

LockBit strikes with new 5.0 version, targeting Windows, Linux and ESXI systems



acronis.com/en/tru/posts/lockbit-strikes-with-new-50-version-targeting-windows-linux-and-esxi-systems



Authors: Acronis Threat Research Unit

Summary

The Acronis Threat Research Unit (TRU) analyzed the latest version of LockBit ransomware (version 5), which targets Windows, Linux and ESXi systems, and shares some similarities with the previous version 4.

The Windows sample has most defense evasion and anti-analysis techniques applied across all analyzed samples. This includes packing, DLL unhooking, process hollowing, patching Event Tracing for Windows (ETW) functions and clearing all available logs in the system.

Linux and ESXi versions are very similar, except for functions that target virtualization. Neither of these versions is packed, but almost all strings are encrypted.

All versions have the same ransom note, append a random extension to each encrypted file, and the same encryption routine that involves XChaCha20 and Curve25519.

The LockBit site was hosted on infrastructure with historical ties to SmokeLoader, indicating possible infrastructure reuse or cooperation.

Introduction

In September 2025, a new version of LockBit ransomware was released, supporting Windows, Linux and ESXi systems, with a primary target being the U.S. business sector. As is typical for the ransomware-as-a-service model, LockBit employs a double-extortion scheme, also exfiltrating files to the attacker's server to increase the likelihood of receiving the ransom. As threat actors advertised, this version has improved defense evasion and fast encryption, and having multiple systems support makes this malware a very serious threat. What's notable among the multiple systems support its proclaimed capability to "work on all versions of Proxmox." Proxmox is an open-source virtualization platform and is being adopted by enterprises as an alternative to commercial hypervisors, which makes it another prime target of ransomware attacks.



Source: LockBit data leak site

Background and context

When it first appeared in the wild in 2019, the LockBit group was known as ABCD due to its use of encrypted file extensions. Since then, they have rebranded and become one of the leading ransomware-as-a-service providers. During group history, they released multiple versions, bringing improvements with each update.

In 2021, with the release of LockBit 2.0, attackers also introduced StealBit software for data theft. In the same year, the LockBit 1.0 version was released for Linux and ESXi systems.

In 2022, [LockBit 3.0](#), also known as LockBit Black, was released, sharing many similarities with Black Matter and ALPHV BlackCat ransomware. With this version, LockBit became the most active ransomware group, performing 44% of global ransomware attacks that year. Additionally, attackers initiated a bug bounty program with the release of this version.

At the start of 2024, their servers were seized by law enforcement, revealing that LockBit 4.0 was under development.

At the start of 2025, LockBit 4.0 was finally released, and in September that year, the LockBit 5.0 version was dropped, targeting Windows, Linux, and ESXI versions and advertised as more modular, with faster encryption and improved methods for defense evasion.



Source: LockBit data leak site

Victimology and targeting

The data leak site contains victims who were attacked with their status. At the time of analysis, it contains 60 victim entries, with the first one dated December 4, 2025.



Throughout LockBit's history, law enforcement has repeatedly disrupted its data leak sites, while the current version maintains reserved mirrors of data leaked by previous iterations.



According to the data leak site affiliate program page, LockBit permits affiliates to target any organization, including critical infrastructure and medical facilities. While many ransomware groups avoid these sectors due to heightened law enforcement attention, LockBit explicitly places full responsibility for such attacks on the affiliates who carry them out.



Additionally, LockBit prohibits attacks on countries from the 'post-Soviet' region.



Analyzing the latest victims from data leak sites, we can see that the private business sector is the primary target of LockBit. Other victims are medical facilities, financial and manufacturing companies, government and educational agencies.



Most victims are located in the U.S., but there are also a lot of victims in other regions.



Technical analysis

Windows



Shown above is the execution chain of Lockbit 5.0 ransomware. The LockBit 5.0 Windows sample is a PE64 file with a fake compilation timestamp. Detect It Easy shows that the '.rdata' section is compressed but cannot determine which packer is used. The previous version of LockBit used a slightly modified version of UPX packer.



This file has an invalid certificate that expired in 1996 and was issued to the BorgWarner company, which is an American manufacturer of car components. The file manifest describes this file as 'Blender'.



Execution

After loading a sample into the disassembler, we can see that its import table is empty and it contains only 123 functions, which is a very low number. In the very first function that the sample enters, we can see numerous calculations that, at first glance, appear to be part of a decryption process. In fact, this is a Mixed Boolean–Arithmetic (MBA) Obfuscation wrapped around a return-address dependent hash.



The primary goal of this logic is to resolve the function address and call it at the end of this routine. This technique is widely used in samples at different execution stages.



One more anti-debugging method is used: passing an invalid handle to the 'NtClose' function. When executed normally, it will just return 'STATUS_INVALID_HANDLE' result, which can be handled in the code. When attached to the debugger, it will raise an exception, and further execution will not be possible. LockBit passes the PE header to this function instead of a valid handle.



At the start of execution, it checks the system language, compares it with 419 in HEX, which is 1049 in decimal, and represents the Russian language. Additionally, it retrieves information about the geographical location and compares it with the 'C9' value. It is common for Russian-based malware to avoid users within the same region.



Next, it obtains command-line arguments and compares them with the saved ones. They can be shown using the '-h' parameter.



Then it creates a mutex using the decoded string. If '-nomutex' argument was passed, it won't be created, allowing multiple instances to run.



Next, it enters the injection routine. Passing '-d' argument will cause LockBit to skip this function and encrypt files directly. Here, it loads the saved string '\\defrag.exe', obtains the system directory, and concatenates these strings into a file path. Using 'GetSystemDirectoryW' instead of storing the full path can indicate that LockBit can also be built for x32 systems, as it has a different system directory compared to the x64 one. Defrag.exe — a system utility responsible for defragmentation — will be started in a suspended state.



When the process starts, it allocates a new memory block and writes data to it. Right before writing, we can observe the 'MZx' header in the buffer, which is actually the image of LockBit. After that, it sets a new thread context, resumes it and terminates execution.



Encryption

LockBit 5.0 employs the same encryption scheme as its predecessor. This involves XChaCha20 for symmetric and Curve25519 for asymmetric encryption. The number of encryption threads depends on the number of processors, as determined by the 'GetSystemInfo' function. The main thread is responsible for file search. It walks through folders, saves found files to the list and drops a ransom note file in each enumerated folder. Encryption threads will grab files from the list and process them. For each encrypted file, it generates a random 16-character extension. After writing encrypted data to a file, it will append an additional data block to the end of the file.



The first data from this block is the original file size (in example — 1A43 = 6723 bytes), followed by 6 bytes of '00', which is used as a separator. The final data block contains an encrypted ChaCha20 key. Due to file extensions being random, this block is also used to determine if a file was encrypted, in case malware tries to process it again.



Post encryption execution

After file encryption is done, it performs some additional anti-analysis and anti-forensic actions. First, it patches the 'EtwEventWrite' function, which is a part of Event Tracing for Windows that is widely used by security software. It replaces the very first byte in this function with the value 'C3', which is a 'return' instruction in assembly.



After patching, it also clears all available event logs by passing different service log files to the 'EvtClearLog' function.



If '-d' argument was provided, the sample will output execution progress, including each file that was encrypted.



The next step is *self-deletion*, which can be skipped with a '-k' argument. Here, it opens its own file with the 1000 (GENERIC_ALL) flag, loads the saved alphabet, and generates a random 6-character string using it. Then, it calls the 'SetInformationByHandle' function with flag 3 (FileRenameInfo) and the generated string as arguments. This will change the file name. It then closes the handle to its file, opens it once more and again calls the 'SetInformationByHandle' function, but this time with flag 4 (FileDispositionInfo). Passing value '1' will trigger file deletion.



Free space wiper

If a '-w' argument was passed, it will create a '.tmp' file in C:\ drive and start writing '00' bytes to it, 4194304 bytes per write until the free space ends. This wiper will always be executed in the injected process 'Defrag.exe', even if the '-d' argument was passed.



Linux and ESXI

Execution

Linux and ESXi versions are very similar, except for a couple of command-line arguments and functions. Compared to the Windows version, they also have some differences in command-line arguments. Both Linux and ESXi versions output execution steps by default, while Windows uses a '-d' argument for this purpose. Additionally, the Linux version can save logs to a file and choose the percentage of the file that must be encrypted. The ESXi version also has commands for virtualization.



After loading samples in the disassembler, we can see that, unlike the Windows version, it has some stored imports and strings, and it is not packed. Despite that, there are still very few functions, but some of them are quite large. Also, most of the strings in the samples are encoded.



To avoid analysis, it gets the parent process name, decodes saved values and compares them. If matches, it will terminate execution.



Here is the saved list of analysis software that LockBit avoids:

gdb – GNU Debugger

lldb – LLDB debugger

strace – diagnostic, debugging, and instructional userspace utility.

ltrace – debugging utility, used to display the calls a userspace application makes to shared libraries.

rr – lightweight tool for recording, replaying, and debugging execution of applications.

The ESXi version also includes additional checks when running on the ESXi system. To do that, it executes '**vmware -v 2> /dev/null**', which retrieves the VMware version and suppresses any output to the console. It will compare the results with decoded strings 'ESXi 4' and 'ESXi x64'. If there is no match, execution will terminate. One more significant difference between Linux and ESXi is that the latter uses the 'fork()' function to create a copy of the LockBit process. While the original process will be terminated, further execution continues in the duplicated one.

Encryption

The number of encryption threads depends on the number of logical processors in the system. Like in the Windows version, the main thread is responsible for directory enumeration. It decodes the saved ransom note and drops it in each encrypted folder.



ESXI has additional search logic that targets virtual machines. It will look for the **'/vmfs/'** folder, which stores all the files of the virtual machines. It also has the ability to terminate virtual machines to ensure that files will not be blocked during encryption. This termination can be disabled using an **'-o'** argument. Using an **'-n'** argument will force the sample to skip virtual machines with a particular ID. In this case, LockBit will use the **'/bin/vim-cmd vmsvc/getallvms'** command to get a list of all registered machines and get their names by ID. The encryption scheme is the same for Windows, Linux and ESXI, and similar to the LockBit version 4.



Hardcoded Curve25519 public keys:



As mentioned before, both these versions have console output enabled by default, printing every file that was encrypted. After the encryption process is completed, it performs a free disk space wipe, which involves creating a TEMP file and writing it with **'00'** bytes, similar to the Windows version.



Unlike the Windows version, it additionally prints a summary of the encryption process.



Ransom Note

All LockBit 5.0 samples have the same ransom note text, except for the victim ID.



SmokeLoader IP address used by LockBit

At the start of December 2025, researcher Rakesh Krishnan exposed the public IP address and domain that contain LockBit sites. This IP address was already used in SmokeLoader samples in 2022 and was linked to **'rodericwalter[.]com'** URL. The SmokeLoader family is a generic backdoor

that is widely used to deliver other malware to the targeted systems. When this IP address was used by LockBit, it had the opportunity to receive RDP connections on port 3389, but it went offline shortly after exposing it.



After a quick SmokeLoader sample analysis, we can see that it uses a saved URL instead of an IP address, meaning that it resolves its address during execution and doesn't store it in code. This means that this sample will be able to connect to this server only if it has the same URL, which the LockBit site doesn't have.



This suggests that LockBit is more likely to have acquired or rented one of the servers from SmokeLoader's infrastructure to host its own. It is common practice for malware operators to cooperate and do business together.

Conclusion and impact

Analysis of LockBit 5.0 reveals a largely unified ransomware framework across its Windows, Linux and ESXi variants. All versions share common execution logic, command-line driven configuration, identical ransom note content, the same encryption scheme based on XChaCha20 and Curve25519, and support for free disk space wiping. The primary architectural difference lies in the Windows variant, which employs custom packing, while the Linux and ESXi versions remain unpacked. This represents a notable shift from LockBit 4.0, which relied on a modified UPX packer, while retaining similar core functionality.

The Windows sample exhibits the most extensive use of defense evasion and anti-analysis techniques, highlighting Windows as the primary development focus, consistent with historical ransomware targeting trends. At the same time, the presence of mature Linux and ESXi variants, combined with explicit support for virtualized environments such as Proxmox, underscores LockBit's continued expansion toward enterprise and infrastructure focused targets. This evolution reinforces that no platform should be considered low risk and that comprehensive, cross platform protection remains critical.

Detection by Acronis

This threat has been detected and blocked by Acronis EDR / XDR:



This threat is detected by Acronis as "SFS:Ransomware:Lockbit:I"

Indicators of Compromise (IoCs)

LockBit Windows x64

[7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82](#)

[180e93a091f8ab584a827da92c560c78f468c45f2539f73ab2deb308fb837b38](#)

LockBit Linux x64

[4dc06ecee904b9165fa699b026045c1b6408cc7061df3d2a7bc2b7b4f0879f4d](#)

[98d8c7870c8e99ca6c8c25bb9ef79f71c25912fbb65698a9a6f22709b8ad34b6](#)

LockBit ESXI x64

[90b06f07eb75045ea3d4ba6577afc9b58078eafeb2cdd417e2a88d7ccf0c0273](#)

SmokeLoader sample with LockBit-related IP address

[1da6525ae1ef83b6f1dc02396ef0933732f9ffdfca0fda9b2478d32a54e3069b](#)

LockBit exposed server

205.185.116[.]233

205.185.116[.]233[:.]3389

karma0[.]xyz

Data leak site:

hxxp[://]lockbitfbinpwhbyomxkiqtwwhiyetrbbk4hnqmshaonqxmsrqwg7yad[.]onion/

Threat actor chat link:

hxxp[://]lockbitsupplyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd[.]onion

Leaked data mirrors:

hxxp[://]lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd[.]onion/

hxxp[://]lockbit7z2mmiz3ryxafn5kapbvbbiywsxwovasfkgf5dqqp5kxlajad[.]onion/

hxxp[://]lockbit7z2og4jlsmdy7dzty3g42eu3gh2sx2b6ywtvhrjtss7li4fyd[.]onion/

hxxp[://]lockbit7z355oalq4hiy5p7de64l6rsqutwlvydqje56uvevcc57r6qd[.]onion/

hxxp[://]lockbit7z36ynytxwjzuoao46ck7b3753gpedary3qvuzn3iczhe4id[.]onion/

hxxp[://]lockbit7z37ntefjdbjextn6tmdkry4j546ejnru5cejeguitiopvhad[.]onion/

hxxp[://]lockbit7z3azdoxdpqxzliszutufbc2fldagztdu47xyucp25p4xtqad[.]onion/

hxxp[://]lockbit7z3ddvg5vuez2vznt73ljqgwx5tnuqaa2ye7lns742yiv2zyd[.]onion/

hxxp[://]lockbit7z3hv7ev5knxbrhsvv2mmu2rddwqizdz4vwfvxt5izr6zqqd[.]onion/

hxxp[://]lockbit7z3ujnkhxwahnjdudh5me2updvzxewhhc5qvk2snxezoi5drad[.]onion/

hxxp[://]lockbit7z4bsm63m3dagp5xglyacr4z4bwytkvkkwtn6enmuo5fi5iyd[.]onion/

hxxp[://]lockbit7z4cgxvictidwfxpuiov4scdw34nxotmbdjyxpkkvg34mykyd[.]onion/

hxxp[://]lockbit7z4k5zer5fbqi2vdq5sx2vuggatwyqvoodrkhxbxftyrvncid[.]onion/

hxxp[://]lockbit7z4ndl6thsct34yd47jrzdcpnfg3acfvpacuccb45pnars2ad[.]onion/

hxxp[://]lockbit7z55tuwaflw2c7torcryobdvhkcgvivhflyndyvcrexafssad[.]onion/

hxxp[://]lockbit7z57mkicfkuq44j6yrpu5finwvjllczkcp2uvdedsdonjztyd[.]onion/

hxxp[://]lockbit7z5ehshj6gzpetw5kso3onts6ty7wrnneya5u4aj3vzkeoaqd[.]onion/

hxxp[://]lockbit7z5hwhf6ywfuzipoa42tjlmal3x5suuccngsamsgklww2xgyqd[.]onion/

hxxp[://]lockbit7z5lthzv46lsg447o3cx2637dloc3qt4ugd3gr2xdkkkeayd[.]onion/

hxxp[://]lockbit7z6choojah4ipvdpzzfzxxchjbecnmtn4povk6ifdvx2dpnid[.]onion/

hxxp[://]lockbit7z6dqiutocr43onmvpth32njp4abfocfauk2belljipobxyd[.]onion/

hxxp[://]lockbit7z6f3gu6rjvrysn5gjbsqj3hk3bvsg64ns6pjdqr2xhvhsyd[.]onion/

hxxp[://]lockbit7z6qinyhhmibvycu5kwmcvgrbpvtztkvmdce5zwtucaeyrqd[.]onion/

hxxp[://]lockbit7z6rzyojiye437jp744d4uwtff7aq7df7gh2jvwqtv525c4yd[.]onion/

© 2003–2026 Acronis International GmbH.