Uncovering LockBit Black's Attack Chain and Anti-forensic activity

seqrite.com/blog/uncovering-lockbit-blacks-attack-chain-and-anti-forensic-activity/

Sathwik Ram Prakki February 1, 2023

01 February 2023

Written by Sathwik Ram Prakki

Ransomware

Estimated reading time: 6 minutes

Since the infamous Conti ransomware group disbanded due to source code leaks during the Russia-Ukraine war, the LockBit group has claimed dominance. The group has adopted new extortion techniques and added a first-of-its-kind bug-bounty program, along with many features, to advance their new leak site. Upon investigation and analysis, we have determined that the new LockBit 3.0 variant has a high infection vector and attack chain exhibiting substantial anti-forensic activity.

Attack Overview

LockBit's new Black variant showed anti-forensic activities which cleared event logs, killed multiple tasks, and deleted services simultaneously. It obtains initial access to the victim's network via SMB brute forcing from various IPs.

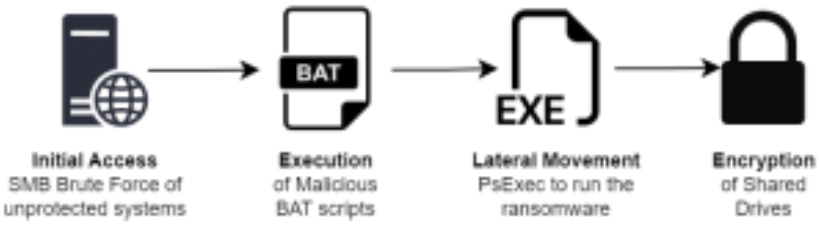


Fig. 1 – Attack Chain

The sys-internal tool PSEXEC is used to execute malicious BAT files on a single system which were later cleaned off. These files indicate activity related to modifying RDP & authentication settings while disabling antivirus at the same time:

- C:\Windows\system32\cmd.exe /c “”openrdp.bat” “
- C:\Windows\system32\cmd.exe /c “”mimon.bat” “
- C:\Windows\system32\cmd.exe /c “”auth.bat” “
- C:\Windows\system32\cmd.exe /c “”turnoff.bat” “

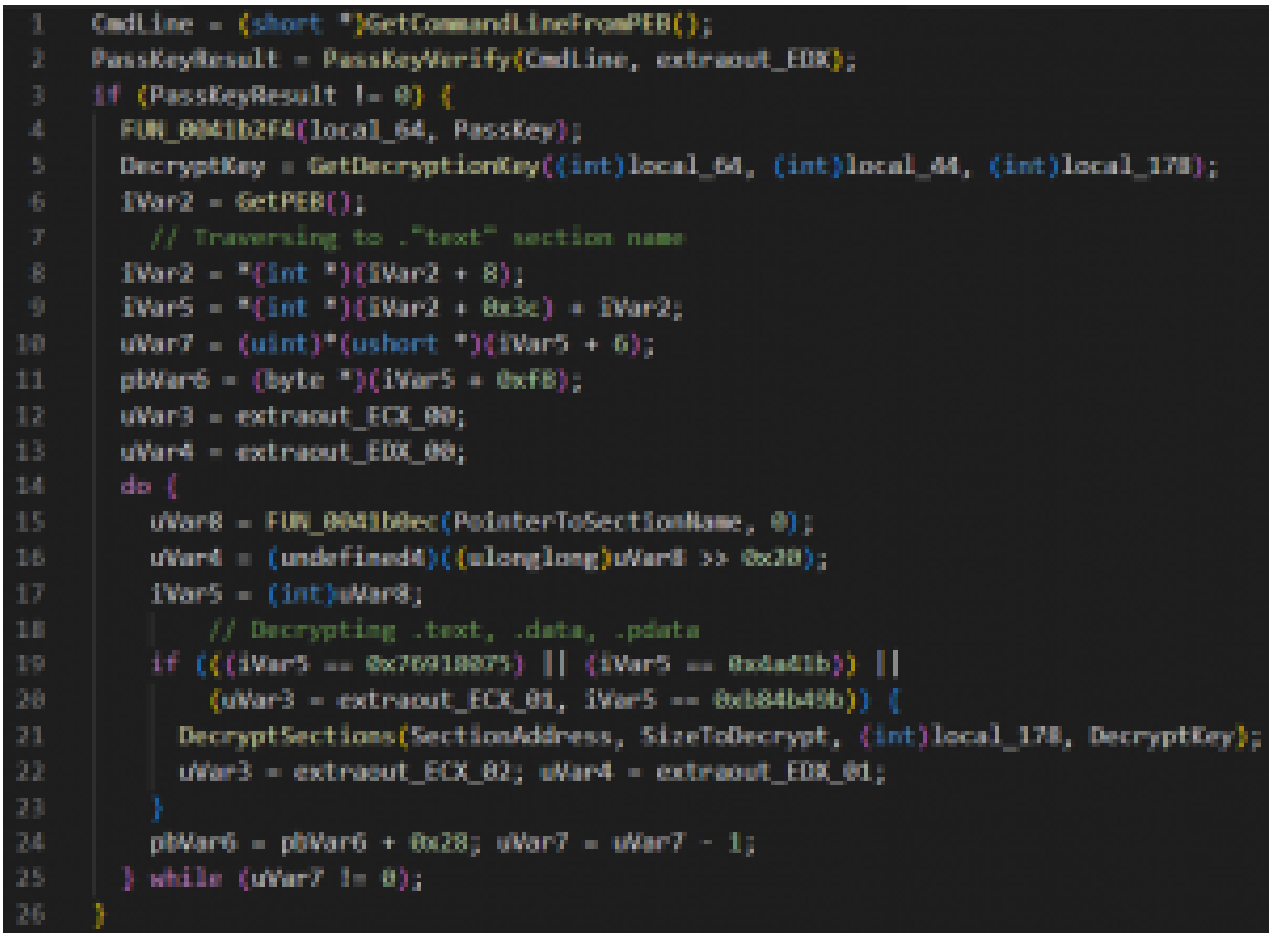
PSEXEC is also used to spread laterally across the victim’s network to execute the ransomware payload. The encryption is done using a multi-threaded approach where only shared drives got encrypted. The executed payload must have a valid key passed along with the command-line option ‘-pass.’ The encrypted files are appended with the *.zbzdbs59d* extension, which suggests that the builder generates each payload with a random static string.

Payload Analysis

The ransomware payload is dropped inside the *Windows* directory, where every variant requires a unique key to be passed as an argument. This feature was previously known to be used by other ransomware groups like *BlackCat* and *Egregor*. Even if the name of the payload is changed from ‘Lock.exe’ to anything else or put in any other directory, it does not run. The pass key used in this case is **60c14e91dc3375e4523be5067ed3b111**.

Let us look at a few stages of the payload below:

Decrypting Sections



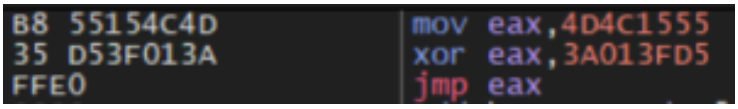
```
CmdLine = (short *)GetCommandLineFromPEB();
PassKeyResult = PassKeyVerify(CmdLine, extraout_EDX);
if (PassKeyResult != 0) {
  FUN_0041b2f4(local_64, PassKey);
  DecryptKey = GetDecryptionKey((int)local_64, (int)local_44, (int)local_178);
  iVar2 = GetPEB();
    // Traversing to ."text" section name
  iVar2 = *(int *)(iVar2 + 8);
  iVar5 = *(int *)(iVar2 + 0x3c) + iVar2;
  uVar7 = (uint)*(ushort *)(iVar5 + 6);
  pbVar6 = (byte *)(iVar5 + 0xf8);
  uVar3 = extraout_ECX_00;
  uVar4 = extraout_EDX_00;
  do {
    uVar8 = FUN_0041b0ec(PointerToSectionName, 0);
    uVar4 = (undefined4)((ulonglong)uVar8 >> 0x20);
    iVar5 = (int)uVar8;
      // Decrypting .text, .data, .pdata
    if (((iVar5 == 0x7691807) || (iVar5 == 0xda41b)) ||
       (uVar3 = extraout_ECX_01, iVar5 == 0xb84b49b)) {
      DecryptSections(SectionAddress, SizeToDecrypt, (int)local_178, DecryptKey);
      uVar3 = extraout_ECX_02; uVar4 = extraout_EDX_01;
    }
    pbVar6 = pbVar6 + 0x28; uVar7 = uVar7 - 1;
  } while (uVar7 != 0);
}
```

Fig. 2 – Pseudo code for decrypting PE Sections

The key passed in the argument is taken from the command line and verified. If it passes verification, this key is further processed to obtain a 1-byte key to decrypt specific sections obtained by traversing the PEB structure. The three sections decrypted in memory are – TEXT, DATA, and PDATA.

Resolving Obfuscated APIs

Being packed and having only a few imports, Win32 APIs are resolved by decrypting the obfuscated string with XOR using the key **0x3A013FD5**, which is again unique to each payload.



```
B8 55154C4D          mov eax,4D4C1555
35 D53F013A          xor eax,3A013FD5
FFE0                 jmp eax
```

Fig. 3 – Resolving APIs

Privilege Escalation

When Admin privileges are not present during execution, it uses **CMSTPLUA COM** to bypass the UAC prompt, a legitimate Windows Connection Manager Service. This elevates the rights from the user to the administrator level with another instance of the ransomware payload, terminating the current process.

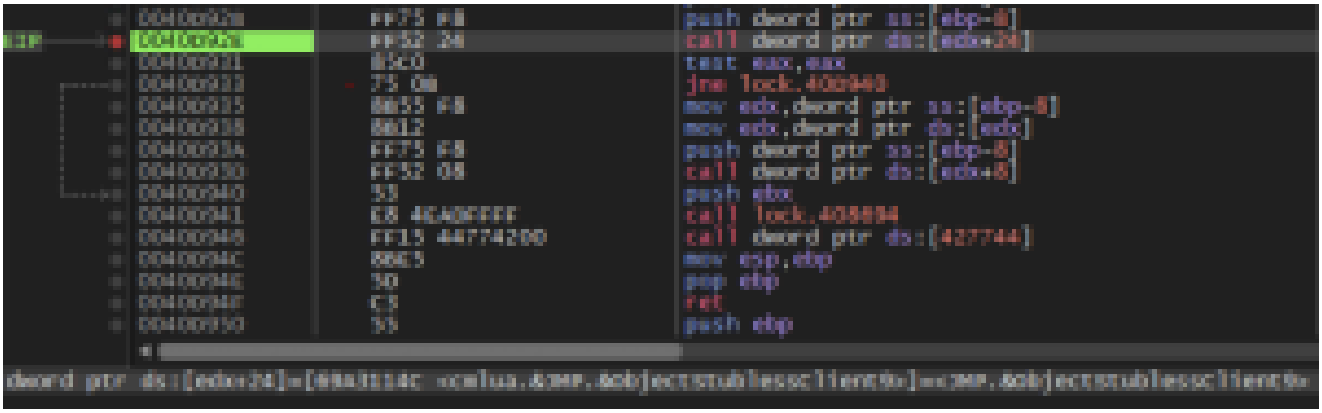


Fig. 4 – UAC Bypass using CMSTPLUA

Anti-Debugging Technique

Threads used for file encryption are hidden from the debugger by calling **NtSetInformationThread** Win32 API via **ThreadInformationClass** with an undocumented value **0x11** that denotes **ThreadHideFromDebugger**. This hinders dynamic analysis by not allowing debug information from the current ransomware's thread to reach the attached debugger.

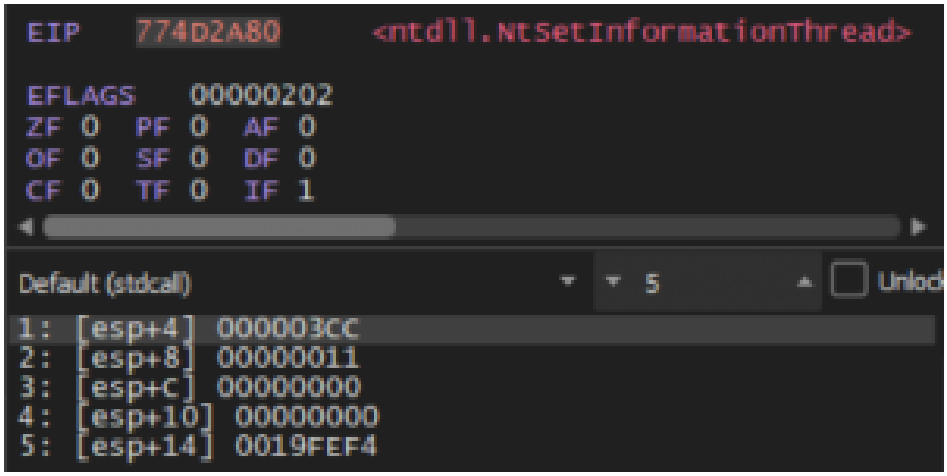


Fig. 5 – Anti-Debugging technique to hide threads

Anti-Forensic Activity

As part of wiping out its traces, lots of anti-forensic activity is observed where Windows Event Logs are disabled by setting multiple registry subkeys to value 0.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

Specifically, Windows Defender is disabled for evasion. An exhaustive list of Events Cleared.

Service Deletion and Process Termination

Process terminated included *SecurityHealthSystray.exe* and the mutex created during execution was **13fd9a89b0eede26272934728b390e06**. Services were enumerated using a pre-defined list and deleted or killed if found on the machine:

1. Sense
2. Sophos
3. Sppsvc
4. Vmicvss
5. Vmvss
6. Vss
7. Veeam
8. Wdnissvc
9. Wscsvc
10. EventLog

A few of the services deleted:

- sc stop “Undelete”
- sc delete “LTService”
- sc delete “LTSvcMon”
- sc delete “WSearch”
- sc delete “MsMpEng”
- net stop ShadowProtectSvc
- C:\Windows\system32\net1 stop ShadowProtectSvc

Tasks Killed

Scheduled tasks are enumerated and deleted, some of which are shown below. An exhaustive list of Tasks Killed.

IBM*	PrnHtml.exe*	DriveLock.exe*	MacriumService.exe*
sql*	PAGEANT.EXE*	CodeMeter.exe*	ReflectMonitor.exe*
vee*	firefox.exe*	DPMClient.exe*	Atenet.Service.exe*
sage*	ngctw32.exe*	ftpdaemon.exe*	account_server.exe*
mysql*	omtsreco.exe	mysqld-nt.exe*	policy_manager.exe*

bes10*	nvwmi64.exe*	sqlwriter.exe*	update_service.exe*
black*	Tomcat9.exe*	Launchpad.exe*	BmsPonAlarmTL1.exe*
postg*	msmdsrv.exe*	MsDtsSrvr.exe*	check_mk_agent.exe*

Shadow Volume Copies Deleted

Volume shadow copies are enumerated using a WMI query and then deleted to prevent system restoration

```
vssadmin.exe Delete Shadows /All /Quiet
```

Removal of all Active Network Connections

```
net use * /delete /y
```

Registry Activity

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticecaption /t REG_SZ /d "ATTENTION to representatives!!!! Read before you log on" /f
```

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticetext /t REG_SZ /d "Your system has been tested for security and unfortunately your system was vulnerable. We specialize in file encryption and industrial (economic or corporate) espionage. We don't care about your files or what you do, nothing personal – it's just business. We recommend contacting us as your confidential files have been stolen and will be sold to interested parties unless you pay to remove them from our clouds and auction, or decrypt your files. Follow the instructions in your system" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA /v RunAsPPL /t REG_DWORD /d 0 /f
```

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
```

Ransom Note

Before encryption, the ransom note is created in every directory except the *Program Files* and the *Windows* directory, which aren't encrypted. We can see that they have moved the naming convention of ransom notes from '*Restore-My-Files.txt*' to a static string format "*zbzdbs59d.README.txt*".

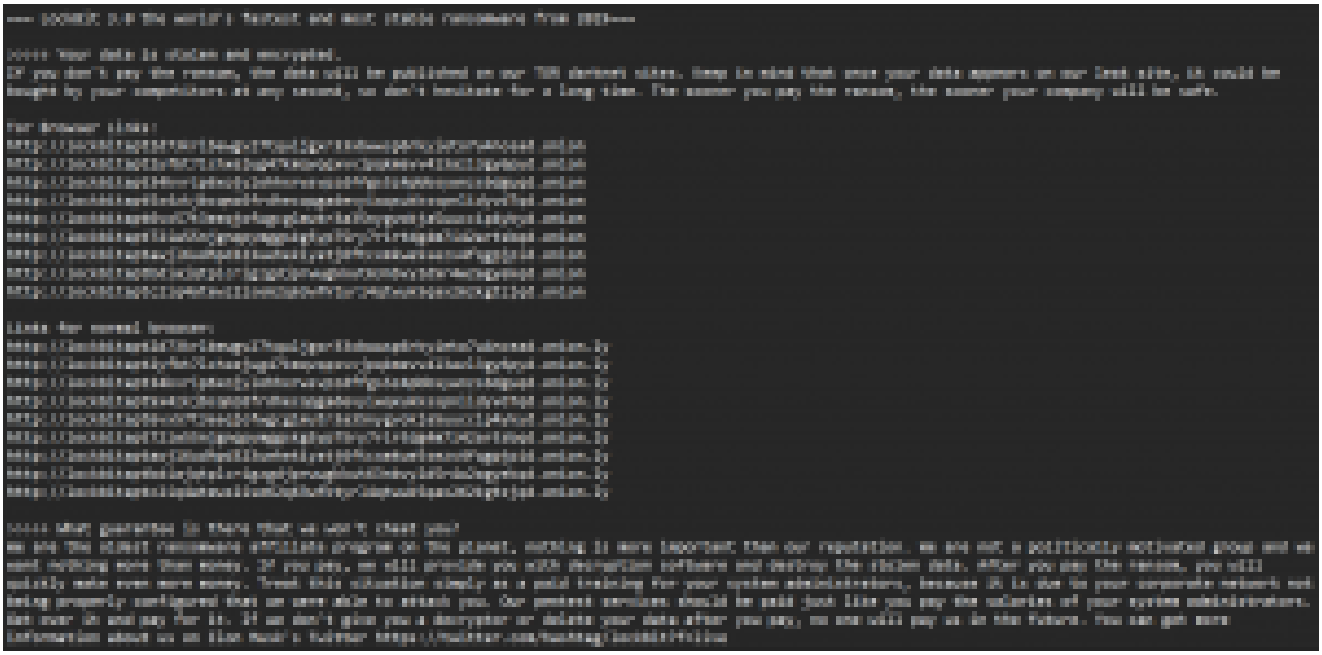


Fig. 6 – Ransom Note

The ransom note contains instructions to install the TOR browser, links for a chat, and the personal ID unique to the victim to communicate with the attackers. It also includes the threat message to leak the stolen data if the ransom amount is not paid and ends with the warnings as usual. Multiple TOR mirrors for their leak site can be seen in the ransom note, which is used to reduce redundancy.

File Encryption

Before starting file encryption, a registry key for *DefaultIcon* is created to associate an icon to all the encrypted files. Along with this ICO file (zbzdbs59d.ico), a BMP file is also dropped in the **C:\ProgramData** directory. Files are encrypted by creating multiple threads where each filename is replaced with a random string generated and appending the extension to them. With full encryption completed under 2 minutes it still has the fastest encryption process since LockBit 2.0.

3QWswsm	ZBZDBS59D File
3wVmRYd	ZBZDBS59D File
04eUA1Q	ZBZDBS59D File
bd9d8Wr	ZBZDBS59D File
GehEBd0	ZBZDBS59D File
LiF56VS	ZBZDBS59D File
MNOwSoN	ZBZDBS59D File
Ofm1jFX	ZBZDBS59D File
OK9AnJJ	ZBZDBS59D File
p9w1GDm	ZBZDBS59D File
Q7sVUZx	ZBZDBS59D File
u3WBseg	ZBZDBS59D File
UHqHpK7	ZBZDBS59D File
xFn67A6	ZBZDBS59D File
XRxPMXH	ZBZDBS59D File
yMBTQmC	ZBZDBS59D File
Yy82qMy	ZBZDBS59D File

Fig. 7 – Encrypted Filenames

Changing Wallpaper

Finally, the desktop background (different from 2.0 variant) of the victim machine is changed with the *systemparametersinfoW* win32 API, and displays LockBit Black, and instructions to be followed for decryption.

Fig. 8 – Modified Wallpaper

Conclusion

Unprotected systems in the network were brute-forced to run the PSEXEC tool for lateral movement across the systems. This was done to execute LockBit's latest Black ransomware variant. With LockBit 3.0 introducing its bug bounty program and adopting new extortion tactics, it is mandatory to take precautions like downloading applications only from trusted sources, using antivirus for enhanced protection, and avoiding clicking on any links received through email or social media platforms. As threat actors create their own variants from the leaked LockBit Black's builder, proactive measures must be taken to stay protected.

IOCs

MD5	Protection
7E37F198C71A81AF5384C480520EE36E	Ransom.Lockbit3.S28401281 HEUR:Ransom.Win32.InP

IPs

3.220.57.224

72.26.218.86

71.6.232.6

172.16.116.149

78.153.199.241

72.26.218.86

5.233.194.222

27.147.155.27

192.168.10.54

87.251.67.65

71.6.232.6

64.62.197.182

43.241.25.6

31.43.185.9

194.26.29.113

Jumpsecuritybusiness[.]com

Subject Matter Experts

- Tejaswini Sandapolla
- Umar Khan A
- Parag Patil
- Sathwik Ram Prakki

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing about...

Articles by Sathwik Ram Prakki »

No Comments

Leave a Reply.Your email address will not be published.