LockBit Resurfaces With Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK

Published: 2021-08-16 · Archived: 2026-04-02 10:59:02 UTC

Ransomware

The ransomware group LockBit resurfaced in June with LockBit 2.0, with reports indicating an increased number of targeted companies and the incorporation of double extortion features. Our detections followed attack attempts in Chile, Italy, Taiwan, and the UK from July to August.

By: Jett Paulo Bernardo, Jayson Chong, Byron Gelera, Nikki Madayag, Mark Marti, Cris Tomboc, Sean Torre Aug 16, 2021
Read time: 6 min (1542 words)

The ransomware group LockBitnews- cybercrime-and-digital-threats resurfaced in June with LockBit 2.0, with reportsopen on a new tab indicating an increased number of targeted companies and the incorporation of double extortion featuresnews-cybercrime-and-digital-threats influenced by ransomware families such as Ryuknews- cybercrime-and-digital-threats and Egregor.

In contrast to LockBit's attacks and featuresnews article in 2019, this version includes automatic encryption of devices across Windows domains by abusing Active Directory (AD) group policies, prompting the group behind it to claim that it's one of the fastest ransomware variants in the market today. The group also includes an advertising campaign to recruit new "affiliates" from inside the target companies themselves in its attacks, seemingly to remove middlemen (of other threat actor groups) and to enable faster attacks by providing valid credentials and access to corporate networks.

From July 1 to Aug. 15, we detected attack attempts involving LockBit 2.0 in Chile, Italy, Taiwan, and the UK. We advise organizations and users to update their systems and enable multilayered defense mechanisms accordingly.

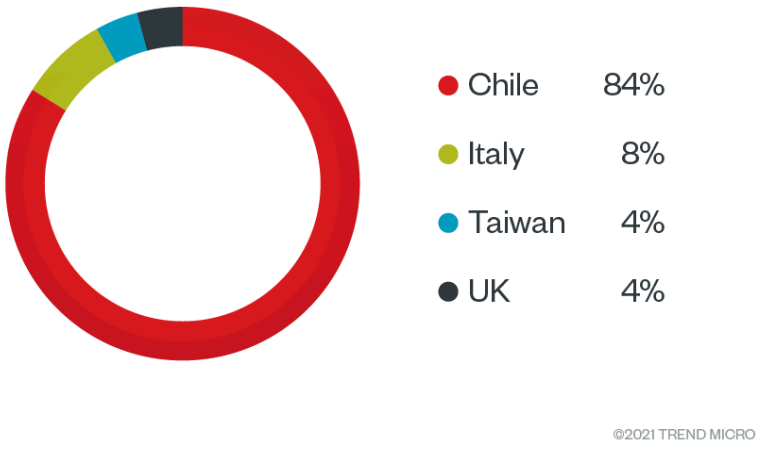

Figure 1. The countries affected by LockBit 2.0, based on our telemetry from July 1 to Aug. 15, 2021

LockBit 2.0 routine and updates

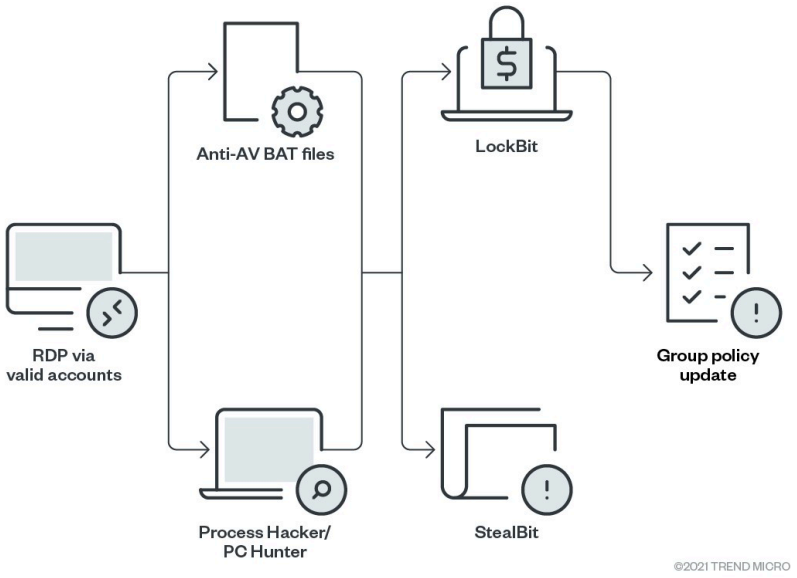

Figure 2. The infection chain of LockBit 2.0

LockBit 2.0 prides itself on having one of the fastest and most efficient encryption methods in today's ransomware threat landscape. Our analysis shows that while it uses a multithreaded approach in encryption, it also only partially encrypts the files, as only 4 KB of data are encrypted per file.

Like other ransomware-as-a-service (RaaS) operations, LockBit 2.0 looks for affiliates to perform the intrusion and exfiltration on targets. The group behind it also helps affiliates by providing StealBit (detected by Trend Micro as TrojanSpy.Win32.STEALBIT.YXBHM), a tool that can automatically exfiltrate data. Attackers can also access victims' systems with valid remote desktop protocol (RDP) accounts.

Once in a system, LockBit 2.0 uses a network scanner to identify the network structure and to find the target domain controller. It also uses multiple batch files that can be used to terminate processes, services, and security tools. There are also batch files for enabling RDP connections on the infected machine. The following are the tools and components that ensure LockBit's smooth execution:

- delsvc.bat (detected by Trend Micro as Trojan.BAT.KILLPROC.D) ensures that crucial processes, such as MySQL and QuickBooks, are unavailable. It also stops Microsoft Exchange and disables other related services.
- AV.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) uninstalls the antivirus program ESET.
- LogDelete.bat (detected by Trend Micro as PUA.BAT.DHARMA.A) clears Windows Event Logs.
- Defoff.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) disables Windows Defender features such as real-time monitoring.

LockBit 2.0 also abuses legitimate toolsnews- cybercrime-and-digital-threats such as Process Hackeropen on a new tab and PC Hunteropen on a new tab to terminate processes and services in the victim system. terminate processes and services in the victim system.

Once in the domain controller, the ransomware creates new group policies and sends them to every device on the network. These policies disable Windows Defender, and distribute and execute the ransomware binary to each Windows machine.

We found LockBIT_7D68A5BFD028A31F.exe (detected by Trend Micro as Ransom.Win32.LOCKBIT.SMYEBGW) as the main ransomware module that appends .lockbit to every encrypted file. Once LockBit 2.0 completes encrypting a device, it drops a ransom note, Restore-My-Files.txt (detected by Trend Micro as Ransom.Win32.LOCKBIT.SMA.note), into every encrypted directory. The note emphasizes that files are not only encrypted but also at risk of being published if the ransom is not paid.

Figure 3. The LockBit 2.0 ransom note dropped into every encrypted directory

LockBit 2.0 also changes the desktop wallpaper into an image with instructions on how victims can pay for the ransom and how organization insiders can be part of the "affiliate recruitment" of the group behind the ransomware. The group guarantees payouts of "millions of dollars" and anonymity in exchange for credentials and access.

Figure 4. The LockBit 2.0 ransom note as a desktop wallpaper

Ryuk and Egregor influences

LockBit worked with the Maze ransomware cartel and was previously dubbed the ransomware "ABCD" because of the extension it appended to encrypted files before updating to the current extension. But after Maze's shutdownopen on a new tab, the LockBit group went on with its own leak site, which led to the development of LockBit in September 2019. The previous version showed characteristics of ready-made ransomware using the double extortion techniques of encrypting files, stealing data, and leaking the stolen data when the ransom was not paid. Two years later, LockBit 2.0 shows influences of and similarities to Ryuk and Egregor, particularly with regard to certain notable behaviors:

Wake-on-LAN feature inspired by Ryuk ransomware, sending the Magic Packet "0xFF 0xFF 0xFF 0xFF 0xFF 0xFF" to wake offline devices.

```
do
{
  buf[v171] = 0xFFu;
  *(&v231 + v171) = *(v171 + v170 + 4);
  ++v171;
}
while ( v171 < 6 );

sendto(v237, buf, 102, 0, &v224, 16);
```

Figure 5. Sending the Magic Packet to devices

- Print bombing of the ransom note onto the victim's network printers, similar to Egregor's technique of attracting the victim's attention. It uses Winspool APIs to enumerate and print a document on connected printers.

```
Enum_Printer_490530(PRINTER_ENUM_LOCAL, v4);
Enum_Printer_490530(PRINTER_ENUM_NETWORK, v0);
Enum_Printer_490530(PRINTER_ENUM_REMOTE, v1);
return Enum_Printer_490530(PRINTER_ENUM_CONNECTIONS, v2);
```

Figure 6. Enumerating printers

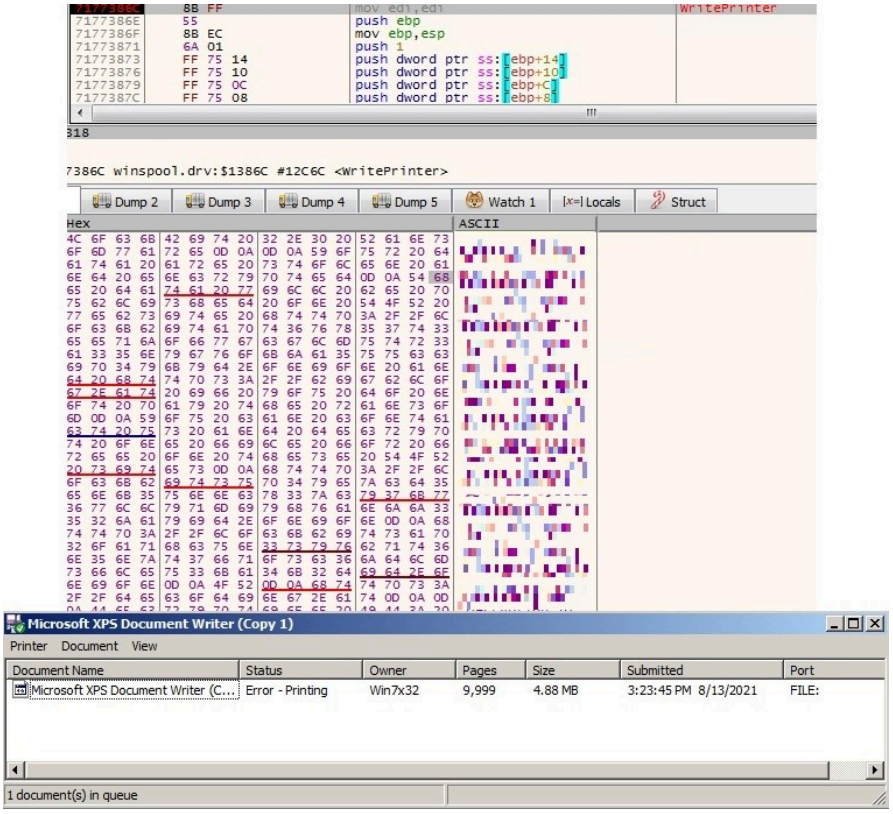

Figure 7. The WritePrinter API used to print ransom notes on printers

Conclusion

The group behind LockBit 2.0 recently conducted a highly publicized attackopen on a new tab, so it should go without saying that organizations need to keep a wary eye on this ransomware variant. LockBit 2.0 is especially tricky for its fast encryption. We also assume that this group will continue to make a scene for a long time, especially since it's currently recruiting affiliates and insiders, making it more capable of infecting many companies and industries. It would also be wise to assume and prepare for upgrades and further developments in LockBit 2.0, especially now that many companies are aware of its capabilities and how it works.

Best practices

Given its persistence, speed of propagation, and methods of intrusion, LockBit 2.0 is likely to cause significant damage to its victims, be it financial or reputational. Here are some best practices from the frameworks set by the Center of Internet Securityopen on a new tab and the National Institute of Standards and Technologyopen on a new tab that can help organizations prevent and mitigate the impact of attacks involving ransomware like LockBit 2.0:

- Audit and inventory: Take an inventory of all organizational assets and data, and identify authorized and unauthorized devices, software, and personnel accessing particular systems. Audit and monitor all logs of events and incidents to identify unusual patterns and behaviors.
- Configure and monitor: Deliberately manage hardware and software configurations, and only grant administrative privileges and access to specific personnel when absolutely necessary. Monitor the use of network ports, protocols, and services. Implement security configurations on network infrastructure devices such as firewalls and routers, and have a software allow list to prevent malicious applications from being executed.
- Patch and update: Perform periodic vulnerability assessments, and conduct regular patching or virtual patching for operating systems and applications. Ensure that all installed software and applications are updated to their latest versions.
- Protect and recover: Enforce data protection, backup, and recovery measures. Implement multifactor authentication in all devices and platforms used whenever available.

- Secure and defend: Perform sandbox analysis to examine and block malicious emails. Employ the latest version of security solutions to all layers of the system, including email, endpoint, web, and network. Spot early signs of an attack such as the presence of suspicious tools in the system, and enable advanced detection technologies such as those powered with AI and machine learning.
-
- Train and test: Perform security skills assessment and training for all personnel regularly, and conduct red-team exercises and penetration tests.

Trend Micro solutions

Organizations can benefit from security solutions that encompass a system's multiple layers (endpoint, email, web, and network) not only for detecting malicious components but also for close monitoring of suspicious behaviors in the network.

Trend Micro™ Vision One™products provides multilayered protection and behavior detection, spotting questionable behaviors that might otherwise seem benign when viewed from only a single layer. For an even closer inspection of endpoints, Trend Micro Apex One™products offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware. This allows detecting and blocking ransomware early on before it can do any real damage to the system.

With techniques such as virtual patching and machine learning, Trend Micro™ Cloud One™ Workload Securityproducts protects systems against both known and unknown threats that exploit vulnerabilities. It also takes advantage of the latest in global threat intelligence to provide up-to-date, real-time protection.

Ransomware often gets into the system through phishing emails. Trend Micro™ Deep Discovery™ Email Inspectorproducts employs custom sandboxing and advanced analysis techniques to effectively block ransomware before it gets into the system.

Indicators of compromise

SHA-256	Filename	Detection
0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049		Ransom.Win32.LOCK
0906a0b27f59b6db2a2451a0e0aabf292818e32ddd5404d08bf49c601a466744		Ransom.Win32.LOCK
21879b5a8a84c5fe5e009c85744caf74b817c57203020bf919037d7ccb6b6a58		Ransom.Win32.LOCK
255f8465962bedaf7a373da5f721aecbc1d6027ca2e4256c6c4352f2de179ca0	Restore-My-Files.txt	Ransom.Win32.LOCK
4db47caf8d93e855b8364def67d3d3282fc964dc4684df6bbe172ea6e902e6fe		
7b64ca8fe1cace0744a28f43961f17f8ea51910a54d6629502bfb9f3f3e5f831		
8c0e4a6fd28f94fa17a96f6e424b122f5d1216b230a33c6dff5dbf6654d0721c		
a05ed65787b390ba33b04b4b99c3810cbaf684b37f8839e57db8316e6f01af31		Ransom.Win32.LOCK
a26250b8d2431b497400c8a754285a6259a81a31ae629ee25331f6030b34e543		Ransom.Win32.LOCK
b09a92dedbcb8d5faed6fcc2194ebaa24da601376b47e1edf705519a7860964e		Ransom.Win32.LOCK
bea7aed0dfbf7ce7491d7c8cfed35a2e626fbd345bb7425a34dae6f5894629b1		Ransom.Win32.LOCK
cb29c6fbd085407e0e8a58e7cd6512c8c5dfa06f88fdeeb9a66d025fdfc6dd32		
f03584ecdee29e63dee1b7bf2347f605d1e1d6379a8f55e9a85c6a329bf3967b		Ransom.Win32.LOCK
28042dd4a92a0033b8f1d419b9e989c5b8e32d1d2d881f5c8251d58ce35b9063	ph.exe	PUA.Win32.ProcHack
3407f26b3d69f1dfce76782fee1256274cf92f744c65aa1ff2d3eaaaf61b0b1d	StealBit.exe.dangerousFile	TrojanSpy.Win32.STE
4bb152c96ba9e25f293bbc03c607918a4452231087053a8cb1a8accb1acc92fd		Ransom.Win32.LOCK TH
4edbf2358a9820e030136dc76126c20cc38159df0d8d7b13d30b1c9351e8b277		
bcbb1e388759eea5c1fbb4f35c29b6f66f3f4ca4c715bab35c8fc56dcf3fa621		
dd8fe3966ab4d2d6215c63b3ac7abf4673d9c19f2d9f35a6bf247922c642ec2d		
4db7eeed852946803c16373a085c1bb5f79b60d2122d6fc9a2703714cdd9dac0	sample.exe	TrojanSpy.Win32.STE

6876eef67648a3797987745617b9fdfb31a703b7809e7f12bb52c6386e185917	CryptNN.exe	Ransom.Win32.LOCK
717585e9605ac2a971b7c7537e6e311bab9db02ecc6451e0efada9b2ff38b474		Ransom.Win32.LOCK TH
73406e0e7882addf0f810d3bc0e386fd5fd2dd441c895095f4125bb236ae7345		Ransom.Win32.LOCK
7b5db447f6c29c939f5e0aae1b16431a132db5a2ab4420ba9818af2bf4496d21	psdelsvc.bat	Trojan.BAT.KILLPRO
aae5e59d6424515c157f3c4a54e4feeb09759d028290ab0271f730e82f58f10f	delsvc.bat	
94e6b969c100483970fc3985bf2b173f2f24d796a079114f584f42484840be28	AV.bat	Trojan.BAT.KILLAV.V
a398c70a2b3bf8ae8b5ceddf53fcf6daa2b68af2fadb76a8ea6e33b8bbe06f65	defoff.bat	
98e4c248377b5b62121c7b9ef20fc03df3473cbd886a059998f4210e8df07f15	pchunter64.exe	PUA.Win32.PCHunter
a7591e4a248c04547579f014c94d7d30aa16a01bb2a25b77df36e30a198df108		Ransom.Win32.LOCK TH
acad2d9b291b5a9662aa1469f96995dc547a45e391af9c7fa24f5921b0128b2c		Ransom.Win32.LOCK
b3faf5d8cbc3c75d4c3897851fdaf8d7a4bd774966b4c25e0e4617546109aed5		Ransom.Win32.LOCK
bd14872dd9fdead89fc074fdc5832caea4ceac02983ec41f814278130b3f943e	StealBit.exe	TrojanSpy.Win32.STE
d089d57b8b2b32ee9816338e96680127babc5d08a03150740a8459c29ab3ba78		Ransom.Win32.LOCK
d089d57b8b2b32ee9816338e96680127babc5d08a03150740a8459c29ab3ba78	LockBIT_7D68A5BFD028A31F.exe	Ransom.Win32.LOCK
f32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202		Ransom.Win32.LOCK

URLs

- hxxp://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion
- hxxp://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did[.]onion
- hxxp://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid[.]onion

MITRE ATT&CK Tactics and Techniques

Tactic	Technique
Initial access	T1078: Valid accounts
Defense evasion	T1562.001: Impair defenses: disable or modify tools T1546.008: Event-triggered execution: accessibility features T1070.001: Indicator removal on host: clear Windows Event Logs
Exfiltration	T1041: Exfiltration Over C2 Channel
Impact	T1486: Data encrypted for impact T1489: Service stop T1490: Inhibit System Recovery

Tags

Source: https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html