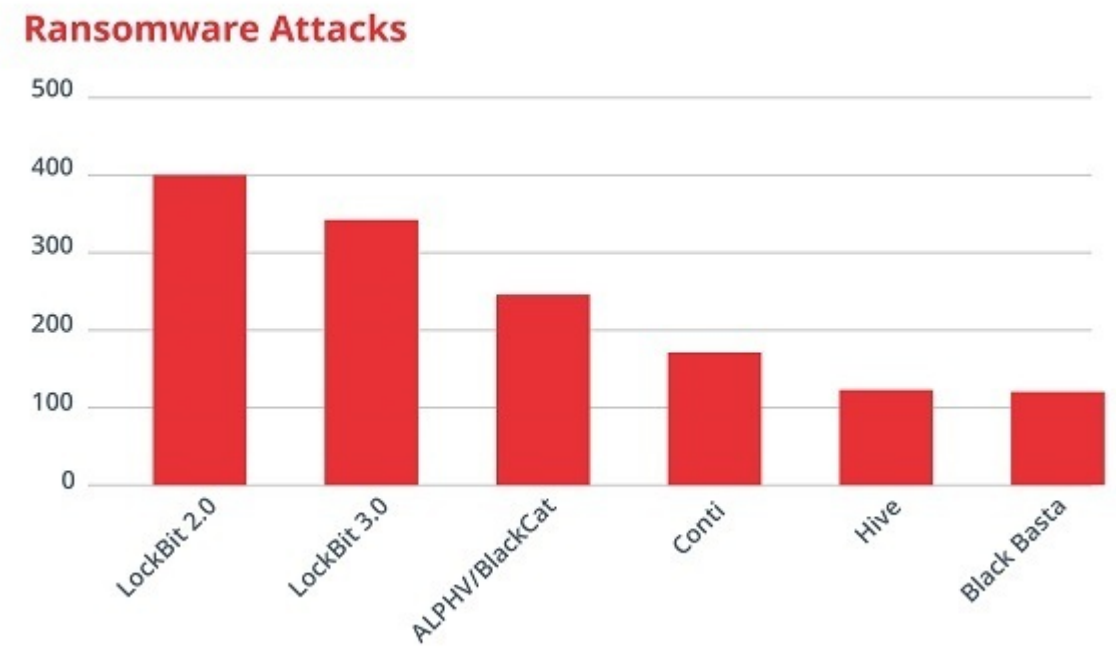
LockBit: response and recovery actions

Archived: 2026-04-06 01:14:58 UTC

LockBit is a ransomware family that has evolved significantly since its first appearance in 2020. One of its best-known variants, LockBit 3.0, stands out from its predecessors by its sophistication and enhanced ability to evade detection and security measures. This release has introduced more robust encryption methods, advanced data exfiltration tactics, and a more refined ransomware-as-a-service (RaaS) structure that attracts a growing number of affiliates.

Released at the end of June 2022, LockBit 3.0 quickly established itself as one of the most damaging of its generation. Since its launch, it has targeted key infrastructure around the world, especially the US and Europe, including government entities, banks, critical communication networks, factories, large consultancies and, particularly worryingly, the healthcare sector. In fact, its impact in terms of the number of attacks has only been surpassed by its predecessor, LockBit 2.0.

One of its most revolutionary aspects was launching its own bug bounty program, the first time this strategy has been observed in the context of ransomware. This innovative approach underscores the sophistication and professionalization of the cybercriminal groups behind LockBit, and represents a paradigm shift in how these actors seek to engage other security experts to help them stay active.



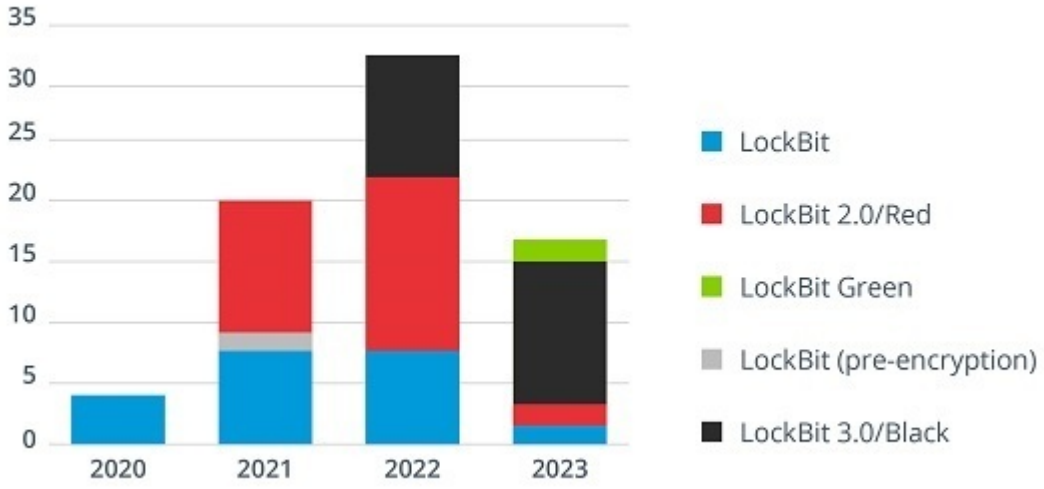
-Most Successful Ransomware Attack Campaigns in 2022. Source -

On February 20, 2024, in an international operation, law enforcement from 11 countries coordinated efforts to seize several darknet domains operated by the LockBit group, exploiting a critical vulnerability in PHP. The site is currently unavailable, thanks to its dismantling by the authorities.

Characteristics

Motivation

Although its origin in Russia also raises global geostrategic interests, LockBit's main motivation has been economic gain from extortion, through the tactic of "double extortion" to exfiltrate data and threaten to publish it if the ransom is not received, complicating detection, and blocking by security software.



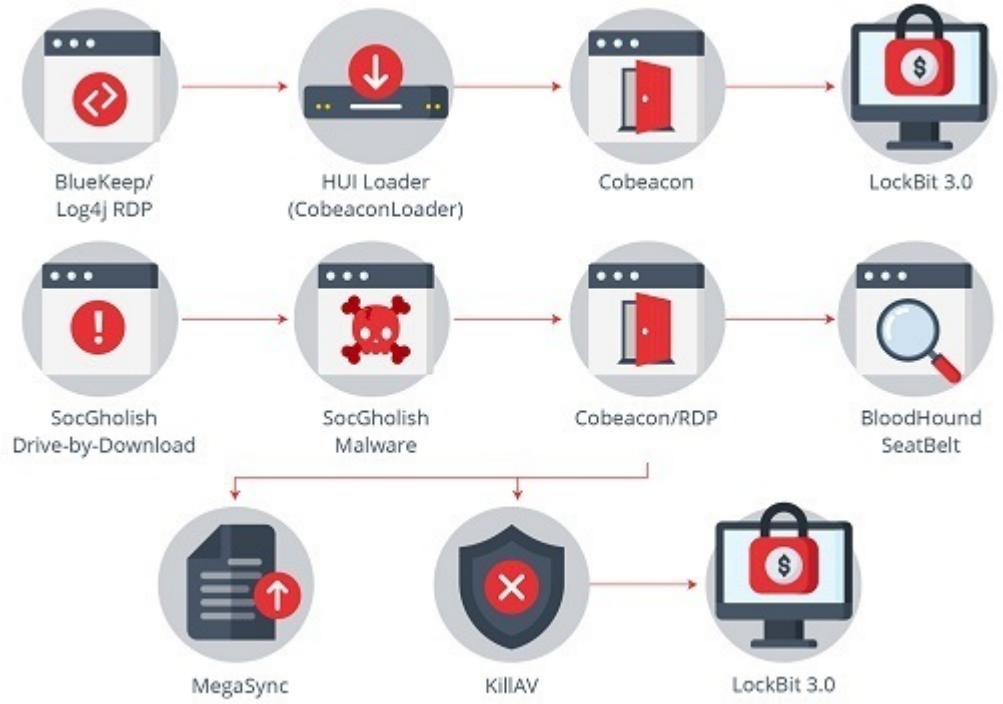
- Instances observed by ANSSI according to LockBit variants between 2020 and 2023. Source -

Infection and spread

Their techniques for penetrating systems also evolved and refined with each release, ranging from the use of insecure remote connections to the spread of emails with harmful content. But, in addition, LockBit, throughout its history, has been characterized by using a very large arsenal of exploits.

Among the most representative CVEs linked to this malware are: ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), PaperCut (CVE-2023-27350), BlueKeep (CVE-2019-0708), Apache Log4j (CVE-2021-44228) and Citrix Bleed (CVE-2023-4966).

Trendmicro identified two different scenarios in the case of LockBit 3.0, although there may be many more variants.



- LockBit 3.0 Execution Scenarios. Source -

- **BlueKeep/Log4j/RDP scenario**: In this scenario, attackers exploited known vulnerabilities such as BlueKeep, which affects unpatched remote desktop services in older versions of Windows, and Log4j, a vulnerability in the Java logging library, as well as weaknesses in the implementation of the Remote Desktop Protocol (RDP). Thus, attackers could obtain an initial entry point into the system or network. Once inside, they used a loader to download and install a Cobalt Strike agent, which was used to establish a persistent presence in the system, allowing lateral movement and preparation for the final phase of the attack: the deployment of LockBit 3.0.
- **SocGholish Drive-by-Download scenario**: This attack method required victims to be pre-infected by visiting a compromised website causing an unwanted download and execution (drive-by-download) of the SocGholish malware. This malware acted as an entry point to download other malicious tools, such as Cobeacon, and allow remote access via RDP. In addition, it can lead to the execution of reconnaissance tools, such as BloodHound and SeatBelt, to gain a detailed understanding of the network and trust relationships within Active Directory, thus facilitating a more targeted and effective attack. This scenario also culminates with the release of LockBit 3.0.

LockBit 3.0's activity has relied on a variety of open-source and third-party tools to facilitate its ransomware attacks. These include compression tools such as 7-zip to prevent detections prior to data exfiltration, network scanning utilities such as Advanced IP Scanner and Advanced Port Scanner to map victim networks and find access vectors, and remote management software, such as AnyDesk and TeamViewer, to control victims' devices remotely. It has also employed specialized security and systems administration tools, such as Bloodhound to rebuild Active Directory relationships and exploit them, and Mimikatz to extract credentials from the system. This arsenal allows them to evade defenses and gain elevated privileges, to exfiltrate data and facilitate lateral

movement within compromised networks. Although it has also developed others such as StealBit for automatic data exfiltration.

Evasion of detection and recovery

Before starting the encryption process, LockBit 3.0 executes several actions to ensure its effectiveness:

- **Terminates specific services and processes**: Detects and terminates a number of processes and services related to security, backup, database management, and other applications that could stop or interfere with the encryption process. For example, it disrupts services linked to antivirus programs, backup systems, and active databases to facilitate seamless encryption of critical files, using scan-evading techniques such as the NtTerminateProcess API, which terminates processes to bypass scans.
- **Disable and alter security services**: Modify system settings to disable security tools capable of detecting their presence. A notable case is the blocking of Windows Defender by alterations in the system registry, or the paralysis of services related to other security products, with the aim of creating an environment where ransomware can operate without being discovered or blocked by security defenses.
- **Delete backups**: The LockBit 3.0 strategy is done using Windows Management Instrumentation (WMI) via COM objects. This method leverages WMI's administrative capabilities to manipulate and delete operating system backups efficiently, making it difficult for victims of the ransomware attack to recover files .
- **Deletes and alters logs**: After executing its malicious operations, ransomware strives to erase or change system event logs to hinder forensic investigation and post-infection analysis. It also empties the contents of the recycle bin.

LockBit 3.0 employs threading when interacting with an API rather than directly calling the API, which is likely an attempt to complicate the analysis by researchers. This approach allows ransomware to execute multiple encryption tasks or processes simultaneously more efficiently, increasing the speed of the attack and reducing detection time.

Encryption

LockBit 3.0 implements a mechanism for its unpacking and decryption process, using an RC4 KSA-specific password to decrypt itself. This password initiates the first stage of the unpacking process, which takes place in several layers, starting with certain source code and then applying the RC4 algorithm.

Finally, the process identifies and executes Windows API functions, thus completing its preparation for the execution of the attack. In addition, it also employs algorithms, such as AES-256, ChaCha20, and RSA-2048, in its encryption operations, as ChaCha20 offers a high-performance alternative for encryption especially useful in environments where AES performance may not be optimal and RSA, on the other hand, is used for key encryption.

Response & Disinfection

On the NoMoreRansom platform you can find a disinfection suite aimed at version 3.0, developed by the Japanese police on the basis of international cooperation. It should be noted that it is based on the use of decryption keys

recovered by law enforcement agencies (around 1,000) and not on the exploitation of any vulnerability of the LockBit 3.0 ransomware. This means that data retrievability is limited. The package, called "Decryption Checker for LockBit.zip", in its version 0.5, offers two tools:

- The first tool, **Decryption ID Checker**, refers to the check_decryption_id.exe binary and compares the user's decryption ID with keys known to authorities, potentially offering a decryption solution with instructions for those with matching IDs.
    - **Preparation**: No special preparation is required beyond having access to the Windows operating system from where the tool will be run.
    - **Run**: From Windows Command Prompt (cmd) or PowerShell, navigate to the directory where the download is located and run check_decryption_id.exe. This step requires entering the unique decryption ID, when prompted.
    - **Result**: If a match is found in the database of known decryption keys, you will be told that a decryption key is available for you, and you will receive instructions on how to proceed.
- The second tool, **Check Decrypt for LockBit 3.0**, refers to the check_decrypt.exe binary, collects diagnostic information on the system, evaluating the possibility of partially decrypting encrypted files, although it does not guarantee a complete recovery. The steps to run this tool are:
    - **Preparation**: You need to have access to a Windows terminal on your system with encrypted files.
    - **Run**: Using a command console or PowerShell, navigate to the folder where check_decrypt.exe is located. Execute the command by providing the two necessary arguments: check_decrypt.exe <path_to_encrypted_files> <common_lockbit_extension>. The lockbit extension replaces the original file extension with a 9-character string. For example:
      E:\check_decrypt.exe "D:\data\lockbit_encrypted" "xE9thWXg6"
      During execution, status information will be displayed per console, including the number of files found with the specified extension and the progress in analyzing the data.
    - **Result**: Upon completion, a CSV file will be created in the directory from which the command was executed, with all the summarized information about all the analyzed files. This file is useful for determining which files might be potentially recoverable. If decryptable files are detected, the number of files amenable to decryption will be provided along with contact details for additional information on how to proceed. If no recoverable files are found, a message will be displayed stating that no decryptable files were found.

Although the scope of current recovery tools is limited, the seizure of large amounts of data from the malware's servers fuels the expectation that new tools with greater capabilities and scope may soon be developed to recover files that cannot be recovered with current tools.

Conclusions

The analysis of LockBit 3.0 underscores the crucial importance of research and development within the cybersecurity community, which has demonstrated its resilience and adaptability in the face of such threats.

International police collaboration is a fundamental pillar in the fight against cybercrime, allowing a more agile and coordinated response thanks to the exchange of intelligence and resources.

On the other hand, the increasing complexity of these attacks highlights the urgent need to strengthen cybersecurity awareness and preparedness, equipping organizations and individuals with the tools and knowledge necessary for early detection and effective response. Together, these elements make up a comprehensive and initiative-taking approach essential to navigating and mitigating risks in today's cyber threat environment.
