00000250	BB	FE	5C	3F	9A	4A	51	BD	A7	24	90	86	05	25	<b>A</b> 7	40	»þ\?šJQ∺§\$.†.%§@
00000260	7E	7E	EF	83	A4	D6	76	2D	D2	B5	73	72	7C	BO	56	B4	~~ïf¤Öv-Òµsr °V′
00000270	16	93	BO	52	E4	FO	40	8F	4D	CC	3C	8C	76	B7	92	22	."°Räð@.MÌ<Œv·/"
00000280	0E	6B	83	EO	1A	12	03	7A	8F	EA	39	EB	D5	16	50	80	.kfàz.ê9ëÕ.P€
00000290	96	CF	45	86	F6	27	61	F7	E4	4B	4E	1B	Fl	F4	0C	36	-ÏE†ö'a÷äKN.ñô.6
000002A0	65	56	A9	49	9A	D6	DF	19	73	7A	19	BD	A6	72	58	7A	eV©IšÖß.sz.½¦rXz
000002B0	96	3D	3D	4A	FE	B5	AF	00	3F	C8	BC	EC	01	37	8B	47	-==Jpµ.?È41.7 <g< td=""></g<>
000002C0	32	2E	85	C2	13	20	CO	82	DB	DD	Al	5F	D4	7C	49	4E	2Â. À,ÛÝ;_Ô IN
000002D0	34	CC	18	97	D6	74	42	CD	07	F4	8D	20	A0	_	A4		4ÌÖtBÍ.ô. »¤í
000002E0	A1	B8	9F	02	86	E4	51	71		05	D3	81	76	79	85	5E	i,Ÿ.täQqJ.Ó.vy…^
000002F0	82	DF	FE	6B	98	AC	A3	54	BO	E7	A2	Cl	3B	97	7D	7B	, Bpk~¬£T°ç¢A;-}{
00000300	F3	D3	El	A7	B2	55	E3	44		CA		OD	53	B8	50	FD	óÓá§⁼UãDŠÊ/.S.Pý
00000310	82		CC	2B	8A		<b>B</b> 3	D2	7C		E8	04	60	92	5D	98	,ZÌ+Š('Ò ]è.`']~
00000320	E7	_	9C	_	13	_	B9		-	FA		1000	4E		8E	73	ç œè²}.ú^cNùŽs
00000330	00	10	E8			9E					6C			1F		84	
00000340	58	5A	67	4F	<b>A</b> 8	77	<b>A</b> 6	CC	23	80	DE	2A			24	10	XZgO~w¦Ì#€Þ*í>\$.
00000350	09	EE	38	E0	FO	36	FO	AB	93	20	2F	12	57	EC		60	.18àð6ð«" /.WìV'
00000360	4B	B5	42	73	1A	7B	8A	B7	D4	3C	EA	29	6E		B8	62	KµBs.{Š·Ô<ê)n.,b
00000370	6C	0B	F8	83	F3	1D	DB	E3	B3	30	DA	94	DA	DO	D4	E9	1.øfó.ÛãºOÚ″ÚĐÔé
00000380	C6	31	63	D9	CD	35		AF	DD	AF	91	DO	9B	5D	6D	05	ÆlcÙÍ5z Ý 'Đ>]m.
00000390	9E	B7	1E	39	2F	30	10			80	20	7B	B5	06	F8	49	ž∙.9/0.N,€ {µ.øI
000003A0	B3	72	8E	29		3F	37	1D	AC	EO	04	OB	7E	19	F2	F6	*rŽ).?7à~.òö
000003B0	4B	10	61	DA	01							1	۸				K.aÚ.
												1	]				
									10 55	De	cry	pti	on	ID	M	ark	er

### **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 authorities

### 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 <u>Stealbit</u> (Data Exfiltration tool)
---	---



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 authorities

### **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://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://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/







Threat Spotlight: Lockbit Black 3.0 Ransomware