Understanding LockBitU

_S security.packt.com/understanding-lockbit/

June 2, 2022

A SecPro Super Issue: Understanding LockBit

For those of you in the UK, you may be winding down for the week already and ready for the Queen's Platinum Jubilee – a celebration of a monarch who has seen the world change from the low tech world of the 1950s to the technological revolution that we are living through today. In a world completely unimaginably different to those who witnessed a coronation in 1953, taking a minute to reflect on the leaps and bounds we have made as a species is something that people often forget to do.

Of course, the rise of modern computers saw another significant rise – cybercriminals. No one is more aware of the rising threat than cybersecurity professionals, so here's some light reading for the long weekend. If you're not in the UK, you can just enjoy a super issue without the special occasion.

Thanks for reading and we'll see you again on Friday!

Cheers!
Austin Miller
Editor-in-Chief

Understanding the LockBit Ransomware

By Andy Pantelli

Breaking down the Bitwise Spider APT

Looking at the origins of the Adversary, how the group evolved, and how they became one of most prolific criminal gangs using Ransomware-as-a-Service. We will take a look at the Tactics, Techniques & Procedures the adversary uses and break these down.

The origins of BitWise Spider began in September of 2019. Known then as ABCD Ransomware the gang set about promoting and supporting their operation via Russian language forums. Developing a strong professional operation until June 2021 when the group were banned from posting on Cyber Security forums. This prompted a rebrand with the group changing name to BitWise Spider and at the same time releasing LockBit 2.0 ransomware & the StealBit information stealer.

This appears to be a milestone for the group which then saw increase in their reputation and popularity amongst the Dark Web Community having matured & added much more functionality into Lockbit 2.0 Ransomware-as-a-Service (RaaS). We will take a deeper look in more detail later in the article at the TTPs (Tactics, Techniques & Procedures) used by the adversary.

Having become one of the most prolific Ransomware gangs the group looked to mature their software, and the business model. LockBit operations were by now increasing and developing the recruitment and marketing with affiliates. What exactly is an ‘affiliate’?

Ransomware-as-a-Service developers can maximize their product exposure by providing it to third parties, or 'affiliates' who in turn focus themselves on targeting victims and infecting their networks. There is a monetary trade between the developers and the affiliates for the number of infections and the numbers of users within an infected organization.

This model worked for BitWise Spider successfully allowing them to focus on development and profit, but also provides a layer between the gang and the victim making detection or prosecution of the developers more difficult with obscurity.   Affiliate schemes are used by almost all Ransomware developers who provide the affiliate with a unique identifier in specific code within the Ransomware which directs any payout to the affiliate that caused the infection.

BitWise Spider comes of age

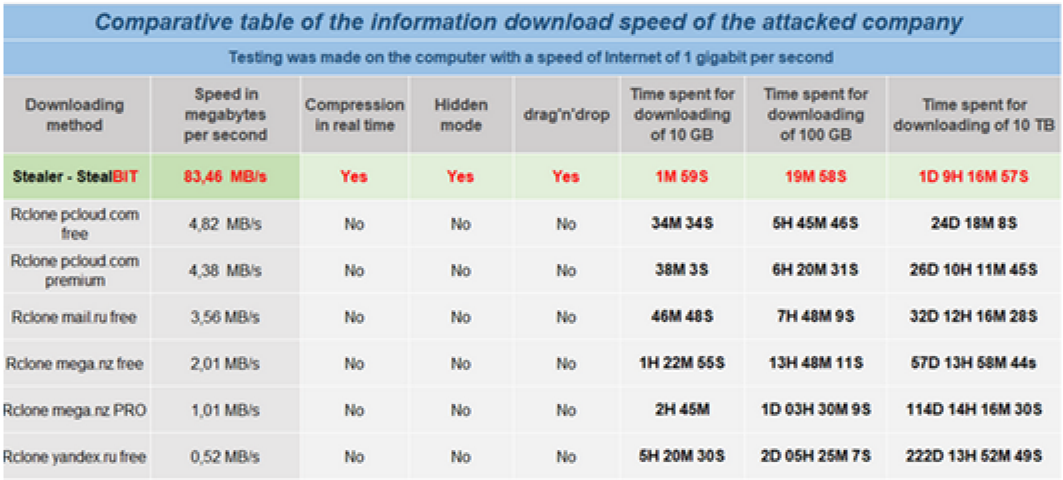
In March of 2022 the gang had matured their code, enriched features, added functionality and introduced new tactics. This included data extortion as they began to detail new victims through their Dark Web site. Using an array of techniques, tactics & procedures (TTP) the group were responsible for many high profile attacks such as the one in 2021 against Accenture, who were at the time were in the process of a marketing campaign to recruit new affiliates. The Fortune 500 Company was later to confirm the breach with a $50m ransom demanded otherwise the company data would be leaked. Accenture were soon forced to file a data breach in the October SEC filings after "extraction of proprietary information." during the August attack.

LockBit has undergone some major development releasing a new version including several new features; automatic encryption of devices across Microsoft Windows Active Directory Domains, the removal of shadow copies, self-propagation, the ability to bypass User Account Control Settings (UAC), ESXi support, and even the capability of printing Ransom notes via the victim's network connected printers. Some of the techniques seen are publicly available such as privilege escalation by using the Mimikatz tool but also the group also claim to have the fastest encryption method which employs a multithread approach using some of the following methods to boost performance:

- Open files with the FILE_FLAG_NO_BUFFERING flag, write by sector size
- Transfer work with files to Native API
- Use asynchronous file I/O
- Use I/O port completion
- Pass control to the kernel yourself, Google KiFastSystemCall

Not content with this improvement, the developers at BitWise Spider introduced StealBit to shift their tactics by employing data exfiltration as a double extortion tactic. Victims of Ransomware may not be willing to pay the fee in some instances, this could be for a number of reasons, lack of financial resources, available backups, concerns that if a payment were to be made to the blackmailers then would the data even be unencrypted? All this made criminal gangs look towards threatening victims of Ransomware that unless a payment were made to the gang then the malicious actors would release the data online or even sell it.

StealBit is developed and maintained by the group and as seen by the graphic compares favourably against other Ransomware tools:

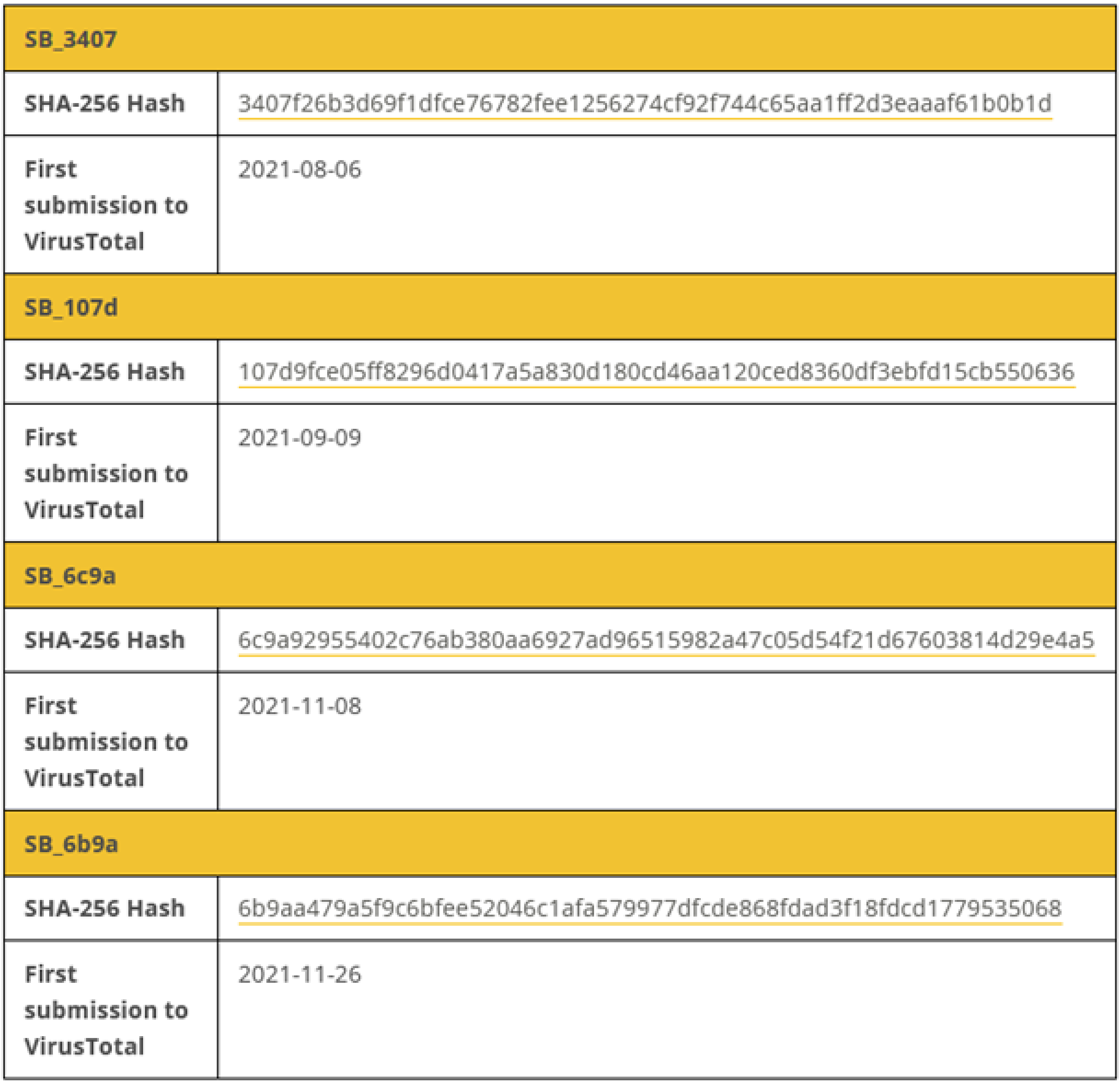


Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

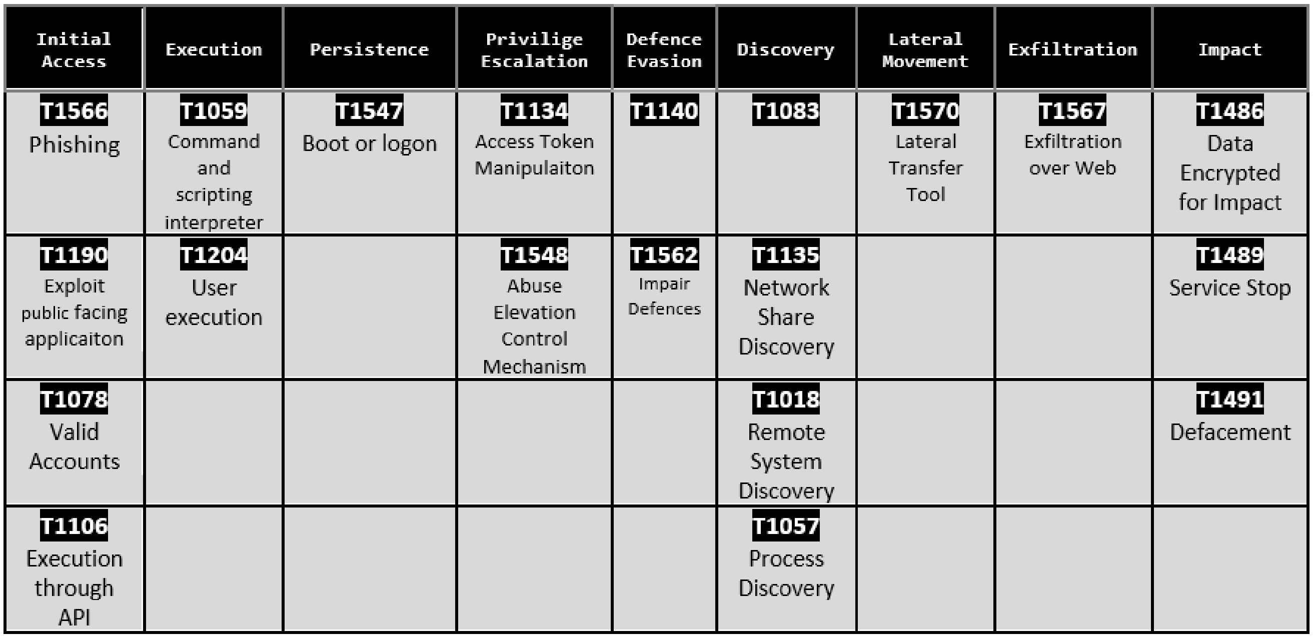
The table represents hash values of selected StealBit samples that have been observed in the security community:



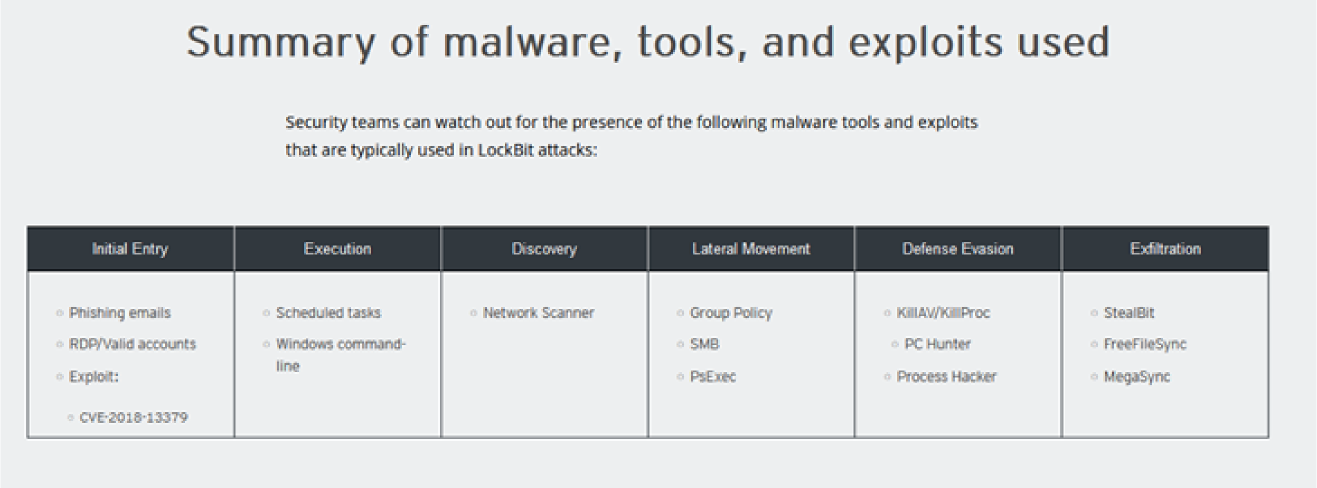
SB_3407	
SHA-256 Hash	3407f26b3d69f1dfce76782fee1256274cf92f744c65aa1ff2d3eaaaf61b0b1d
First submission to VirusTotal	2021-08-06
SB_107d	
SHA-256 Hash	107d9fce05ff8296d0417a5a830d180cd46aa120ced8360df3ebfd15cb550636
First submission to VirusTotal	2021-09-09
SB_6c9a	
SHA-256 Hash	6c9a92955402c76ab380aa6927ad96515982a47c05d54f21d67603814d29e4a5
First submission to VirusTotal	2021-11-08
SB_6b9a	
SHA-256 Hash	6b9aa479a5f9c6bfee52046c1afa579977dfcde868fdad3f18fdcd1779535068
First submission to VirusTotal	2021-11-26

MITRE ATT&CK

Tactics, techniques & procedures (TTPs) observed to be used by the adversary:



Initial Access	Execution	Persistence	Privilige Escalation	Defence Evasion	Discovery	Lateral Movement	Exfiltration	Impact
T1566 Phishing	T1059 Command and scripting interpreter	T1547 Boot or logon	T1134 Access Token Manipulaiton	T1140	T1083	T1570 Lateral Transfer Tool	T1567 Exfiltration over Web	T1486 Data Encrypted for Impact
T1190 Exploit public facing applicaiton	T1204 User execution		T1548 Abuse Elevation Control Mechanism	T1562 Impair Defences	T1135 Network Share Discovery			T1489 Service Stop
T1078 Valid Accounts					T1018 Remote System Discovery			T1491 Defacement
T1106 Execution through API					T1057 Process Discovery			



Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in LockBit attacks:

Initial Entry	Execution	Discovery	Lateral Movement	Defense Evasion	Exfiltration
○ Phishing emails ○ RDP/Valid accounts ○ Exploit: ○ CVE-2018-13379	○ Scheduled tasks ○ Windows command-line	○ Network Scanner	○ Group Policy ○ SMB ○ PsExec	○ KillAV/KillProc ○ PC Hunter ○ Process Hacker	○ StealBit ○ FreeFileSync ○ MegaSync

Industries & Countries Targeted

LockBit targets diverse industry sectors & geographical regions. Most attacks are observed in the US, India & Brazil with the Commonwealth of Independent States being avoided. Business sectors indicate the Healthcare closely followed by the Education Sector although the group have issued a statement to claim that they do not target "healthcare, charity or educational institutions". This has prompted the US Department of Health Services HHS) to issue "contradictory code of ethics" note warning the public not to rely on such statements and these are shown not be true.

Initial Access

LockBit affiliates gain access via compromised servers, or by using RDP or VPN accounts using brute force insecure credentials. A further delivery method is by exploiting Fortinet VPN CVE-2018-13379 vulnerability. LockBit also makes use of Mimikatz to escalate privileges.

Execution

Executed by command line or by scheduled tasks and can be propagated in other machines. It is also known to use PowerShell Empire post exploitation agent.

Persistence

Registry Run Keys / Start up Folders

Discovery

Advanced Port Scanner, Network Scanner & AdFind are used to enumerate connected machines.

Lateral movement

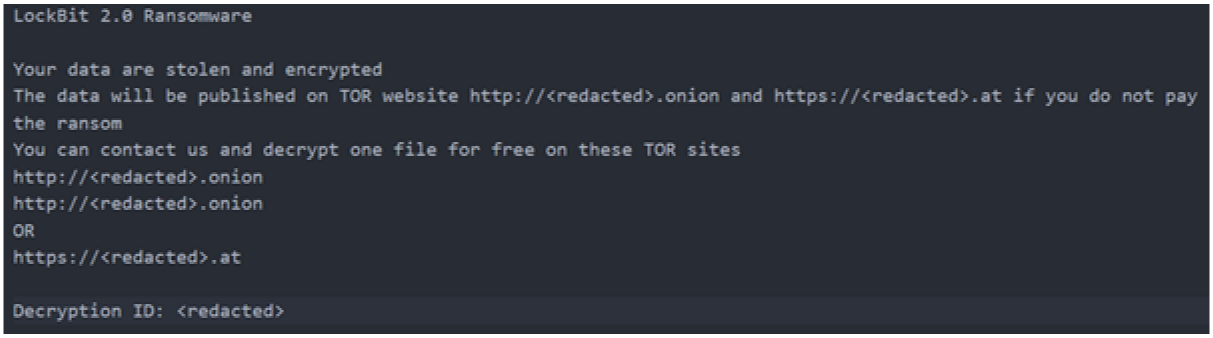
Self-Propagation via SMB using compromised credentials or Group Policy. PsExec or Cobalt Strike is used for lateral movement.

Exfiltration

Data extracted to Cloud Storage Web Applications MEGA, or FreeFileSync. Also used for exfiltration is the groups own StealBit.

Impact

Ransomware payload will encrypt victim machines upon execution. This includes local and network drives. Encrypting with AES-256. Can print ransom note using connected printers. The desktop wallpaper is also replaced.



```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR website http://<redacted>.onion and https://<redacted>.at if you do not pay
the ransom
You can contact us and decrypt one file for free on these TOR sites
http://<redacted>.onion
http://<redacted>.onion
OR
https://<redacted>.at

Decryption ID: <redacted>
```

Ransom note, file name Restore-My-Files.txt

Tactics

The use of affiliates, marketing & the gangs Direct Leak Site to upload stolen data are direct tactics to propagate the monetization. Offering Ransomware-as-a-Service provides a tactic to avoid direct involvement and obfuscate any law enforcement action.

Known target industries include and are not limited to Cryptocurrency, Academics, Aviation, Aerospace, Healthcare Insurance, Food and Beverage, Chemicals Energy Oil and Gas, Manufacturing, Hospitality, Real Estate Travel, Opportunistic, Logistics Transportation, Legal, Retail, and Government.

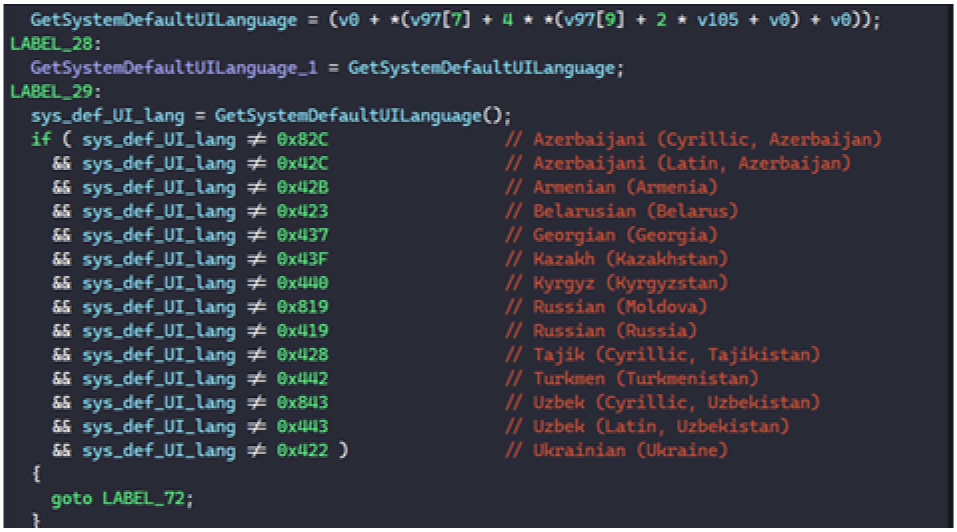
The known 74 target countries include Taiwan, China, Poland, Netherlands, Mexico, the United States, Belgium, Colombia, Denmark, Chile, Vietnam, and Peru.

The gang have developed a strong selling point with affiliates using the speed of the malware with its capabilities being well known. The group maximizes this selling point through various means of publicity. External factors influence the targeting of victims with a preference for victims that have concerns over GPDR in Europe.

Techniques

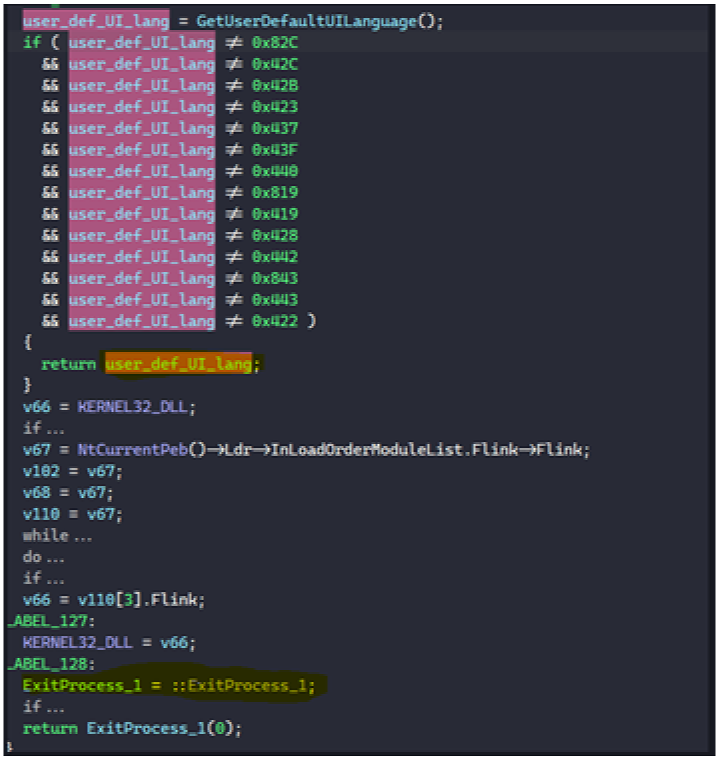
As with many Ransomware gangs LockBit will the check system language to avoid encrypting systems in Russia or other nearby CIS states The Malware issues the commands GetSystemDefaultUILanguage and GetUserDefaultUILanguage to check if the system of user default UI is in the language list to avoid.

Azerbaijani (Cyrillic, Azerbaijan), Azerbaijani (Latin, Azerbaijan), Armenian (Armenia), Belarusian (Belarus), Georgian (Georgia), Kazakh (Kazakhstan), Kyrgyz (Kyrgyzstan), Russian (Moldova), Russian (Russia), Tajik (Cyrillic, Tajikistan), Turkmen (Turkmenistan), Uzbek (Cyrillic, Uzbekistan), Uzbek (Latin, Uzbekistan), and Ukrainian (Ukraine).



```
  GetSystemDefaultUILanguage = (v0 + *(v97[7] + 4 * *(v97[9] + 2 * v105 + v0) + v0));
LABEL_28:
  GetSystemDefaultUILanguage_1 = GetSystemDefaultUILanguage;
LABEL_29:
  sys_def_UI_lang = GetSystemDefaultUILanguage();
  if ( sys_def_UI_lang ≠ 0x82C                // Azerbaijani (Cyrillic, Azerbaijan)
    && sys_def_UI_lang ≠ 0x42C                // Azerbaijani (Latin, Azerbaijan)
    && sys_def_UI_lang ≠ 0x42B                // Armenian (Armenia)
    && sys_def_UI_lang ≠ 0x423                // Belarusian (Belarus)
    && sys_def_UI_lang ≠ 0x437                // Georgian (Georgia)
    && sys_def_UI_lang ≠ 0x43F                // Kazakh (Kazakhstan)
    && sys_def_UI_lang ≠ 0x440                // Kyrgyz (Kyrgyzstan)
    && sys_def_UI_lang ≠ 0x819                // Russian (Moldova)
    && sys_def_UI_lang ≠ 0x419                // Russian (Russia)
    && sys_def_UI_lang ≠ 0x428                // Tajik (Cyrillic, Tajikistan)
    && sys_def_UI_lang ≠ 0x442                // Turkmen (Turkmenistan)
    && sys_def_UI_lang ≠ 0x843                // Uzbek (Cyrillic, Uzbekistan)
    && sys_def_UI_lang ≠ 0x443                // Uzbek (Latin, Uzbekistan)
    && sys_def_UI_lang ≠ 0x422 )              // Ukrainian (Ukraine)
  {
    goto LABEL_72;
  }
```

The malware uses and Ifstatement and calls ExitProcess to terminate itself if the user of system UI language is identified.



```
user_def_UI_lang = GetUserDefaultUILanguage();
if ( user_def_UI_lang ≠ 0x82C
  && user_def_UI_lang ≠ 0x42C
  && user_def_UI_lang ≠ 0x42B
  && user_def_UI_lang ≠ 0x423
  && user_def_UI_lang ≠ 0x437
  && user_def_UI_lang ≠ 0x43F
  && user_def_UI_lang ≠ 0x440
  && user_def_UI_lang ≠ 0x819
  && user_def_UI_lang ≠ 0x419
  && user_def_UI_lang ≠ 0x428
  && user_def_UI_lang ≠ 0x442
  && user_def_UI_lang ≠ 0x843
  && user_def_UI_lang ≠ 0x443
  && user_def_UI_lang ≠ 0x422 )
{
  return user_def_UI_lang;
}
v66 = KERNEL32_DLL;
if ...
v67 = NtCurrentPeb()->Ldr->InLoadOrderModuleList.Flink->Flink;
v102 = v67;
v68 = v67;
v110 = v67;
while ...
do ...
if ...
v66 = v110[3].Flink;
ABEL_127:
KERNEL32_DLL = v66;
ABEL_128:
ExitProcess_1 = ::ExitProcess_1;
if ...
return ExitProcess_1(0);
}
```

Strings seen in LockBit executables are encoded and then stored as a stack string. Before use they are decoded dynamically through computations such as addition, subtraction or XOR, this is the Stack String Anti-Analysis.

As with many major Ransomware variants LockBit resolves APIs dynamically to make the Inline Anti-Analysis more difficult but the gang have enhanced the technique by making the entire resolving process inline which makes the decompiled code much larger, and therefore more difficult & time consuming to analyse.

Then using methods to load the API libraries into memory, the malware uses hashing & obfuscation methods to access the DLL base and export table which returns the target API address. After loading all required libraries LockBit will restrict access to its own process by calling NTOpenProcess to get a handle on the current process then resolve GetSecurityInfo to get the process security descriptor.

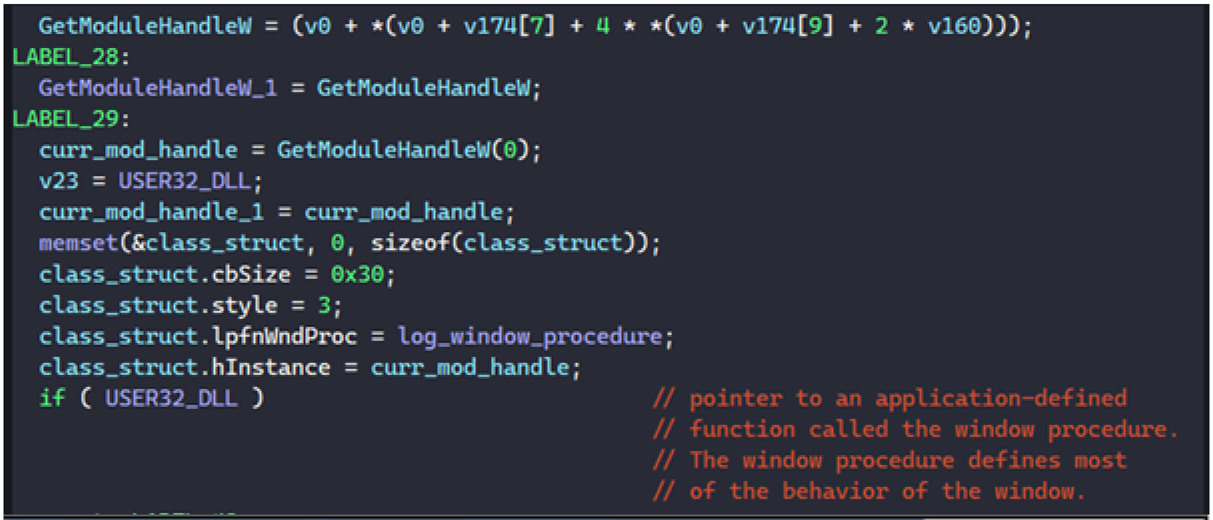
By initializing an SID for the EVERYONE group and using the RtlAddAccessDeniedAce to add the ACCESS_DENIED access control entry for the EVERYONE group the malware process is effectively protected. Additional ACEs are iterated for each process that the malware uses. Critical system messages are suppressed and calls to RtlAdjustPrivilege which enables the SE_TAKE_OWNERSHIP_PRIVILEGE.

Privilege escalation

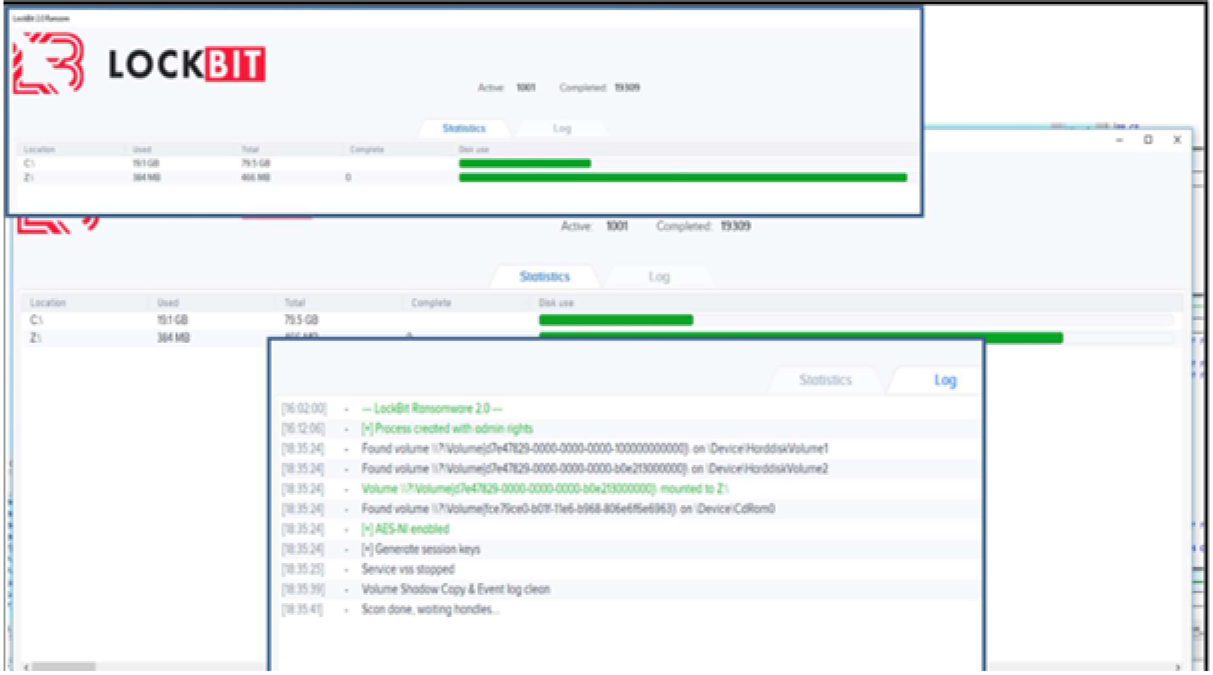
In the next stages LockBit will look to elevate privilege of the user account using the GetTokenInformation call to retrieve information about the user account associated with the Token. Using a combination retrieving and comparing account SID the malware begins the process to escalate itself.

Logging

The malware then makes a number of calls to create hidden debug windows which can be viewed during the process by a combination of hot keys Shift+F1.



```
  GetModuleHandleW = (v0 + *(v0 + v174[7] + 4 * *(v0 + v174[9] + 2 * v160)));
LABEL_28:
  GetModuleHandleW_1 = GetModuleHandleW;
LABEL_29:
  curr_mod_handle = GetModuleHandleW(0);
  v23 = USER32_DLL;
  curr_mod_handle_1 = curr_mod_handle;
  memset(&class_struct, 0, sizeof(class_struct));
  class_struct.cbSize = 0x30;
  class_struct.style = 3;
  class_struct.lpfnWndProc = log_window_procedure;
  class_struct.hInstance = curr_mod_handle;
  if ( USER32_DLL )                                 // pointer to an application-defined
                                                    // function called the window procedure.
                                                    // The window procedure defines most
                                                    // of the behavior of the window.
```



Active: 1001 Completed: 19309

```
Location    Used       Total      Complete    Disk use
C:\         15.1 GB    79.5 GB
Z:\         384 MB     466 MB     0
```

```
[16:02:00]  -  --- LockBit Ransomware 2.0 ---
[16:12:06]  -  [+] Process created with admin rights
[18:35:24]  -  Found volume \\?\Volume{d7e47829-0000-0000-0000-100000000000} on \Device\HarddiskVolume1
[18:35:24]  -  Found volume \\?\Volume{d7e47829-0000-0000-0000-b0e213000000} on \Device\HarddiskVolume2
[18:35:24]  -  Volume \\?\Volume{d7e47829-0000-0000-0000-b0e213000000} mounted to Z:\
[18:35:24]  -  Found volume \\?\Volume{fce79ce0-b01f-11e6-b968-806e6f6e6963} on \Device\CdRom0
[18:35:24]  -  [+] AES-NI enabled
[18:35:24]  -  [+] Generate session keys
[18:35:25]  -  Service vss stopped
[18:35:39]  -  Volume Shadow Copy & Event log clean
[18:35:41]  -  Scan done, waiting handles...
```

Command Line

Command-line is to be used with or without arguments. Once encryption of the target file/directory is complete the process is terminated

Mutex

LockBit checks for, and avoids multiple Ransomware instances by checking the stack string \{\%02X%02X%02X%02X-%02X%02X-%02X%02X-%02X%02X%02X%02X%02X%%02X}”

Active Directory

LockBit seeks out the OS Version, if Windows Vista or above it tries to create and set up new group policies for other hosts within Active Directory using NtQueryInformationToken_1 and the NtOpenProcessToken commands the malware looks up the Admin account and Domain. To then connect to the AD Domain LockBit will generate the LDAP display name for the Group Policy Object.

By resolving the stack string and formats it with the public key. Manually extracting the DNS Domain Name, and name LockBit is able to create a new GPO, lastly the path is built by formatting the string LDAP://CN=<GPO GUID>,CN=Policies,CN=System,DC=<Domain component 1>,DC=<Domain Component 2> which allows the AD path and GPO to call CreateGPOLink to connect the GPO to the Active Directory Domain.

DNS Retrieval

LockBit formats ScheduledTasks.xml file to execute a taskkill.exe for each process in the process list before dropping in the Registy.pol file1 which contains the following list of registry paths and values:

- Software\Policies\Microsoft\Windows Defender\DisableAntiSpyware: True
- Software\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring: True
- Software\Policies\Microsoft\Windows Defender\Spynet\SubmitSamplesConsent: Never send
- Software\Policies\Microsoft\Windows Defender\Threats\Threats_ThreatSeverityDefaultAction: Enabled
- Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction\Low: Ignored
- Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction\Medium: Ignored
- Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction\High: Ignored
- Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction\Severe: Ignored
- Software\Policies\Microsoft\Windows Defender\UX Configuration\Notification_Suppress: Enabled

These following registry configurations disable Windows Defender features such as anti-spyware, real-time protection, submitting samples to Microsoft servers, default actions, and displaying notification on all network hosts.

Persistence

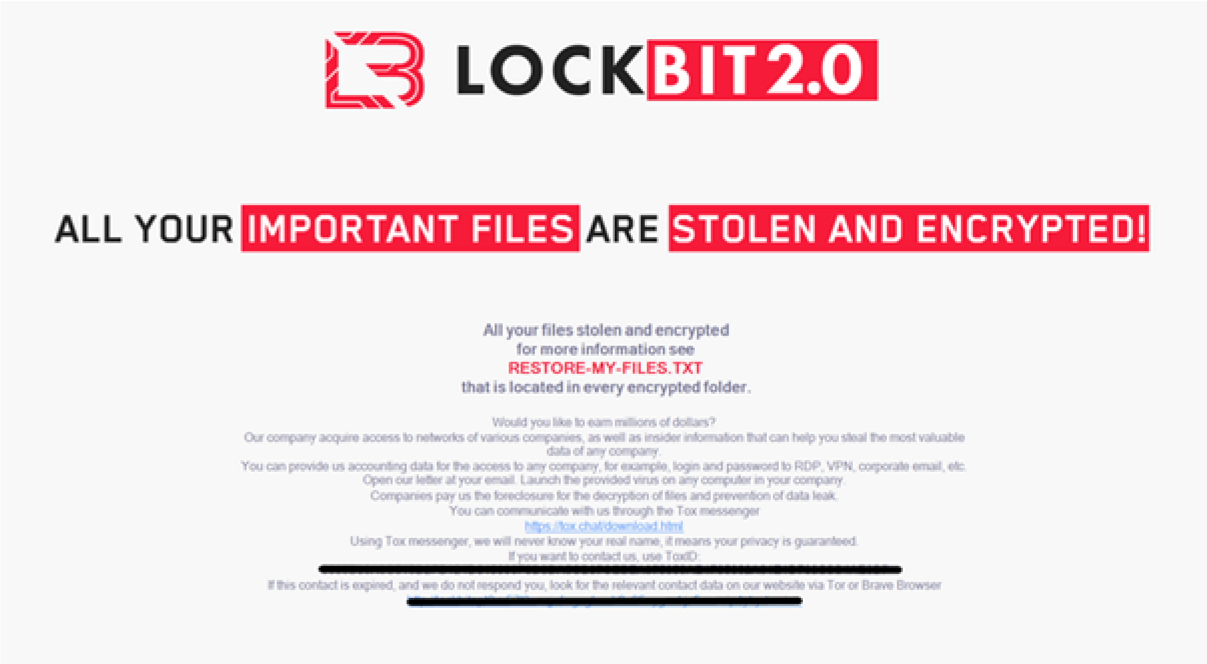
Before executing encryption routines LockBit configures persistence using Registry Keys if the Malware is interrupted by a system shutdown. Once encryption is complete, the malware will remove the persistence key calling RegDeleValueW to prevent itself from running again if the user restarts the machine following encryption.

Deleting backups

LockBit will delete shadow copies by resolving the string /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no then passes the fields to ShellExecuteA. The command uses vssadmin and wmic to delete all shadow copies and bcdedit to disable file recovery.

Wallpaper

Setting the default file extension, desktop background and ransom note printing tasks are completed.



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[redacted]

Printing

Using the call EnumPrintersW to retrieve printers' information. The internal function resolves two strings Microsoft Print to PDF and Microsoft XPS Document Writer to compare the printer name. If the value is one of the two, the function will exit and the ransom note will not be printed.

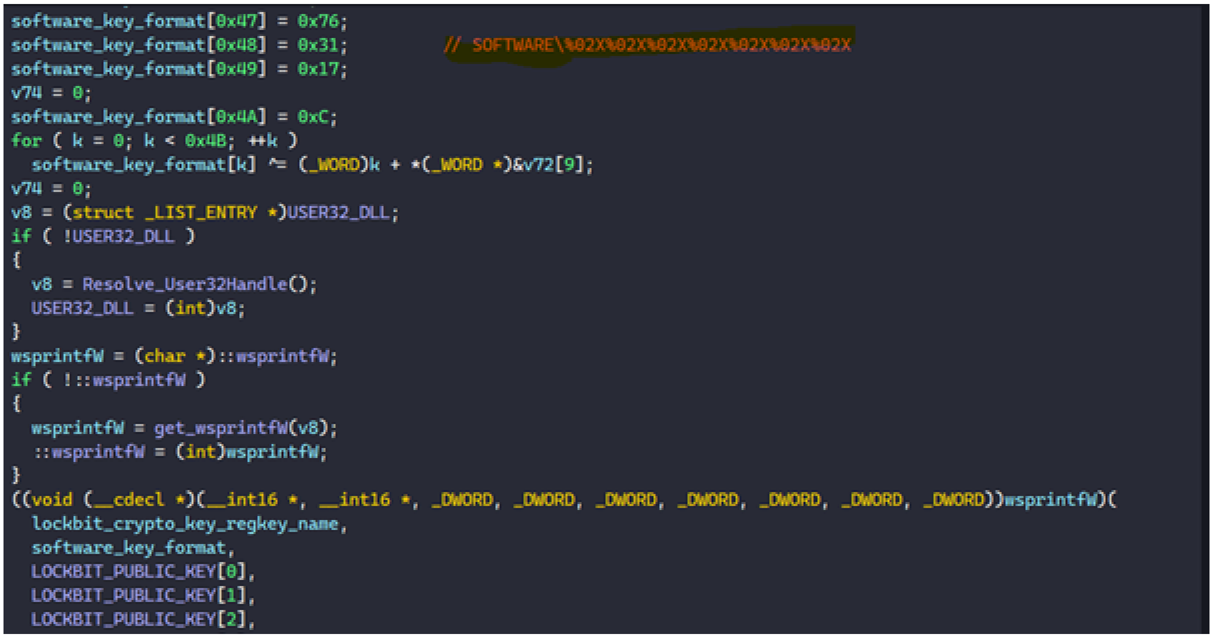
This is to ensure that the note is not printed to a file and only to print from a physical printer.

Extension

All files encrypted by LockBit have the file extinction .lockbit after calling NtCreateFile and NtWriteFile resolves \Registry\Machine\Software\Classes\.lockbit stack string and calls NTCreateKey to create the registry extension, this is done after formatting using its public key.

File Encryption

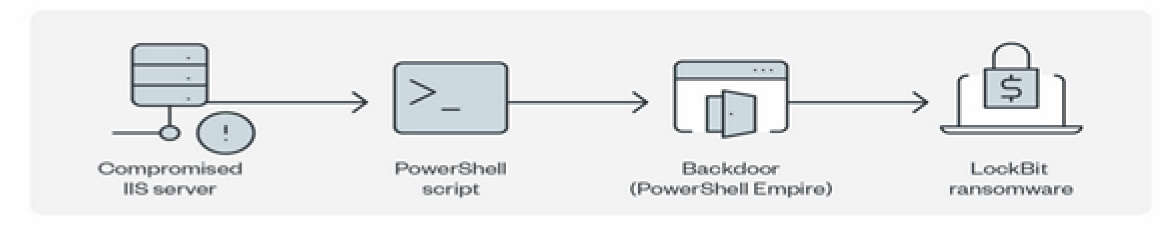
Prior to encryption LockBit will enumerate all volumes on the target system using FindFirstVolumeW and FindNextVolumeW and proceeds to retrieve a list of Drive letters and any mounted folder paths. Then each drive path is iterated from Z to A before being mounted to a specific drive letter by calling SetVolumeMountPointW. Libsodium Cryptography is used for the public key crypto using functions bcrypt.dll and LoadLibraryA, it will use BCryptGenRandom for the RNG function or CryptGenRandom. Next, as seen before the stack string is resolved and the public key is used to format it which is later used as a Registry key to store the victim crypto keys. The malware calls Libsodium crypto_box_keypair to generate a random 32-bit private key and the corresponding public key. Next it will encrypt the 64-bit buffer containing both keys using Libsodium crypto_box_easy then deletes the victims private key from memory.

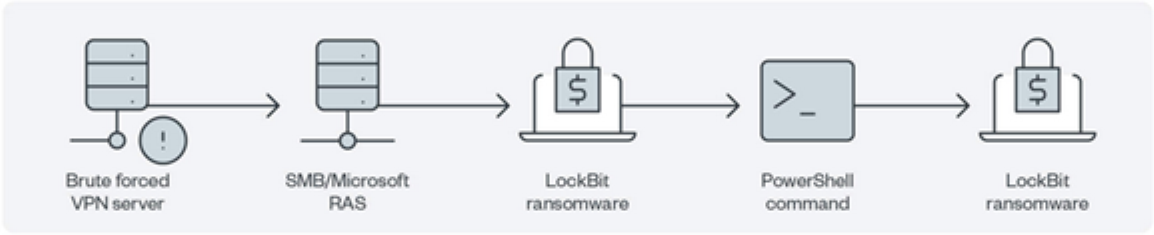


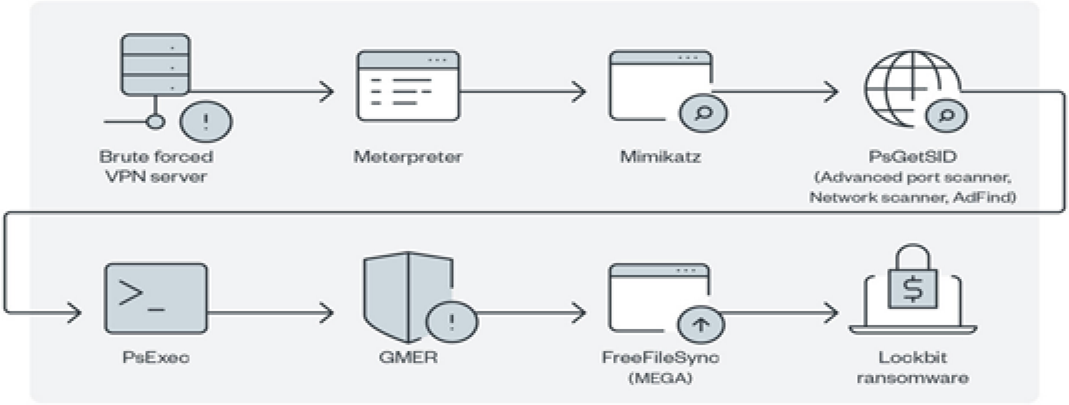
```
software_key_format[0x47] = 0x76;
software_key_format[0x48] = 0x31;          // SOFTWARE\%02X%02X%02X%02X%02X%02X%02X
software_key_format[0x49] = 0x17;
v74 = 0;
software_key_format[0x4A] = 0xC;
for ( k = 0; k < 0x4B; ++k )
  software_key_format[k] ^= (_WORD)k + *(_WORD *)&v72[9];
v74 = 0;
v8 = (struct _LIST_ENTRY *)USER32_DLL;
if ( !USER32_DLL )
{
  v8 = Resolve_User32Handle();
  USER32_DLL = (int)v8;
}
wsprintfW = (char *)::wsprintfW;
if ( !::wsprintfW )
{
  wsprintfW = get_wsprintfW(v8);
  ::wsprintfW = (int)wsprintfW;
}
((void (__cdecl *)(__int16 *, __int16 *, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))wsprintfW)(
  lockbit_crypto_key_regkey_name,
  software_key_format,
  LOCKBIT_PUBLIC_KEY[0],
  LOCKBIT_PUBLIC_KEY[1],
  LOCKBIT_PUBLIC_KEY[2],
```

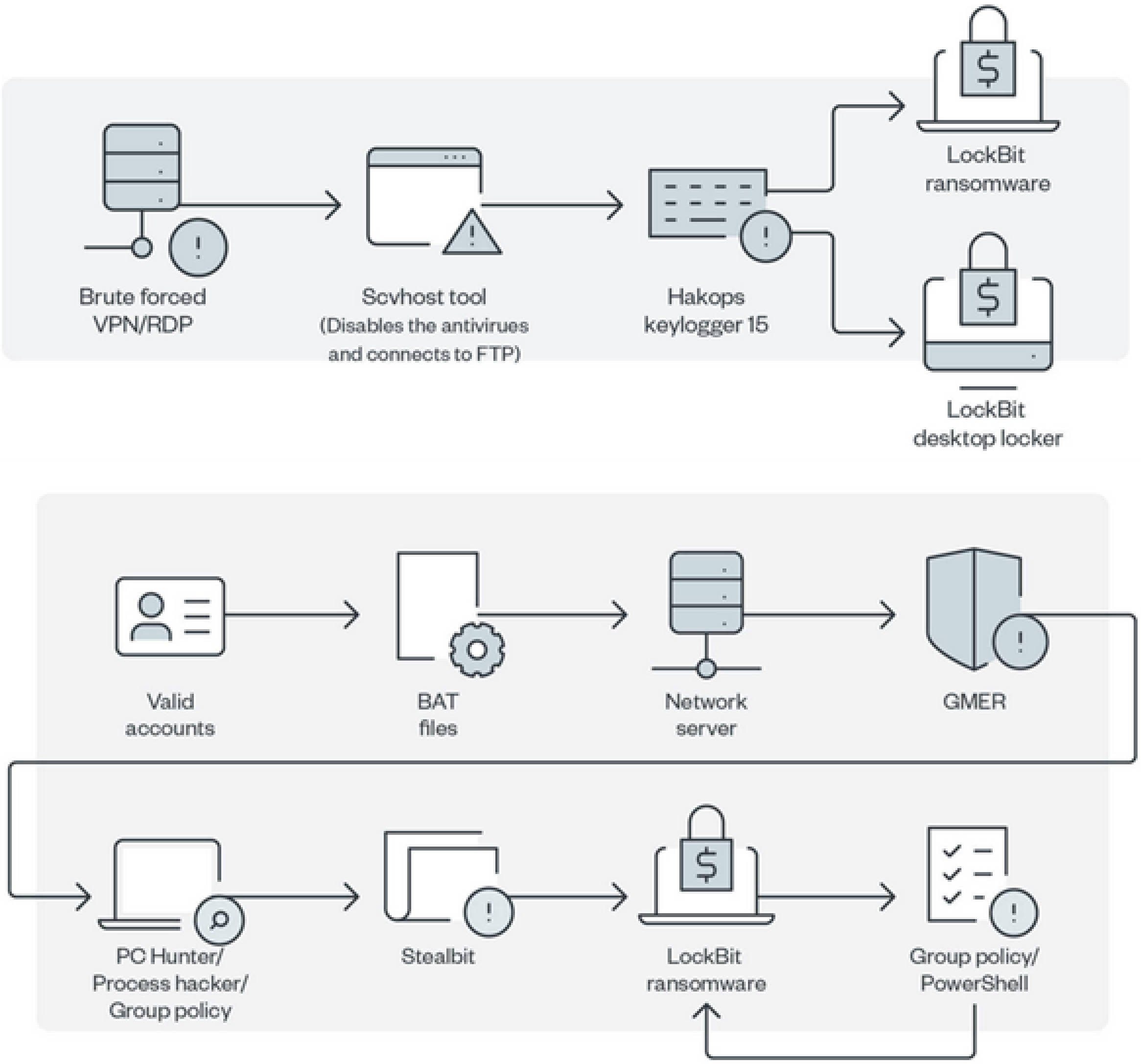
After setting up the crypto keys, LockBit initialises its multithreading method we reference earlier it then traverses through all local drives using techniques to skip drives that are not available, or that have already been encrypted. Files that are recognised as read-only changes the attribute to FILE_ATTRIBUTE_NORMAL making it writable and available for encryption. The files are encrypted using 512 byte chunks and given the extension .lockbit Again calling the RNG function the malware randomly generates a 16-byte AES key and 16-byte AES IV and writes into the file structure before renaming the file before the encryption by populating a FILE_NAME_INFORMATION with the encrypted file name before calling NTSetInformationFile with the information class FileNameInformation. In the final stages LockBit will create threads to traverse and encrypt other network hosts and network drives by using the GetAdaptorInfo the inet_addr call is made to convert the system IP address and mask. Once the broadcast domain is identified LockBit will scan the network iterating from the network ID address and incrementing up to the broadcast address trying to connect over ports 135 or 445, if successful it will try to encrypt the network hosts.

Procedures









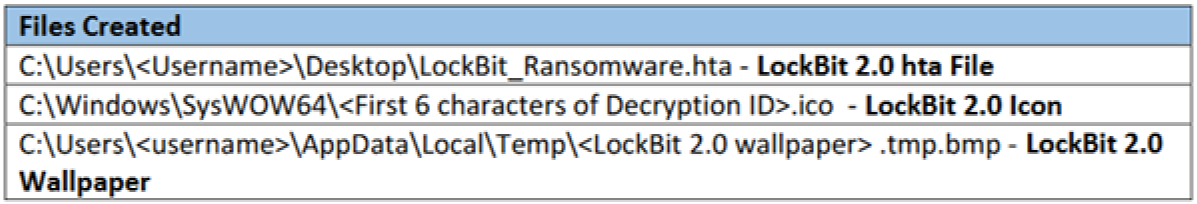
Indicators of Compromise

Command Line Activity:

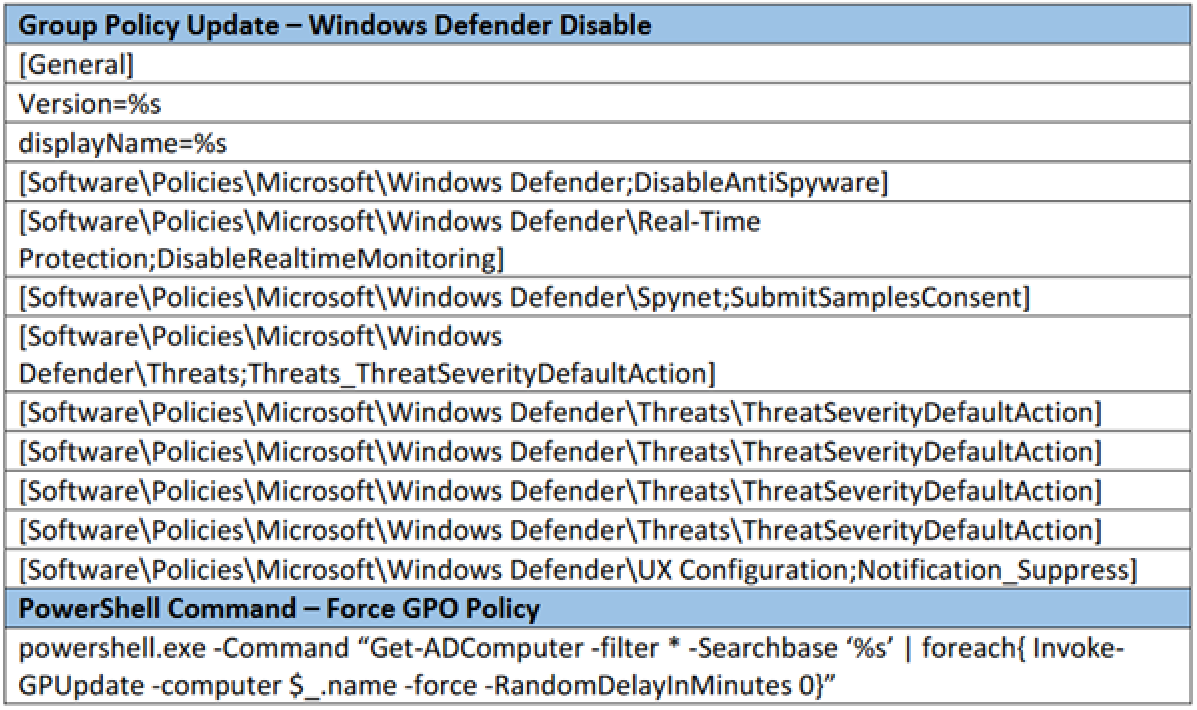
The activity below provides a listing of all observed command line activity during execution:

Recorded Commands
cmd.exe /c vssadmin Delete Shadows /All /Quiet *Description: Deletes Shadow Copies*
cmd.exe /c bcdedit /set {default} recoveryenabled No *Description: Disables Win 10 recovery*
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures *Description: Ignore boot failures*
cmd.exe /c wmic SHADOWCOPY /nointeractive *Description: This command has an invalid syntax and errors out*
cmd.exe /c wevtutil cl security *Description: Deletes security log*
cmd.exe /c wevtutil cl system *Description: Deletes system log*

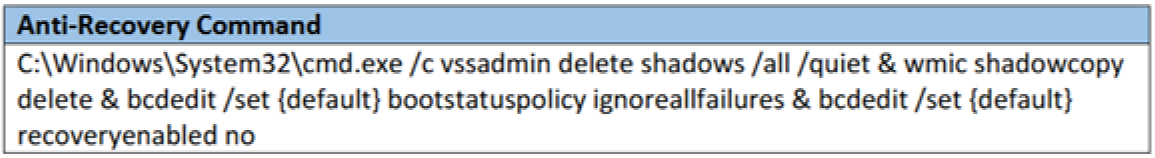
Registry Keys
Created - UAC Bypass
Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
Value: Display Calibrator
Data: <LockBit 2.0 Ransomware path>
Created - LockBit 2.0 Wallpaper Change
Key: HKEY_CLASSES_ROOT\Lockbit\shell\Open\Command
Data: "C:\Windows\system32\mshta.exe" "C:\Users\<username>\Desktop\LockBit_Ransomware.hta"
Key: HKEY_CLASSES_ROOT\Lockbit\DefaultIcon
Data: C:\Windows\<First 6 characters of LockBit 2.0 Decryption ID>.ico
Created - Persistence
Key: HKEY_CURENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{GUID}
Data: C:\Users\<Username>\Desktop\LockBit_Ransomware.hta
Data: <LockBit 2.0 Ransomware path>
Created - Encryption
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Private
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Public
Created - LockBit 2.0 Icon Location
Key: HKEY_LOCAL_MACHINE\Software\Classes\.lockbit\DefaultIcon
Created / Modified - LockBit 2.0 Desktop
KEY: HKEY_CURRENT_USER\Control Panel\Desktop
String Value: %APPDATA%\Local\Temp\<LockBit 2.0 wallpaper>.tmp.bmp
String Value: TitleWallpaper=0
String Value: WallpaperStyle = 2



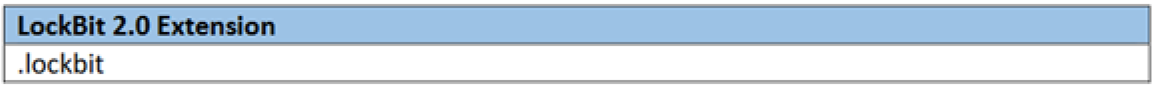
Files Created
C:\Users\<Username>\Desktop\LockBit_Ransomware.hta - **LockBit 2.0 hta File**
C:\Windows\SysWOW64\<First 6 characters of Decryption ID>.ico - **LockBit 2.0 Icon**
C:\Users\<username>\AppData\Local\Temp\<LockBit 2.0 wallpaper> .tmp.bmp - **LockBit 2.0 Wallpaper**



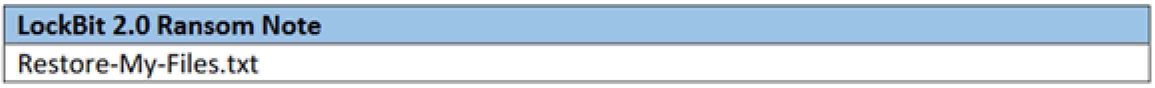
Group Policy Update – Windows Defender Disable
[General]
Version=%s
displayName=%s
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[Software\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\UX Configuration;Notification_Suppress]
PowerShell Command – Force GPO Policy
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"



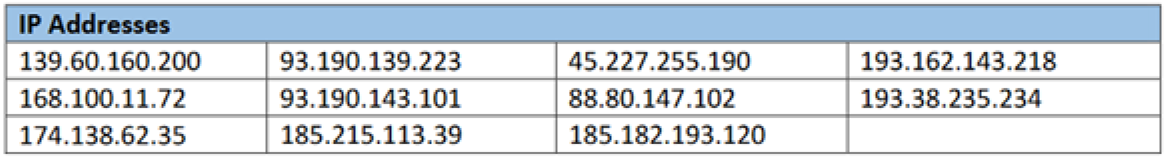
Anti-Recovery Command
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no



LockBit 2.0 Extension
.lockbit



LockBit 2.0 Ransom Note
Restore-My-Files.txt



IP Addresses			
139.60.160.200	93.190.139.223	45.227.255.190	193.162.143.218
168.100.11.72	93.190.143.101	88.80.147.102	193.38.235.234
174.138.62.35	185.215.113.39	185.182.193.120	

Further reading

Want to find out more about LockBit? Check out these links.