

LockBit 2.0: How This RaaS Operates and How to Protect Against It

By Amer Elsad, JR Gumarin, Abigail Barr

Published: 2022-06-09 · Archived: 2026-04-05 15:51:13 UTC

Executive Summary

LockBit 2.0 is ransomware as a service (RaaS) that first emerged in June 2021 as an upgrade to its predecessor LockBit (aka ABCD Ransomware), which was first observed in September 2019.

Since its inception, the LockBit 2.0 RaaS attracted affiliates via recruitment campaigns in underground forums, and thus became particularly prolific during the third quarter of calendar year 2021. The LockBit 2.0 operators claimed to have the fastest encryption software of any active ransomware strain as of June 2021, claiming accordingly that this added to its effectiveness and ability to disrupt the ransomware landscape.

While several top-tier RaaS affiliate programs, such as Babuk, [DarkSide](#) and [REvil](#) (aka Sodinokibi) disappeared from the underground in 2021, LockBit 2.0 continued to operate and gradually became one of the most active ransomware operations. While Conti was recognized as being the most prolific ransomware deployed in 2021 per our [2022 Unit 42 Ransomware Threat Report](#), LockBit 2.0 is the most impactful and widely deployed ransomware variant we have observed in all ransomware breaches during the first quarter of 2022, considering both leak site data and data from cases handled by Unit 42 incident responders.

According to data analysis of ransomware groups' dark web leak sites, LockBit 2.0 was the most impactful RaaS for five consecutive months. As of May 25, LockBit 2.0 accounted for 46% of all ransomware-related breach events for 2022. And the LockBit 2.0 RaaS leak site has the most significant number of published victims, with over 850 in total.

Additionally, LockBit 2.0 has affected many companies globally, with top victims based in the U.S., Italy and Germany. Its most highly targeted industry verticals include professional services, construction, wholesale and retail, and manufacturing.

Palo Alto Networks customers receive protections against LockBit 2.0 attacks from Cortex XDR, as well as from the WildFire cloud-delivered security subscription for the Next-Generation Firewall. (Please see the [Conclusion](#) section for more detail.)

LockBit 2.0 Overview

LockBit 2.0 is another example of RaaS that leverages double extortion techniques as part of the attack to pressure victims into paying the ransom.

In some cases, LockBit 2.0 operators have performed DDoS attacks on the victims' infrastructure as well as using a leak site. This practice is known as triple extortion, a tactic observed in groups like BlackCat, Avaddon and SunCrypt in the past.

Like other ransomware families such as [BlackByte](#), LockBit 2.0 avoids systems that use Eastern European languages, including many written with Cyrillic alphabets.

Unlike other RaaS programs that don't require the affiliates to be super technical or savvy, LockBit 2.0 operators allegedly only work with experienced penetration testers, especially those experienced with tools like Metasploit and [Cobalt Strike](#). Affiliates are tasked with gaining initial access to the victim network, allowing LockBit 2.0 to conduct the rest of the attack.

LockBit 2.0 has been observed changing infected computers' backgrounds to a ransomware note. The ransomware note was also used to recruit insiders from victim organizations. The notes claimed the threat actors would pay "millions of dollars" to insiders who provided access to corporate networks or facilitated a ransomware infection by opening a phishing email and/or launching a payload manually. The threat actors also expressed interest in other access methods such as RDP, VPN and corporate email credentials. In exchange, they offer a cut of the paid ransom.

Victimology

LockBit 2.0 targets organizations opportunistically. The operators work with initial access brokers to save time and allow for a larger profit potential. While typically seeking victims of opportunity, LockBit 2.0 does appear to have victim limitations. The group announced that they would not target healthcare facilities, social services, educational institutions, charitable organizations and other organizations that "contribute to the survival of the human race". However, despite these claims, there have been instances of affiliates undermining these guidelines by still opting to attack industry verticals such as healthcare and education.

Organizations in Europe and the U.S. are hit more often by LockBit 2.0 than those in other countries, likely due to the high profitability and insurance payouts.

Leak Site Data

During the first calendar year quarter of 2022, LockBit 2.0 persisted as the most impactful and the most deployed ransomware variant we observed in all ransomware breaches shared on leak sites.

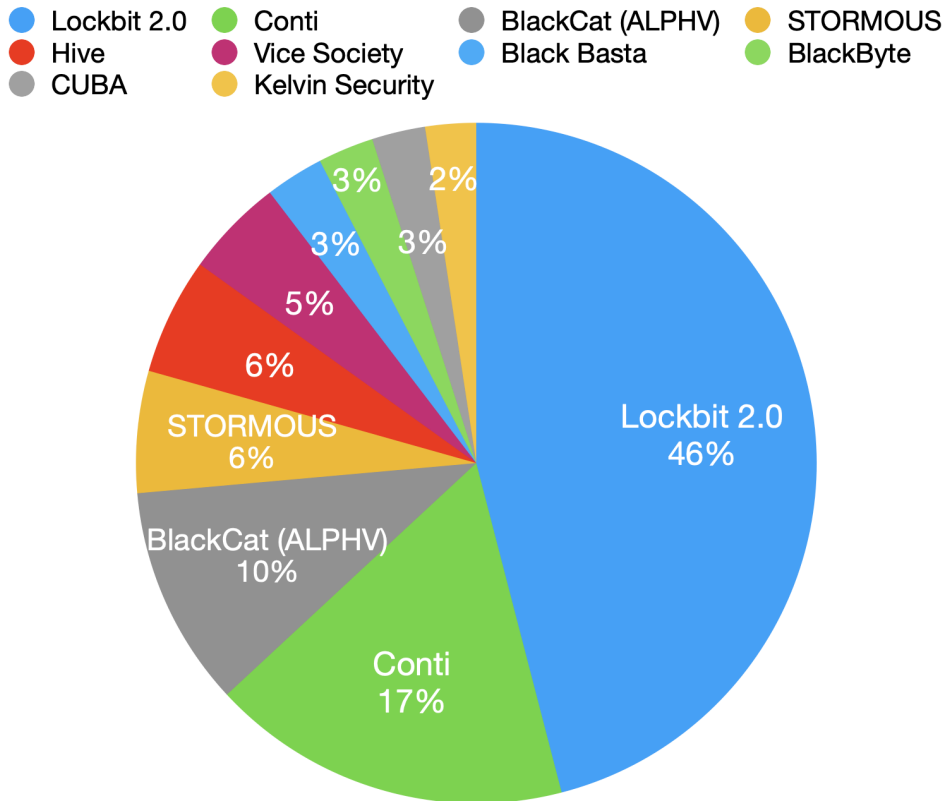


Figure 1. Ransomware leak site data from the first calendar year quarter of 2022.

According to leak site data analysis, LockBit 2.0 was the most impactful RaaS for five consecutive months. As of May 25, LockBit 2.0 accounted for 46% of all ransomware-related breach events for 2022 shared on leak sites.

Additionally, the LockBit 2.0 RaaS leak site has the most significant number of published victims, with over 850 in total. The site itself typically features information such as victim domains, a time tracker and measures of how much data was compromised.

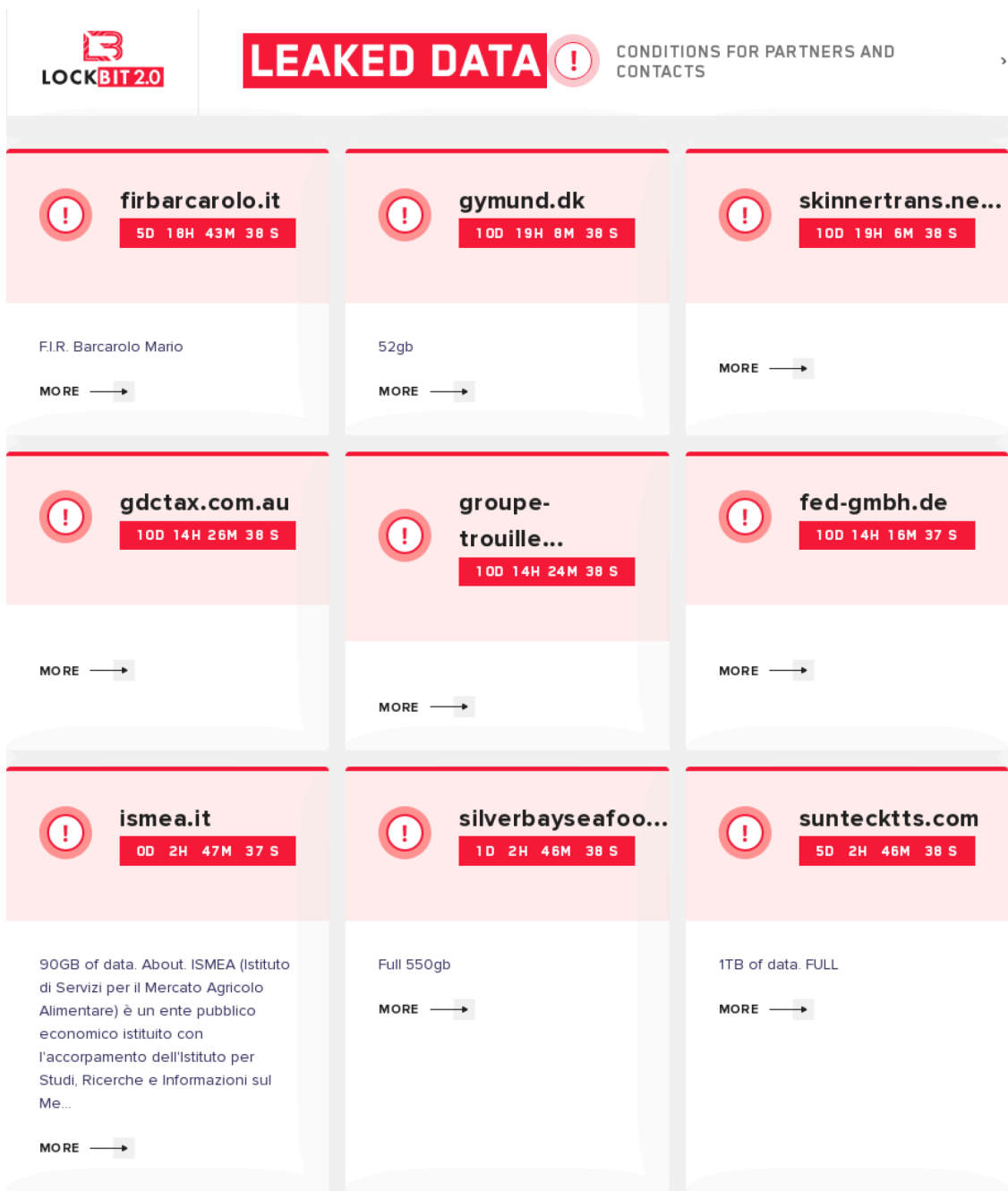


Figure 2. LockBit 2.0 leak site extortion site.

LockBit 2.0 [claims](#) that they have demanded ransom from at least 12,125 companies, as shown in the figure below.

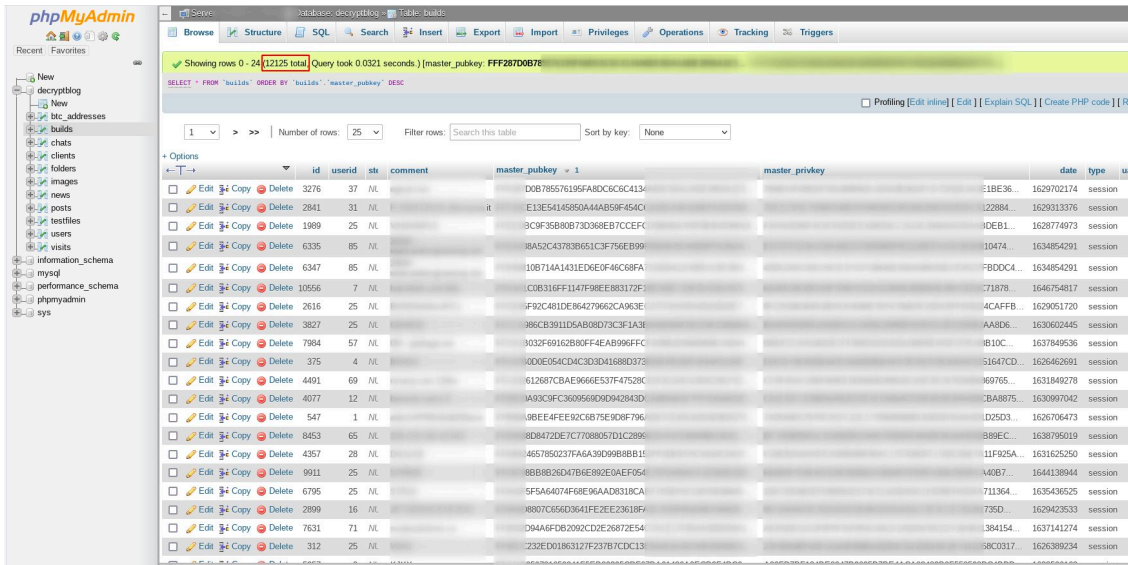


Figure 3. Source: VX-underground.

According to leak site data for LockBit 2.0, since its inception in June 2021, the RaaS has affected many companies globally, with top victims based in the U.S., Italy and Germany.

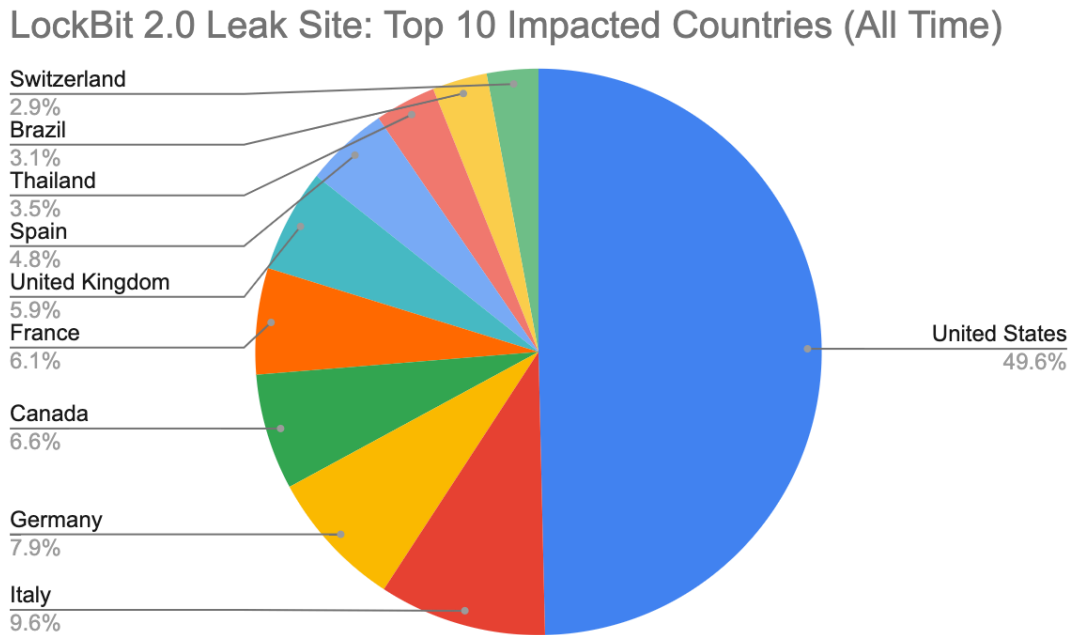


Figure 4. LockBit 2.0 geographical impact chart.

LockBit 2.0 has also impacted various victims across multiple industry verticals. Its most highly targeted industry verticals include professional services, construction, wholesale and retail and manufacturing.

LockBit 2.0 Leak Site: Top Leaked Industry Verticals (All Time)

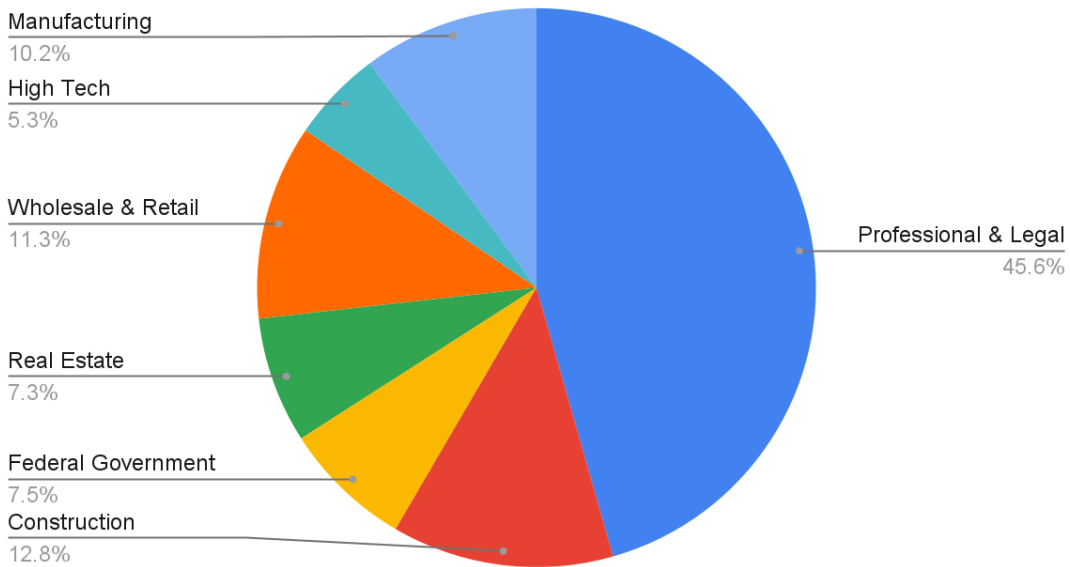


Figure 5. LockBit 2.0 impacted industry vertical chart.

When looking at leak site data across all ransomware families, we’ve observed LockBit 2.0 targeting the highest number of organizations in the following regions: JAPAC, EMEA, and LATAM.

Unit 42 Incident Response Data on LockBit 2.0

Cases handled by Unit 42 security consultants involving LockBit 2.0 since its appearance in June 2021 demonstrate shorter dwell times and less flexibility in negotiation in the beginning of FY 2022 (measured October-September) in comparison to the end of FY 2021. The following data is broken into fiscal years and quarters based on when the threat actor breached the network, not when the activity was noticed by a client.

LockBit 2.0 has shown a decrease in dwell time in FY 2022. From the last two quarters of FY 2021 to the first two quarters of FY 2022, there has been an average 37-day difference.

LockBit 2.0 Average Dwell Time (U42 IR)

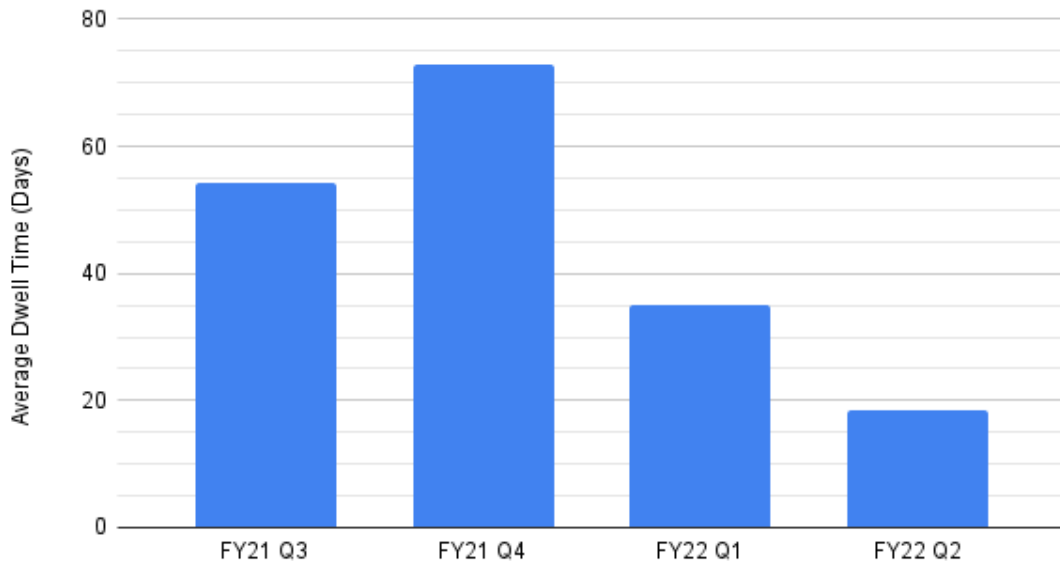


Figure 6. LockBit 2.0 average dwell time by fiscal quarter.

The difference in initial and final ransom demands over the past fiscal year has been converted to percentages and then averaged. The graph below demonstrates that at the end of FY 2021, threat actors using LockBit 2.0 were much more open to negotiations of ransom amounts; during that time the ransom was dropped approximately 83% from the initial ask on average. In comparison, we see less flexibility in FY 2022 Q1 and Q3 – threat actors only offered an average of about 30% as a price drop. FY 2022 Q2 is not included due to lack of sufficient information.

LockBit 2.0 Average Difference in Initial vs Final Ransom

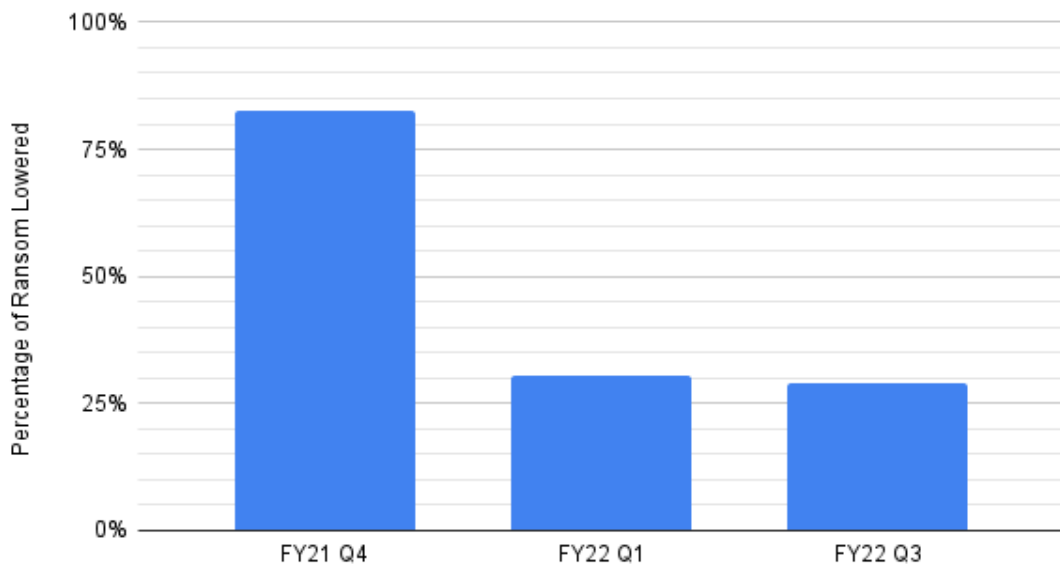


Figure 7. LockBit 2.0 average difference in initial vs final ransom amount, shown as percentages.

LockBit 2.0 Tactics, Techniques and Procedures

Technically speaking, we have observed LockBit 2.0 affiliates leveraging the following tactics, techniques and procedures:

| | |
|--|--|
| TA0001 Initial Access | |
| T1078 Valid Accounts | Credentials that have either been reused across multiple platforms or have previously been exposed. Additionally, this includes VPN accounts – not just domain and local accounts. |
| T1133 External Remote Services | Affiliates have been seen brute forcing exposed RDP services and compromising accounts with weak passwords. |
| T1190 Exploit Public-Facing Applications | Vulnerabilities such as ProxyShell (CVE-2021-34473) and improper SQL sanitization (CVE-2021-20028) have been observed being utilized as footholds into the environment. |
| TA0002 Execution | |
| T1053.005 Scheduled Task/Job | Scheduled Task. LockBit 2.0 can be executed via scheduled tasks. |
| T1059 Command and Scripting Interpreter | LockBit 2.0 is typically executed via command line arguments via a hidden window. Windows SysInternals PsExec has been utilized for both persistence and execution purposes. Its ability to execute processes on other systems spread the ransomware and assisted in reconnaissance activities. |
| TA0003 Persistence | |
| T1053.005 Scheduled Task/Job | Scheduled Task. It was quite common to see scheduled tasks used to create persistence for the ransomware executable, PsExec, and occasionally some defense evasion batch scripts. |
| T1078 Valid Accounts | Compromised accounts may be used to maintain access to the network. |
| T1136.001 Create Account | In rare cases, LockBit 2.0 has been observed to create accounts for persistence with simple names, such as “a.” |
| T1505.003 Server Software Component | With the upsurge of ProxyShell, webshells have become more common entry points. |
| TA0004 Privilege Escalation | |

| | |
|--|---|
| T1068 Exploitation for Privilege Escalation | The ProxyShell elevation of privilege on the Exchange PowerShell Backend (CVE-2021-34523), Windows Background Intelligent Transfer Service (BITS) improperly handling symbolic links (CVE-2020-0787), and abusing the CMSTPLUA COM interface have all been seen as methods of privilege escalation. |
| T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control | LockBit 2.0 has utilized a UAC bypass tool. |
| TA0005 Defense Evasion | |
| T1070 Indicator Removal on Host | Indicators, such as logs in Windows Event Logs or malicious files, are typically removed using wevtutil, a batch script, or CCleaner. |
| T1140 Deobfuscate/Decode Files or Information | Most PowerShell scripts involved in LockBit 2.0 cases are Base64 encoded. |
| T1484.001 Domain Policy Modification: Group Policy Modification | LockBit 2.0 has been seen using the PowerShell module InvokeGPUpdate to update the group policy. |
| T1562.001 Impair Defenses: Disable or Modify Tools | Windows Defender, other anti-malware solutions and monitoring tools are disabled utilizing a process explorer tool, a batch script or a specially crafted command line script. |
| T1564.003 Hide Artifacts: Hidden Window | Affiliates use hidden windows to hide malicious activity from plain sight. |
| TA0006 Credential Access | |
| T1003 OS Credential Dumping | As seen with other ransomware cases, Mimikatz is a key player in dumping credentials but LockBit 2.0 has been occasionally seen utilizing MiniDump as well. |
| T1555 Credentials from Password Stores | LockBit 2.0 has been seen utilizing numerous tools to dump passwords from password stores and Chrome using GrabChrome and GrabRFF. |
| TA0007 Discovery | |
| T1046 Network Service Discovery | Both Advanced Port Scanner and NetScan have been used to discover local network infrastructure devices and services running on remote hosts. Active Directory queries for remote systems have been performed by ADFind. |
| T1057 Process Discovery | Process Explorer, Process Monitor and PCHunter have been utilized to discover any anti-malware or monitoring software and terminate it. |

| | |
|---|---|
| T1082 System Information Discovery | LockBit 2.0 enumerates system information such as hostname, shares, and domain information. |
| T1614 System Location Discovery | Attempts to check the language settings. |
| TA00008 Lateral Movement | |
| T1021 Remote Services | Although Cobalt Strike has many capabilities beneficial to threat actors in ransomware attacks, it was mainly seen in LockBit 2.0 investigations acting as a command and control beacon, a method of lateral movement and a tool for downloading/executing files. |
| T1021.002 Remote Services: SMB/Windows Admin Shares | LockBit 2.0 has been known to self-propagate via SMB. |
| TA0010 Exfiltration | |
| T1030 Data Transfer Size Limits | In some cases, LockBit 2.0 will limit the data transfer sizes to fly under the radar of any monitoring services a client may have set up. |
| T1041 Exfiltration over C2 Channel | MEGASync is the leading way for LockBit 2.0 affiliates to exfiltrate data from clients with it being occasionally replaced by RClone. |
| TA0011 Command and Control | |
| T1219 Remote Access Software | AnyDesk has been the most common legitimate desktop software used to establish an interactive command and control channel, with ConnectWise seen slightly less frequently. |
| TA0040 Impact | |
| T1486 Data Encrypted for Impact | LockBit 2.0 is known for its extortion tactics, encrypting devices and demanding a ransom. |
| T1489 Service Stop | During the defense evasion phase, anti-malware and monitoring software is often disabled. Firewall rules have occasionally been seen being disabled as well. |

LockBit 2.0 Technical Details

LockBit 2.0 was developed using the Assembly and Origin C programming languages and leverages advanced encryption standard (AES) and elliptic-curve cryptography (ECC) algorithms to encrypt victim data. It can affect both Windows and Linux OS, as the operator released a Linux version of LockBit 2.0 to target VMware ESXi hypervisor systems in October 2021, coded exclusively in the C programming language.

The LockBit group claimed that LockBit 2.0 is “the fastest encryption software all over the world” and provided a comparative table showing the encryption speed of various ransomware samples.

| Encryption speed comparative table for some ransomware - 02.08.2021 | | | | | | | |
|---|---------------------|-------------------------------|-------------------------------------|------------------------------------|-------------|-------------------|---|
| PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD | | | | | | | |
| Name of the ransomware | Date of a sample | Speed in megabytes per second | Time spent for encryption of 100 GB | Time spent for encryption of 10 TB | Self spread | Size sample in KB | The number of the encrypted files (All file in a system 257472) |
| LOCKBIT 2.0 | 5 Jun, 2021 | 373 MB/s | 4M 28S | 7H 26M 40S | Yes | 855 KB | 109964 |
| LOCKBIT | 14 Feb, 2021 | 266 MB/s | 6M 16S | 10H 26M 40S | Yes | 146 KB | 110029 |
| Cuba | 8 Mar, 2020 | 185 MB/s | 9M | 15H | No | 1130 KB | 110468 |
| BlackMatter | 2 Aug, 2021 | 185 MB/s | 9M | 15H | No | 67 KB | 111018 |
| Babuk | 20 Apr, 2021 | 166 MB/s | 10M | 16H 40M | Yes | 79 KB | 109969 |
| Sodinokibi | 4 Jul, 2019 | 151 MB/s | 11M | 18H 20M | No | 253 KB | 95490 |
| Ragnar | 11 Feb, 2020 | 151 MB/s | 11M | 18H 20M | No | 40 KB | 110651 |
| NetWalker | 19 Oct, 2020 | 151 MB/s | 11M | 18H 20M | No | 902 KB | 109892 |
| MAKOP | 27 Oct, 2020 | 138 MB/s | 12M | 20H | No | 115 KB | 111002 |
| RansomEXX | 14 Dec, 2020 | 138 MB/s | 12M | 20H | No | 156 KB | 109700 |
| Pysa | 8 Apr, 2021 | 128 MB/s | 13M | 21H 40M | No | 500 KB | 108430 |
| Avaddon | 9 Jun, 2020 | 119 MB/s | 14M | 23H 20M | No | 1054 KB | 109952 |
| Thanos | 23 Mar, 2021 | 119 MB/s | 14M | 23H 20M | No | 91 KB | 81081 |
| Ranzy | 20 Dec, 2020 | 111 MB/s | 15M | 1D 1H | No | 138 KB | 109918 |
| PwndLocker | 4 Mar, 2020 | 104 MB/s | 16M | 1D 2H 40M | No | 17 KB | 109842 |
| Sekhmet | 30 Mar, 2020 | 104 MB/s | 16M | 1D 2H 40M | No | 364 KB | random extension |
| Sun Crypt | 26 Jan, 2021 | 104MB/s | 16M | 1D 2H 40M | No | 1422 KB | random extension |
| REvil | 8 Apr, 2021 | 98 MB/s | 17M | 1D 4H 20M | No | 121 KB | 109789 |
| Conti | 22 Dec, 2020 | 98 MB/s | 17M | 1D 4H 20M | Yes | 186 KB | 110220 |
| Hive | 17 Jul, 2021 | 92 MB/s | 18M | 1D 6H | No | 808 KB | 81797 |
| Ryuk | 21 Mar, 2021 | 92 MB/s | 18M | 1D 6H | Yes | 274 KB | 110784 |
| Zeppelin | 8 Mar, 2021 | 92 MB/s | 18M | 1D 6H | No | 813 KB | 109963 |
| DarkSide | 1 May, 2021 | 83 MB/s | 20M | 1D 9H 20M | No | 30 KB | 100549 |
| DarkSide | 16 Jan, 2021 | 79 MB/s | 21M | 1D 11H | No | 59 KB | 100171 |
| Nephilim | 31 Aug, 2020 | 75 MB/s | 22M | 1D 12H 40M | No | 3061 KB | 110404 |
| DearCry | 13 Mar, 2021 | 64 MB/s | 26M | 1D 19H 20M | No | 1292 KB | 104547 |
| MountLocker | 20 Nov, 2020 | 64 MB/s | 26M | 1D 19H 20M | Yes | 200 KB | 110367 |
| Nemty | 3 Mar, 2021 | 57 MB/s | 29M | 2D 0H 20M | No | 124 KB | 110012 |
| MedusaLocker | 24 Apr, 2020 | 53 MB/s | 31M | 2D 3H 40M | Yes | 661 KB | 109615 |
| Phoenix | 29 Mar, 2021 | 52 MB/s | 32M | 2D 5H 20M | No | 1930 KB | 110026 |
| Hades | 29 Mar, 2021 | 47 MB/s | 35M | 2D 10H 20M | No | 1909 KB | 110026 |
| DarkSide | 18 Dec, 2020 | 45 MB/s | 37M | 2D 13H 40M | No | 17 KB | 114741 |
| Babuk | 4 Jan, 2021 | 45 MB/s | 37M | 2D 13H 40M | Yes | 31 KB | 110760 |
| REvil | 7 Apr, 2021 | 37 MB/s | 45M | 3D 3H | No | 121 KB | 109790 |
| BlackKingdom | 23 Mar, 2021 | 32 MB/s | 52M | 3D 14H 40M | No | 12460 KB | random extension |
| Avos | 18 Jul, 2021 | 29 MB/s | 59M | 4D 2H | No | 402 KB | 79486 |

Figure 8. LockBit encryption comparative table | Source: LockBit blog.

LockBit 2.0 also contains a self-spreading feature, clears logs and can print the ransom note on network printers until the paper runs out.

A management panel that affiliates can use to manage victims and affiliate accounts, generate new ransomware builds and generate the decryptor if the demanded ransom is paid also exists.

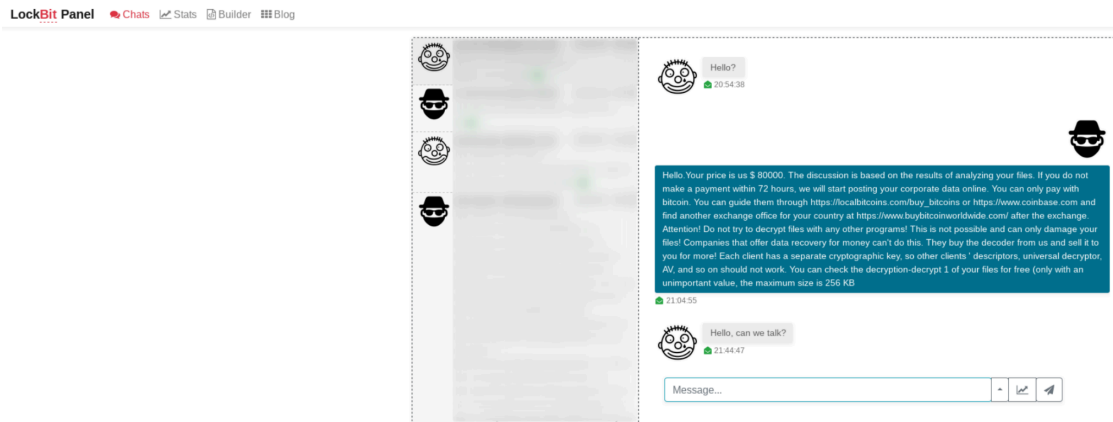


Figure 9. LockBit 2.0 management panel. Source: ProDaft.

LockBit 2.0 operators also released an information-stealer dubbed StealBit, which was developed to support affiliates of the LockBit 2.0 RaaS when exfiltrating data from breached companies.

StealBit contains the following capabilities:

- Operates as a file grabber and dumps/uploads victim data to the LockBit victim-shaming site.
- No reliance on third-party cloud file-sharing services, where data can be easily removed if the victim submitted a complaint.
- The download speed is limited only by internet connection bandwidth, so it is possible to clone folders from corporate networks and upload them to the LockBit victim shaming blog quickly.

The operator of LockBit 2.0 has provided a comparative table speed showing the information stealer compared to other tools.

| Comparative table of the information download speed of the attacked company | | | | | | | |
|---|-------------------------------|--------------------------|-------------|-------------|-------------------------------------|--------------------------------------|-------------------------------------|
| Testing was made on the computer with a speed of Internet of 1 gigabit per second | | | | | | | |
| Downloading method | Speed in megabytes per second | Compression in real time | Hidden mode | drag'n'drop | Time spent for downloading of 10 GB | Time spent for downloading of 100 GB | Time spent for downloading of 10 TB |
| Stealer - StealBIT | 83,46 MB/s | Yes | Yes | Yes | 1M 59S | 19M 58S | 1D 9H 16M 57S |
| Rclone pcloud.com free | 4,82 MB/s | No | No | No | 34M 34S | 5H 45M 46S | 24D 18M 8S |
| Rclone pcloud.com premium | 4,38 MB/s | No | No | No | 38M 3S | 6H 20M 31S | 26D 10H 11M 45S |
| Rclone mail.ru free | 3,56 MB/s | No | No | No | 46M 48S | 7H 48M 9S | 32D 12H 16M 28S |
| Rclone mega.nz free | 2,01 MB/s | No | No | No | 1H 22M 55S | 13H 48M 11S | 57D 13H 58M 44s |
| Rclone mega.nz PRO | 1,01 MB/s | No | No | No | 2H 45M | 1D 03H 30M 9S | 114D 14H 16M 30S |
| Rclone yandex.ru free | 0,52 MB/s | No | No | No | 5H 20M 30S | 2D 05H 25M 7S | 222D 13H 52M 49S |

Figure 10. LockBit 2.0 download speed, according to LockBit 2.0 operator.

LockBit 3.0

There was a bug that existed in LockBit 2.0 that allowed researchers to revert the encryption process on an MSSQL database. After the bug's disclosure, LockBit forum members discussed how the bug will not exist in LockBit's next iteration. Moreover, on March 17, LockBit forum members mentioned the release of LockBit's

next version in one or two weeks. On March 25, VX underground posted a [tweet](#) with details of this new version, dubbed LockBit Black.

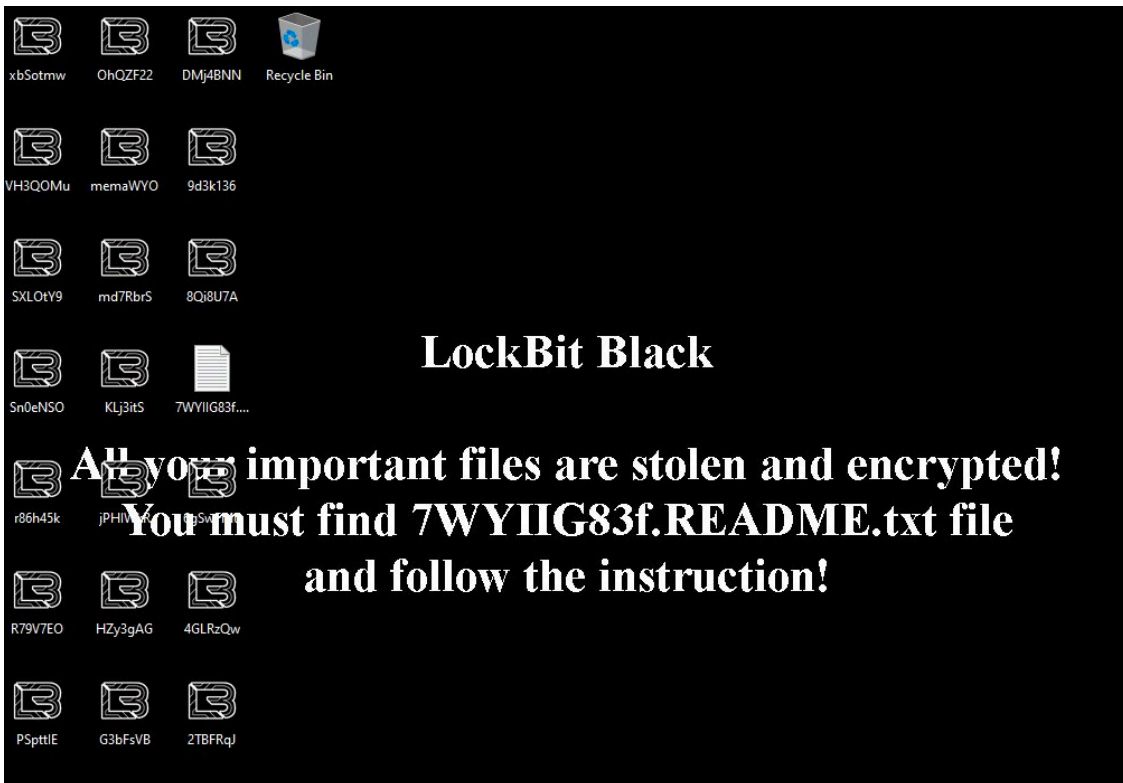


Figure 11. LockBit Black post-infection desktop wallpaper (Source: VX-underground).

Courses of Action

Several adversarial techniques were observed in this activity and the following measures are suggested within Palo Alto Networks products and services to ensure mitigation of threats related to LockBit 2.0 ransomware, as well as other malware using similar techniques:

| Product / Service | Course of Action |
|---|--|
| Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion | |
| The courses of action below mitigate the following techniques: Exploit Public-Facing Application [T1190], Command and Scripting Interpreter [T1059], Local Account [T1136.001], Web Shell [T1505.003], Exploitation for Privilege Escalation [T1068], Indicator Removal on Host [T1070], Deobfuscate/Decode Files or Information [T1140], Disable or Modify Tools [T1562.001], Hidden Window [T1564.003], Valid Accounts [T1078], External Remote Services [T1133], Scheduled Task [T1053.005], Bypass User Account Control [T1548.002], Group Policy Modification [T1484.001] | |
| THREAT PREVENTION | Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic |

| | |
|---------------------------|--|
| | <p>Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities</p> <p>Ensure DNS sinkholing is configured on all anti-spyware profiles in use</p> <p>Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats</p> <p>Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the internet</p> <p>Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use</p> |
| CORTEX XSOAR | <p>Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint</p> <p>Deploy XSOAR Playbook - Block Account Generic</p> <p>Deploy XSOAR Playbook - Access Investigation Playbook</p> <p>Deploy XSOAR Playbook - Impossible Traveler</p> |
| NEXT-GENERATION FIREWALLS | <p>Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist</p> <p>Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone</p> <p>Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists</p> <p>Ensure that the User-ID service account does not have interactive logon rights</p> <p>Define at least one 'Include Network'.</p> <p>Ensure that User-ID is only enabled for internal trusted interfaces</p> <p>Ensure that 'Include/Exclude Networks' is used if User-ID is enabled</p> <p>Ensure remote access capabilities for the User-ID service account are forbidden.</p> <p>Ensure that the User-ID Agent has minimal permissions if User-ID is enabled</p> |
| CORTEX XDR PREVENT | <p>Enable Anti-Malware Protection</p> <p>Enable Anti-Exploit Protection</p> <p>Configure Host Firewall Profile</p> |

| | |
|---|--|
| | Configure Behavioral Threat Protection under the Malware Security Profile |
| Credential Access | |
| <p>The courses of action below mitigate the following techniques:</p> <p>OS Credential Dumping [T1003], Credentials from Password Stores [T1555]</p> | |
| CORTEX XDR PREVENT | Enable Anti-Exploit Protection |
| | Enable Anti-Malware Protection |
| Discovery | |
| <p>The below courses of action mitigate the following techniques:</p> <p>Network Service Scanning [T1046], Process Discovery [T1057], System Location Discovery [T1614], System Information Discovery [T1082]</p> | |
| CORTEX XDR PREVENT | Configure Behavioral Threat Protection under the Malware Security Profile |
| NEXT-GENERATION FIREWALLS | Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions |
| | Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist |
| | Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists |
| | Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone |
| CORTEX XSOAR | Deploy XSOAR Playbook - Port Scan |
| Lateral Movement | |
| <p>The courses of action below mitigate the following techniques:</p> <p>Remote Services [T1021], SMB/Windows Admin Shares [T1021.002]</p> | |
| NEXT-GENERATION FIREWALLS | Ensure remote access capabilities for the User-ID service account are forbidden. |
| | Ensure that User-ID is only enabled for internal trusted interfaces |
| | Ensure that the User-ID Agent has minimal permissions if User-ID is enabled |

| | |
|--|---|
| | Ensure that the User-ID service account does not have interactive logon rights |
| | Ensure that 'Include/Exclude Networks' is used if User-ID is enabled |
| | Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones |
| CORTEX XSOAR | Deploy XSOAR Playbook - Block Account Generic |
| | Deploy XSOAR Playbook - Access Investigation Playbook |
| Command and Control | |
| The courses of action below mitigate the following techniques: | |
| Remote Access Software [T1219] | |
| NEXT-GENERATION FIREWALLS | Ensure that the Certificate used for Decryption is Trusted |
| | Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone |
| | Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists |
| | Ensure 'SSL Forward Proxy Policy' for traffic destined to the internet is configured |
| | Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS |
| | Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist |
| THREAT PREVENTION | Ensure DNS sinkholing is configured on all anti-spyware profiles in use |
| | Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use |
| | Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet |
| | Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3' |
| | Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats |
| | Ensure a secure antivirus profile is applied to all relevant security policies |

| | |
|---|---|
| URL FILTERING | Ensure secure URL filtering is enabled for all security policies allowing traffic to the internet |
| | Ensure all HTTP Header Logging options are enabled |
| | Ensure that PAN-DB URL Filtering is used |
| | Ensure that URL Filtering uses the action of 'block' or 'override' on the URL categories |
| | Ensure that access to every URL is logged |
| CORTEX XSOAR | Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators |
| Exfiltration | |
| The courses of action below mitigate the following techniques: Data Transfer Size Limits [T1030], Exfiltration Over C2 Channel [T1041] | |
| THREAT PREVENTION | Ensure DNS sinkholing is configured on all anti-spyware profiles in use |
| | Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3' |
| | Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats |
| | Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use |
| | Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet |
| | Ensure a secure antivirus profile is applied to all relevant security policies |
| URL FILTERING | Ensure that PAN-DB URL Filtering is used |
| | Ensure that access to every URL is logged |
| | Ensure that URL Filtering uses the action of 'block' or 'override' on the URL categories |
| | Ensure secure URL filtering is enabled for all security policies allowing traffic to the internet |
| | Ensure all HTTP Header Logging options are enabled |
| CORTEX XSOAR | Deploy XSOAR Playbook - Block URL |

| | |
|---|---|
| | Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators |
| | Deploy XSOAR Playbook - Block IP |
| DNS SECURITY | Enable DNS Security in Anti-Spyware profile |
| NEXT-GENERATION FIREWALLS | Setup NetFlow Monitoring |
| | Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone |
| | Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist |
| | Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists |
| Impact | |
| The courses of action below mitigate the following techniques: Data Encrypted for Impact [T1486], Service Stop [T1489] | |
| CORTEX XSOAR | Deploy XSOAR Playbook - Ransomware Manual for incident response. |

†These capabilities are part of the NGFW security subscriptions service

Note: This is not an all-inclusive list of the protections provided by Palo Alto Networks. This is a subset of our current Courses of Action initiative and will be updated as the project progresses.

Conclusion

LockBit 2.0 and its evolution over time is a perfect example to illustrate the persistence, increasing complexity and impact brought by the ransomware landscape as a whole. With claims of this RaaS offering the fastest encryption on the ransomware market, coupled with the fact that it has been delivered in high volume by experienced affiliates, this RaaS poses a significant threat. LockBit’s continuation with operations and its next iteration coming up on the horizon means that organizations and their security teams need to stay vigilant in the ever-evolving threat landscape.

Palo Alto Networks detects and prevents LockBit 2.0 ransomware in the following ways:

- [WildFire](#): All known samples are identified as malware.
- [Cortex XDR](#):
 - Identifies indicators associated with LockBit 2.0.
 - Anti-Ransomware Module to detect LockBit 2.0 encryption behaviors on Windows.
 - Local Analysis detection for LockBit 2.0 binaries on Windows.
- [Next-Generation Firewalls](#): DNS Signatures detect the known C2 domains, which are also categorized as malware in [Advanced URL Filtering](#).

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

Appendix A

In August 2021, a Russian blogger published a 22-minute interview with an alleged representative of the group behind LockBit 2.0 called “LockBitSupp” on a YouTube channel called “[Russian-language open source intelligence \(OSINT\)](#).” The same Russian blogger previously published interviews with a representative of the group behind the REvil ransomware-as-a-service (RaaS), hackers and security experts.

Some key takeaways from the claims made in the interview were:

- The LockBit 2.0 threat actor claimed the group’s RaaS was unlikely to be rebranded since the team allegedly was a business that was honest with their customers – suggesting a supposed contrast between LockBit 2.0 and Avaddon, DarkSide and REvil affiliates.
- The LockBit 2.0 ransomware disregarded keyboard layout, but it allegedly would not run on a host where the system language was set to any of the languages spoken in the Commonwealth of Independent States region.
- The group did not devise attacks on companies of their choice; they simply worked with initial access to any corporate network they obtained elsewhere, since this was more profitable and saved time. The team selected targets for ransomware attacks based on the company’s finances — the bigger, the better. The location also did not matter. However, team members allegedly did not attack healthcare facilities, social services, educational institutions and charitable organizations or any other organization that “contributed to the survival of the human race.” [Note that Unit 42 case data does include indications that threat actors using LockBit 2.0 have targeted healthcare organizations at times.]
- The threat actor claimed that the largest number of victims who paid ransom were company representatives who did not care about creating backup copies and did not protect their sensitive data. According to the threat actor’s claims, companies that violated regulations about collecting and handling customer or user personal information were among those eager to pay. The threat actor claimed that there generally were only a few companies who refused to pay ransom on principle, while most of the victims evaluated profit and loss to decide whether or not to pay a ransom.
- LockBit 2.0 operators allegedly almost always offered discounts to their victims since the goal was to streamline attacks.
- The threat actor claimed that the COVID-19 pandemic facilitated ransomware attacks significantly, saying it was easy to compromise home computers of employees who work remotely and use them as a

springboard to access other networked systems.

- Companies in Europe and the U.S. were hit with ransomware much more often than companies based in other countries allegedly because of high profit and insurance and not because of language barriers.
- Ransomware operators usually recruit negotiators, who coerce victims to pay ransom, since professional penetration testers allegedly lack the time for chatter.

Table of Contents

-
- [Executive Summary](#)
- [LockBit 2.0 Overview](#)
 - [Victimology](#)
 - [Leak Site Data](#)
 - [Unit 42 Incident Response Data on LockBit 2.0](#)
- [LockBit 2.0 Tactics, Techniques and Procedures](#)
- [LockBit 2.0 Technical Details](#)
- [LockBit 3.0](#)
- [Courses of Action](#)
- [Conclusion](#)
- [Appendix A](#)
- [Additional Resources](#)

Related Articles

- [The Golden Scale: 'Tis the Season for Unwanted Gifts](#)
- [Threat Actor Groups Tracked by Palo Alto Networks Unit 42 \(Updated Aug. 1, 2025\)](#)
- [Threat Assessment: Repellent Scorpius, Distributors of Cicada3301 Ransomware](#)

 Enlarged Image

Source: <https://unit42.paloaltonetworks.com/lockbit-2-ransomware/>