Indian Power Sector targeted with latest LockBit 3.0 variant

seqrite.com/blog/indian-power-sector-targeted-with-latest-lockbit-3-0-variant/

Sathwik Ram Prakki August 10, 2022

10 August 2022

Written by Sathwik Ram Prakki

Estimated reading time: 5 minutes

After the infamous Conti ransomware group was disbanded, its former members started to target energy and power sectors with a new unknown ransomware payload. The intelligence derived by Quick Heal researchers had already identified the Energy and Power sector as a segment prone to cyberattacks and had increased the vigil on the same. This proactive monitoring proved fruitful soon after we identified one of the recent premium entities attacked in this segment. Our investigation and analysis determined that the new LockBit 3.0 ransomware variant caused the infection. The same has been claiming its dominance over other ransomware groups this year.

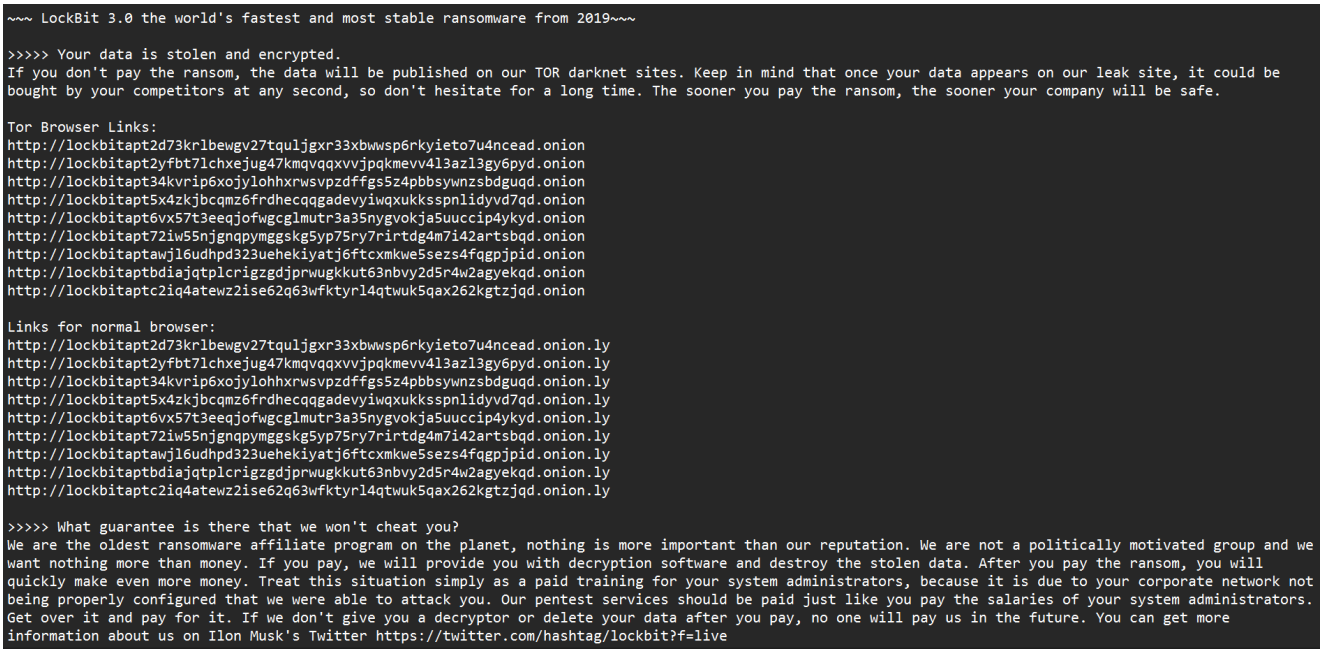

Fig. 1 – Ransom Note

The entity that bore the brunt of this ransomware attack had endpoints at multiple locations, connected with each other & the server in a mesh-topology spread across numerous locations. From the logs of multiple systems and telemetry, we observed that Windows Sys-Internal tool **PSEXEC** was utilized from an unprotected system to execute the ransomware payload (Lock.exe) on all the systems laterally. The noteworthy observation was that only the shared drives were found to be encrypted.

Initial access was obtained via brute forcing techniques where multiple user names were used for lateral movement. The encryption timestamp was in the early morning of 27-June-2022. Anti-forensic activities were also observed, which cleared event logs, killed multiple tasks, and deleted services simultaneously.

Initial Analysis

The service PSEXESVC was first observed to be installed a week before the encryption, with successful SMB connections surging just before the encryption. Malicious BAT files were executed by the same service only on one endpoint:

- 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” “

PSEXESVC executed the ransomware payload that must have a valid key passed along with the command-line option ‘-pass’. The encrypted files were appended with *.zbzdbs59d* extension which suggests that random generation was done with each payload.

Engine and ARW Telemetry show that the ransomware payload (Lock.exe) was detected at multiple locations on the same day. This shows that the payload was dropped in all these systems but was detected by AV.

Payload Analysis

All the sections on the payload are encrypted, which can only be decrypted bypassing the decryption key as a command-line parameter '-pass'. The key obtained for this sample is: **60c14e91dc3375e4523be5067ed3b111**

The key is further processed to decrypt specific sections in memory that are obtained by traversing the PEB and later calls the decrypted sections.

```
psVar1 = (short *)FUN_0041b2e4();      // GetCommandLine
iVar2 = FUN_0041b248(extraout_ECX,extraout_EDX,psVar1,(byte *)local_380);
if (iVar2 != 0) {
  FUN_0041b2f4(local_64,local_380);
  local_68 = FUN_0041b348((int)local_64,(int)local_44,(int)local_178);
  iVar2 = FUN_0041b2d4();      // Get PEB
  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(uVar3,uVar4,pbVar6,0);
    uVar4 = (undefined4)((ulonglong)uVar8 >> 0x20);
    iVar5 = (int)uVar8;
        /* Decrypting Specific Sections */
    if (((iVar5 == 0x76918075) || (iVar5 == 0x4a41b)) ||
       (uVar3 = extraout_ECX_01, iVar5 == 0xb84b49b)) {
      FUN_0041b41c((byte *)(*(int *)(pbVar6 + 0xc) + iVar2),*(int *)(pbVar6 + 0x10),(int)local_178
                   ,local_68);
      uVar3 = extraout_ECX_02;
      uVar4 = extraout_EDX_01;
    }
    pbVar6 = pbVar6 + 0x28;
    uVar7 = uVar7 - 1;
  } while (uVar7 != 0);
}
```

Fig. 2 – Decrypting Sections

Being packed and having only a few imports, Win32 APIs are resolved by decrypting the obfuscated string with XOR using the key **0x3A013FD5**.

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

Fig. 3 – Resolving Win32 APIs

Privilege Escalation

When Admin privileges are not present during execution, it uses **CMSTPLUA COM** for UAC bypass to elevate the privileges with another instance of the ransomware payload, terminating the current process.

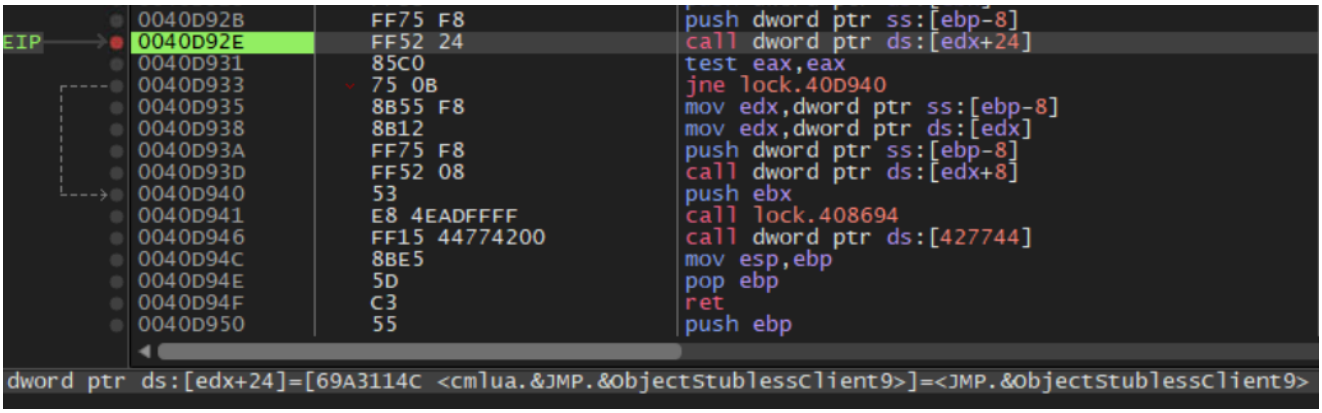

Fig. 4 – UAC Bypass

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 were deleted 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

Anti-Debugging Technique

Threads used for file encryption were hidden from the debugger using ***NtSetInformationThread*** function with undocumented value (ThreadHideFromDebugger = 0x11) for ThreadInformationClass parameter.

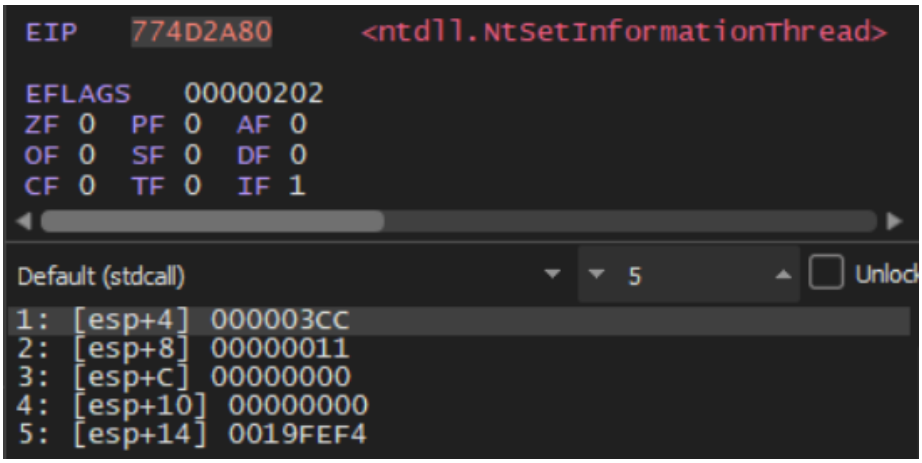

Fig. 5 – NtSetInformationThread technique

File Encryption

Before starting file encryption, the malware associated an icon to encrypted files by creating and writing it into an image file in the **C:\ProgramData** directory as *zbzdbs59d.ico*. Files were encrypted by creating multiple threads where each filename was replaced with a random string generated and appending the extension to them.

Fig. 6 – Encrypted Filenames

The ransom note '*zbzdbs59d.README.txt*' is created inside every directory except the *Program Files* and the *Windows* directory, which aren't encrypted. It contains instructions to install the TOR browser, links for a chat along with the personal ID and ends with the warnings as usual. The victim machine's wallpaper is modified with the name 'LockBit Black' and mentions the instructions to be followed:

Fig. 7 – Modified Wallpaper

Anti-Forensic Activity

As part of wiping out its traces, the ransomware disabled Windows Event Logs by setting multiple registry subkeys to value 0.

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

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*

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

Shadow Volume Copies Deleted

vssadmin.exe Delete Shadows /All /Quiet

Removal of all Active Network Connections

net use * /delete /y

Exhaustive List of all the Logs

- Events Cleared
- Tasks Killed

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

Conclusion

Unprotected systems in the network were brute-forced to run the PSEXEC tool for lateral movement across the systems to execute the ransomware payload. 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.

IOCs

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

IPs

3.220.57.224

72.26.218.86

71.6.232.6

172.16.116.14

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.

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 »

Related Posts

- 

  CVE-2022-26134: Actively Exploited Atlassian OGNL Injection Zero-Day Vulnerability

  July 5, 2022

- 

  CVE-2022-30190: Zero-day vulnerability “Follina” in MSDT exploited in the wild

  June 10, 2022

- 

  Threat Advisory: CVE-2022-30190 ‘Follina’ – Severe Zero-day Vulnerability discovered in MSDT

  June 3, 2022

No Comments

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