Cybereason vs. LockBit2.0 Ransomware

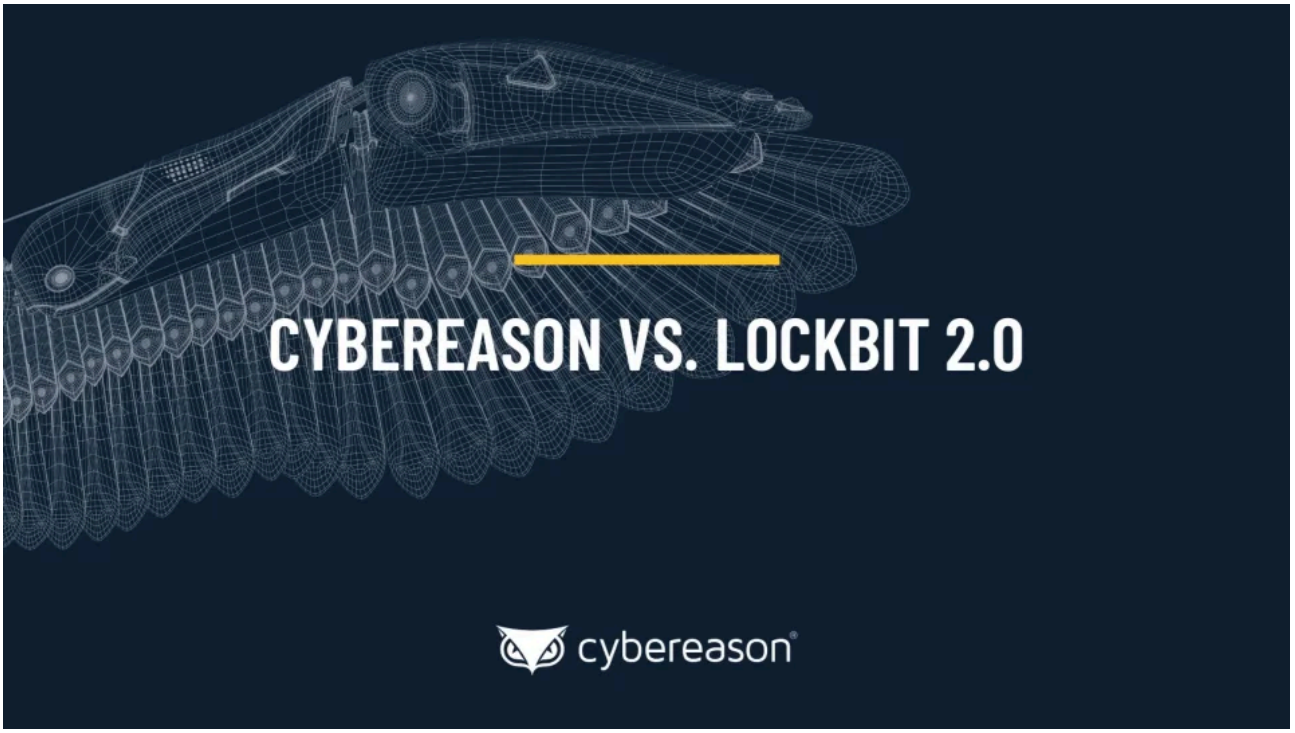
By Cybereason Nocturnus

Archived: 2026-04-05 20:22:19 UTC

The Cybereason Nocturnus team has been tracking the LockBit ransomware since it first emerged in September 2019 as a ransomware-as-a-service (RaaS). Following the rise of the new LockBit2.0 and the latest events, including the attack against the global IT company Accenture, we wanted to provide more information about the attack and show how the Cybereason Defense Platform protects customers from this threat.

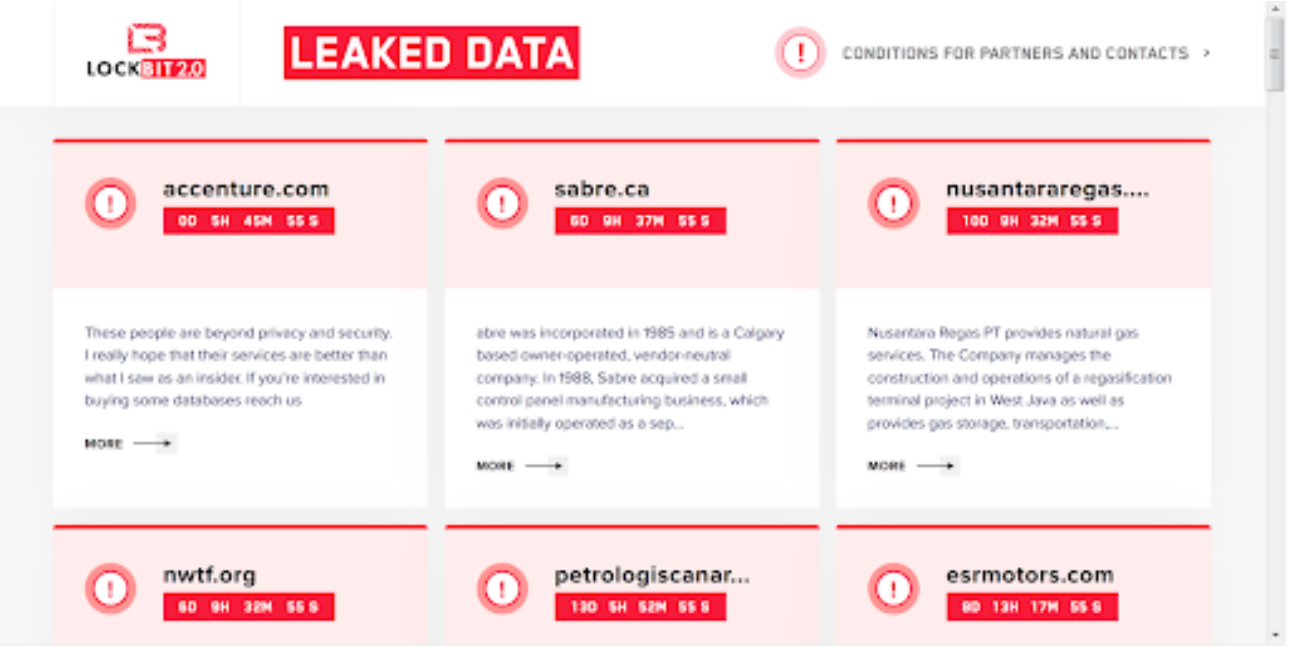
LockBit2.o Ransomware Key Details:

- **Emerging Threat**: In a short amount of time, Lockbit2.0 ransomware caused great damage and made headlines across the world, with over 40 known victims on their website.
- **High Severity**: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
- **The fastest encryption on the market**: The group claims that both the LockBit2.0 ransomware and the StealBit info-stealer are the fastest on the market - in encrypting files and in stealing them.
- **Uses group policy update to encrypt network**: LockBit2.0 is the first ransomware to automate the process of executing the ransomware on the entire network with a single command.
- **Possibly triple extortion?**: The group claims to attack Accenture, one of its victims, using DDOS attacks daily.
- **Detected and Prevented**: The Cybereason Defense Platform fully detects and prevents the LockBit2.0 ransomware.



Cybereason Blocks LockBit2.0 Ransomware

In August 2021, the group published on their website that they have [breached the security company Accenture](), and threaten to publish their sensitive information and stolen data.



LockBit2.0 leaked data website

After a few days of not publishing the data stolen from them, and extending their countdown multiple times. The group added this sentence to Accenture's description: [“Dudos every day” -]() which might imply that they are conducting DDOS activity against Accenture to push them into paying the ransom fee. This tactic is not unique, different ransomware groups have adopted the [triple extortion]() trend, since (apparently) sometimes, [double extortion]() is not enough for them.

The LockBit group is suspected to be operated by Russian speakers. In the past, the group was recruiting affiliates in Russian hacking forums but since many hacking forums started to ban ransomware-related threads, the group started recruiting directly on their website. Similar to other Russian-based threat actors, they avoid targeting any victims in former Soviet states.

According to the LockBit group, LockBit2.0 is “the fastest encryption software all over the world,” and they are even sharing a test sample on their website, so everyone who “has any doubts” can check their claim:

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)

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

Encryption speed comparative table as shown in the LockBit2.0 blog

If you have any doubts concerning this table, you can easily check the provided information downloading the samples, which have been used for testing. Follow the link RansomwareSamples.7z

The ransomware test sample as shown in the LockBit2.0 blog

According to the group's website, there are major improvements in the new version of LockBit2.0, and addition of new features. Among the new features are: port scanner, using wake-on-lan to switch on turned off machines, print-out using network printers and automatic distribution in the domain, which puts corporates and small businesses in great danger:

Brief feature set:

- administrator panel in Tor system;
- communication with the company via Tor, chat room with PUSH notifications;
- automatic test decryption;
- automatic decryptor detection;
- port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;
- automatic distribution in the domain network at run-time without the necessity of scripts;
- termination of interfering services and processes;
- blocking of process launching that can destroy the encryption process;
- setting of file rights and removal of blocking attributes;
- removal of shadow copies;
- creation of hidden partitions, drag and drop files and folders;
- clearing of logs and self-clearing;
- windowed or hidden operating mode;
- launch of computers switched off via Wake-on-Lan;
- print-out of requirements on network printers;
- available for all versions of Windows OS;

List of features as shown in the LockBit2.0 blog

Same as other ransomware emerged over the years, the LockBit group follows the growing trend of double extortion (and sometimes even triple extortion, as mentioned above). They steal sensitive files and information from their victims, potentially by using another tool from their arsenal called StealBit, and later use it to extort the victims by threatening to publish the data unless the ransom is paid:

Along with the encrypting system, you get access to the fastest stealer all over the world - StealBit automatically downloading all files of the attacked company to our updated blog.

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

Introducing StealBit in the LockBit2.0 blog

Breaking Down the LockBit Ransomware Attack:

LockBit2.0 Ransomware Infection Vector

Since LockBit mostly relies on affiliates to carry out the operations, there are different infection vectors observed being used to infiltrate a network and install the ransomware. Most commonly seen method is through buying Remote Desktop Protocol (RDP) access to servers, but some affiliates also use typical phishing attacks to launch their operations.

Another interesting approach the LockBit group uses is trying to gain access to corporate networks by recruiting employees who can grant them insider access. They offer "millions of dollars" for corporate insiders who provide access to networks where they have an account. Since the message appears after the already breached the network, it is most likely targeting external IT/IR consultants who may see the message while responding to the attack, or other people reading about it:

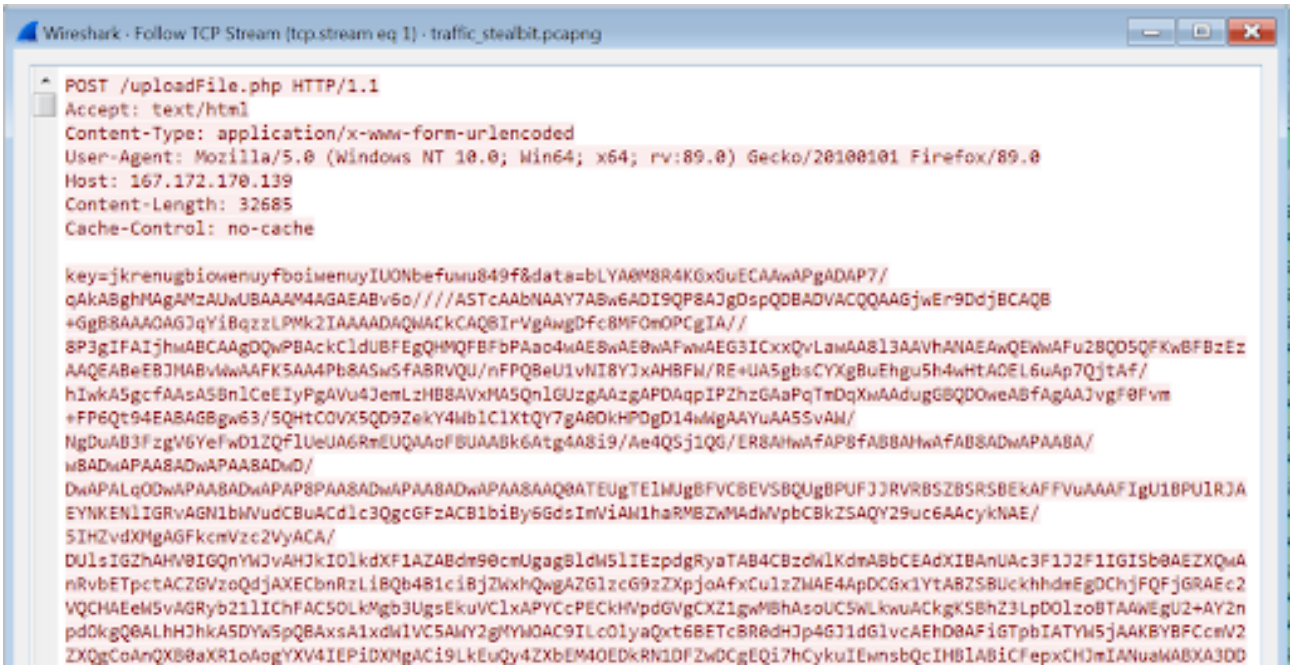
Part of the message targeting corporate insiders

LockBit2.0 Ransomware Data Exfiltrator

Once the ransomware operator or affiliate makes their way into a network, they begin to collect sensitive information and files and exfiltrate them. One tool that is used for this purpose, and is also offered to affiliates by the LockBit group, is a stealer they named “StealBit”, which, according to the group, is the fastest stealer in the world and it automatically downloads all the files to the LockBit blog:

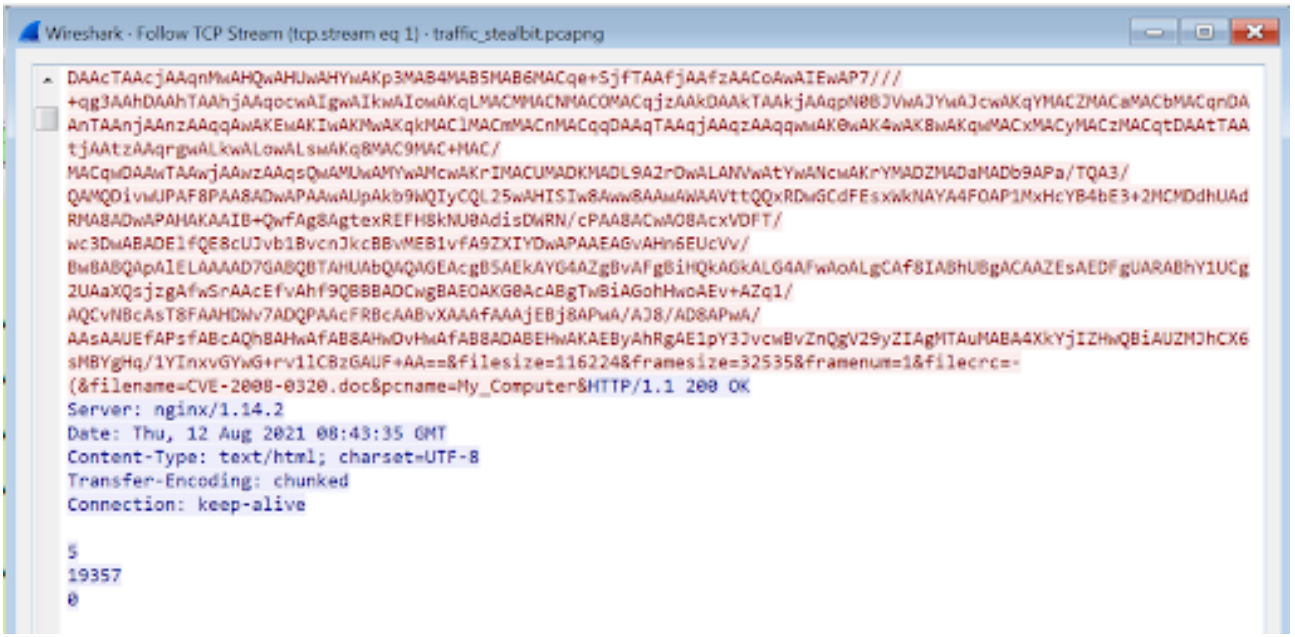
***PDB found**: E:\work\proj\file_sender\x64\file_sender.pdb*

First, the stealer collects information about the environment such as machine name, username, OS version, available disk space and physical and virtual memory status. The stealer enumerate the logical drives that are available on the victim's computer and recursively walk through the files in them and collects office documents files and pdf files, encrypts them send it to the server as “uploadFile.php” using HTTP POST method:



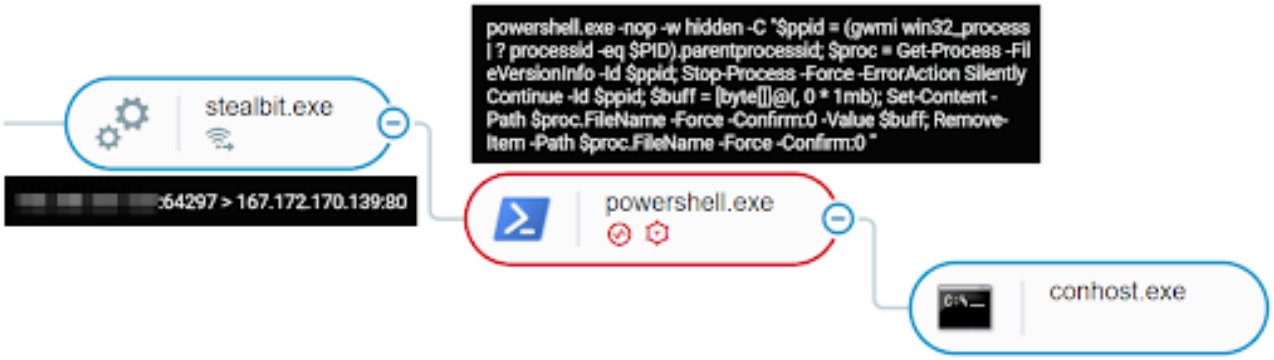
WireShark packet showing the communication with the C2 -1

Each file is added with information such as the file size, original file name and machine name:



WireShark packet showing the communication with the C2 -2

After exfiltrating the files, the stealer runs a PowerShell command that kills the malware's process and then deletes the malware file from the filesystem:



StealBit as shown in the Cybereason Defense Platform

LockBit2.0 Ransomware Spreading in the Network

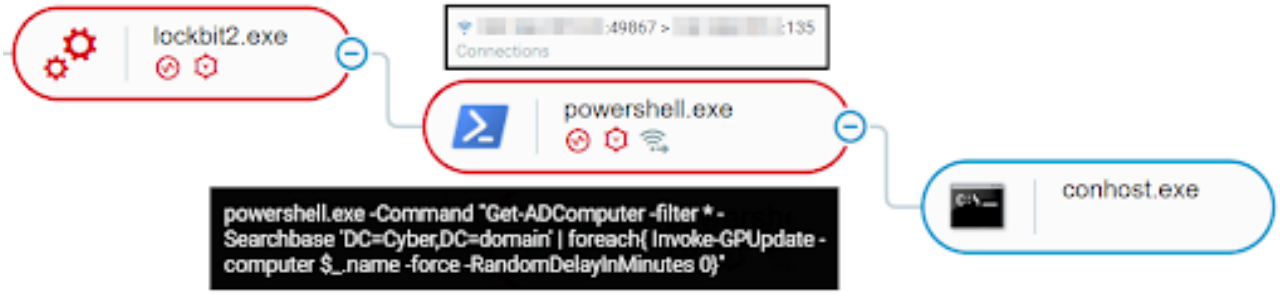
LockBit2.0 tries to spread via shared folders. It copies it's binary to remote machines and then executes it. In addition, the group mentioned on their website that they provide a port scanner to their affiliates that can detect all DFS, SMB, WebDav shares - which suggest other ways of spreading in the network.

LockBit2.0 Ransomware Uses Group Policy Update to Encrypt Network

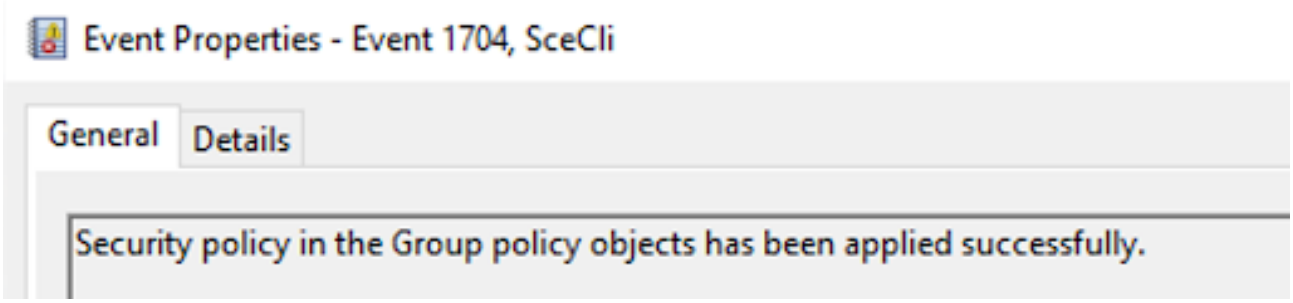
When executed on the Domain Controller, the ransomware has the ability to spread in the network using GPO.

First, the ransomware will query the Active Directory and create a list of machines to whom it will attempt to spread. For that it will perform LDAP queries and search for *objectCategory=computer*. Then, the ransomware will create several new group policies on the domain controller that are then pushed out to every device on the network using the following PowerShell command:

*PowerShell.exe -command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"*



LockBit2.0 execution as shown in the Cybereason Defense Platform



Windows Event log showing the creation of a new group policy object

One policy was created for disabling Microsoft Defender's real-time protection, alerts, submitting samples to Microsoft, and default actions when detecting malicious files:

```
[Software\Policies\Microsoft\Windows Defender
;DisableAntiSpyware
][Software\Policies\Microsoft\Windows Defender\Real-Time Protection
;DisableRealtimeMonitoring
][Software\Policies\Microsoft\Windows Defender\Spynet
;SubmitSamplesConsent
][Software\Policies\Microsoft\Windows Defender\Threats
;Threats_ThreatSeverityDefaultAction
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
][Software\Policies\Microsoft\Windows Defender\UX Configuration
;Notification_Suppress
```

Strings from memory - disabling Windows Defender

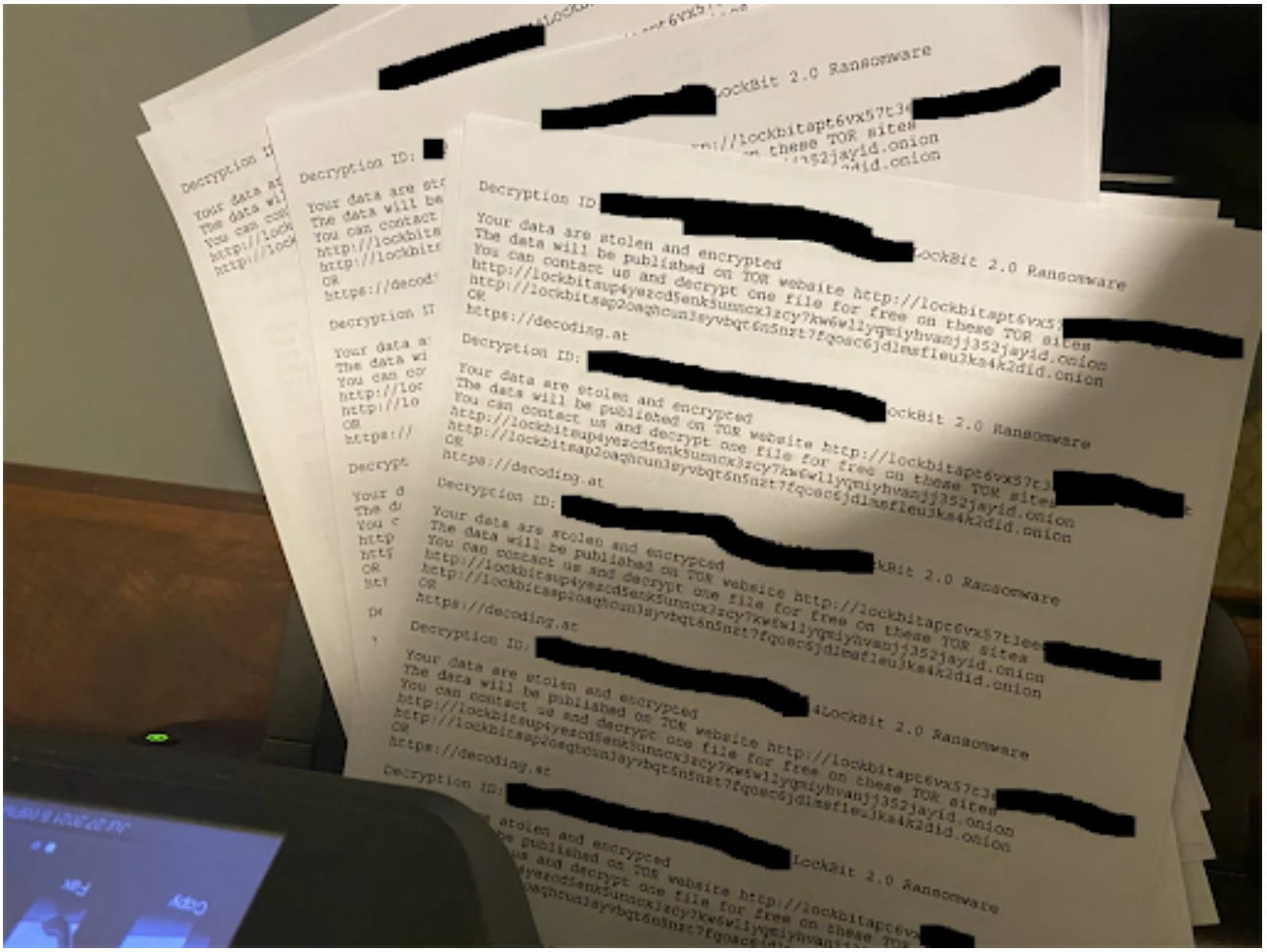
Another group policy was created for the purpose of spreading the ransomware binary and creating persistence on the remote machines to execute it via scheduled task:

```
ScheduledTasks
DisplayCalibrator
Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
```

Strings from memory - creation of a scheduled task named “DisplayClibrator”

LockBit2.0 Ransomware Print Bombing Network Printers

After LockBit has finished the encryption process, it starts to bomb the ransom note to all networked printers- repeatedly print the ransom note to any connected network printers to get the victim's attention. This feature was previously used by the Egregor Ransomware, which caused ransom notes to shoot out of receipt printers:



Printed ransom notes Source: BleepingComputer

LockBit2.0 Ransomware Encrypting the Files and Leaving the Ransom Note

Once the files are encrypted, the ransomware drops the ransom “Restore-My-Files.txt” note in every folder, making sure it is noticeable to the victim. In addition, the icons of the files are replaced with LockBit's icon and the extensions .lock and .lockbit are added to the encrypted files:

Encrypted files by LockBit2.0

To make sure that the end user wouldn’t miss the message, LockBit also start a process that is responsible to shows this message:

Pop-up message opened by LockBit2.0

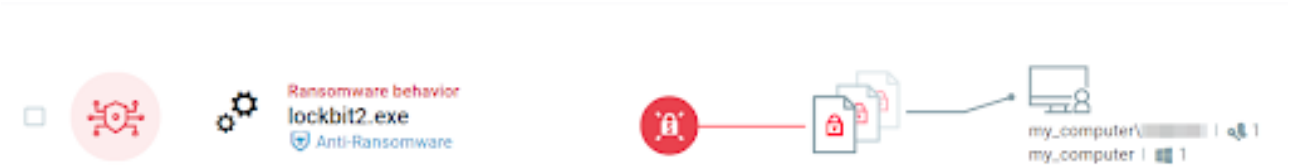
If, by any chance, the end user didn't see the pop-up message, the new files icons, the ransom notes, or the printed ransom notes, LockBit also changes the desktop background:

Desktop background changed by LockBit2.0

Finally, same as most of the ransomware gangs these days, LockBit sets a deadline for the victim to pay the ransom, and if the deadline passes without payment, they leak the victim data on their website.

Cybereason Detects and Prevents LockBit2.o Ransomware

The Cybereason Defense Platform is able to prevent the execution of LockBit2.0 Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a Malop™ for it:



Ransomware MalOp triggered due to the malicious activity

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), The Cybereason Defense Platform will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which prevents both known and unknown hashes:

User notification, blocking the execution of the ransomware in the endpoint

Security Recommendations

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - more information for customers can be found here
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information can be found here
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data

- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

INDICATORS OF COMPROMISE

Open the chatbot on the bottom right corner of this report to access the LockBit2.0 ransomware IOCs

MITRE ATT&CK TECHNIQUES

Initial Access	Lateral Movement	Persistence	Defense Evasion	Discovery	Command and Control	Impact
Phishing	Taint Shared Content	Scheduled Task/Job	Deobfuscate / Decode Files or Information	Account Discovery	Commonly Used Port	Data Encrypted for Impact
Valid Accounts	Lateral Tool Transfer	Boot or Logon Autostart Execution	Masquerading	Application Window Discovery	Remote File Copy	System Shutdown/Reboot
			Domain Policy Modification	File and Directory Discovery	Standard Application Layer Protocol	
				Process Discovery	Standard Cryptographic Protocol	
				System Information Discovery	Standard Non-Application Layer Protocol	

Author: LIOR ROCHBERGER, SENIOR THREAT RESEARCHER AND THREAT HUNTER, CYBEREASON

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus
