LockBit ransomware now encrypts Windows domains using group policies

bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/

Lawrence Abrams

By
Lawrence Abrams

- July 27, 2021
- 05:10 PM
- 1

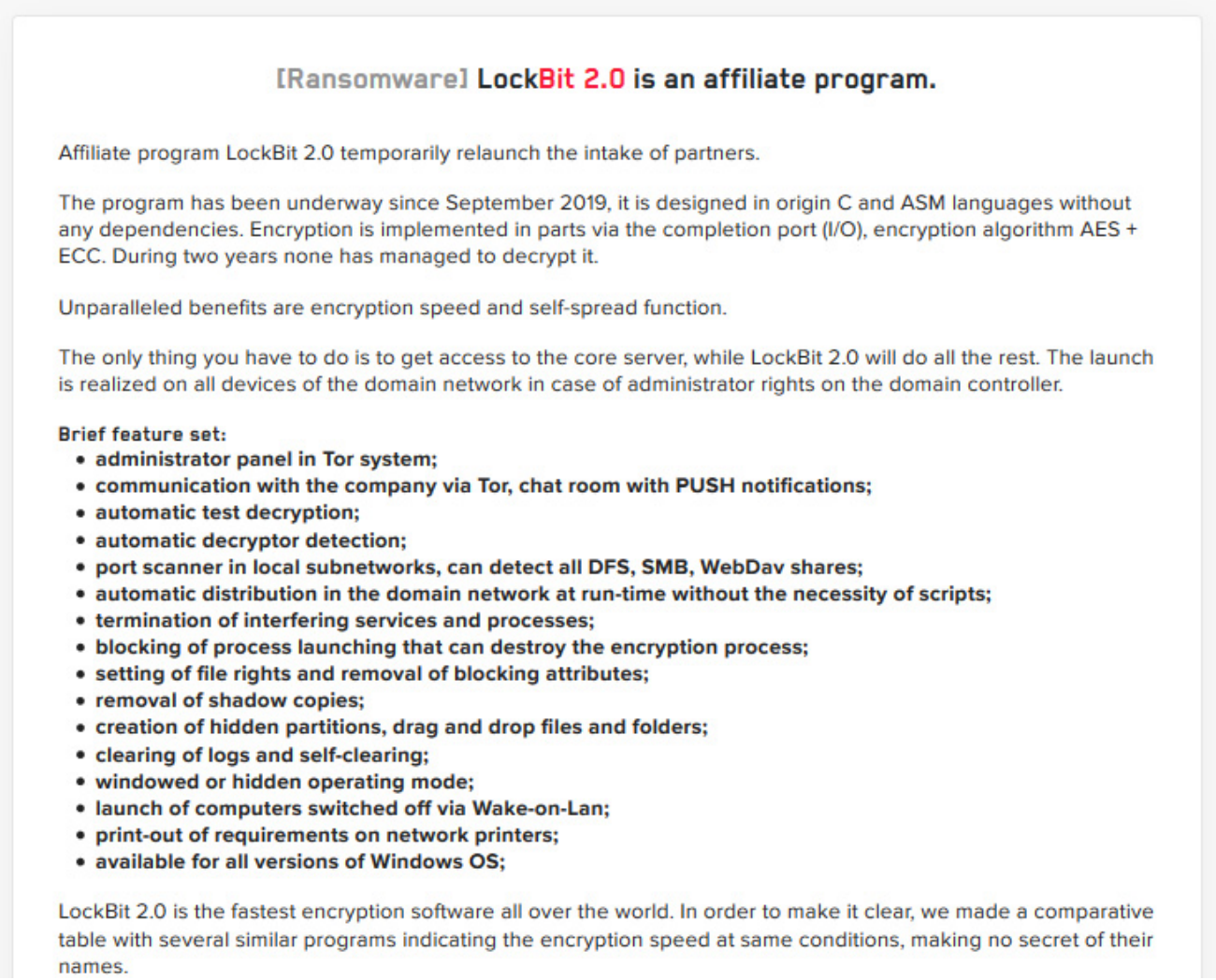
A new version of the LockBit 2.0 ransomware has been found that automates the encryption of a Windows domain using Active Directory group policies.

The LockBit ransomware operation launched in September 2019 as a ransomware-as-a-service, where threat actors are recruited to breach networks and encrypt devices.

In return, the recruited affiliates earn 70-80% of a ransom payment, and the LockBit developers keep the rest.

Over the years, the ransomware operation has been very active, with a representative of the gang promoting the activity and providing support on hacking forums.

After ransomware topics were banned on hacking forums [1, 2], LockBit began promoting the new LockBit 2.0 ransomware-as-a-service operation on their data leak site.



[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

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;

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.

LockBit 2.0 affiliate program features

Included with the new version of LockBit are numerous advanced features, with two of them outlined below.

Uses group policy update to encrypt network

LockBit 2.0 promotes a long list of features with many used by other ransomware operations in the past.

However, one promoted feature stuck out where the developers claim to have automated the ransomware distribution throughout a Windows domain without the need for scripts.

When threat actors breach a network and finally gain control of the domain controller, they utilize third-party software to deploy scripts that disable antivirus and then execute the ransomware on the machines on the network.

In samples of the LockBit 2.0 ransomware discovered by MalwareHunterTeam and analyzed by BleepingComputer and Vitali Kremez, the threat actors have automated this process so that the ransomware distributes itself throughout a domain when executed on a domain controller.

When executed, the ransomware will create new group policies on the domain controller that are then pushed out to every device on the network.

These policies disable Microsoft Defender's real-time protection, alerts, submitting samples to Microsoft, and default actions when detecting malicious files, as shown below.

```
[General]
Version=%s
displayName=%s
[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]
```

Other group policies are created, including one to create a scheduled task on Windows devices that launch the ransomware executable.

The ransomware will then run the following command to push the group policy update to all of the machines in the Windows domain.

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

Kremez told BleepingComputer that during this process, the ransomware will also use Windows Active Directory APIs to perform LDAP queries against the domain controller's ADS to get a list of computers.

Using this list, the ransomware executable will be copied to each device's desktop and the scheduled task configured by group policies will launch the ransomware using the UAC bypass below:

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

As the ransomware will be executed using a UAC bypass, the program will run silently in the background without any outward alert on the device being encrypted.

While MountLocker had previously used Windows Active Directory APIs to perform LDAP queries this is the first time we have seen a ransomware automate the distribution of the malware via group policies.

"This is the first ransomware operation to automate this process, and it allows a threat actor to disable Microsoft Defender and execute the ransomware on the entire network with a single command," Kremez told BleepingComputer.

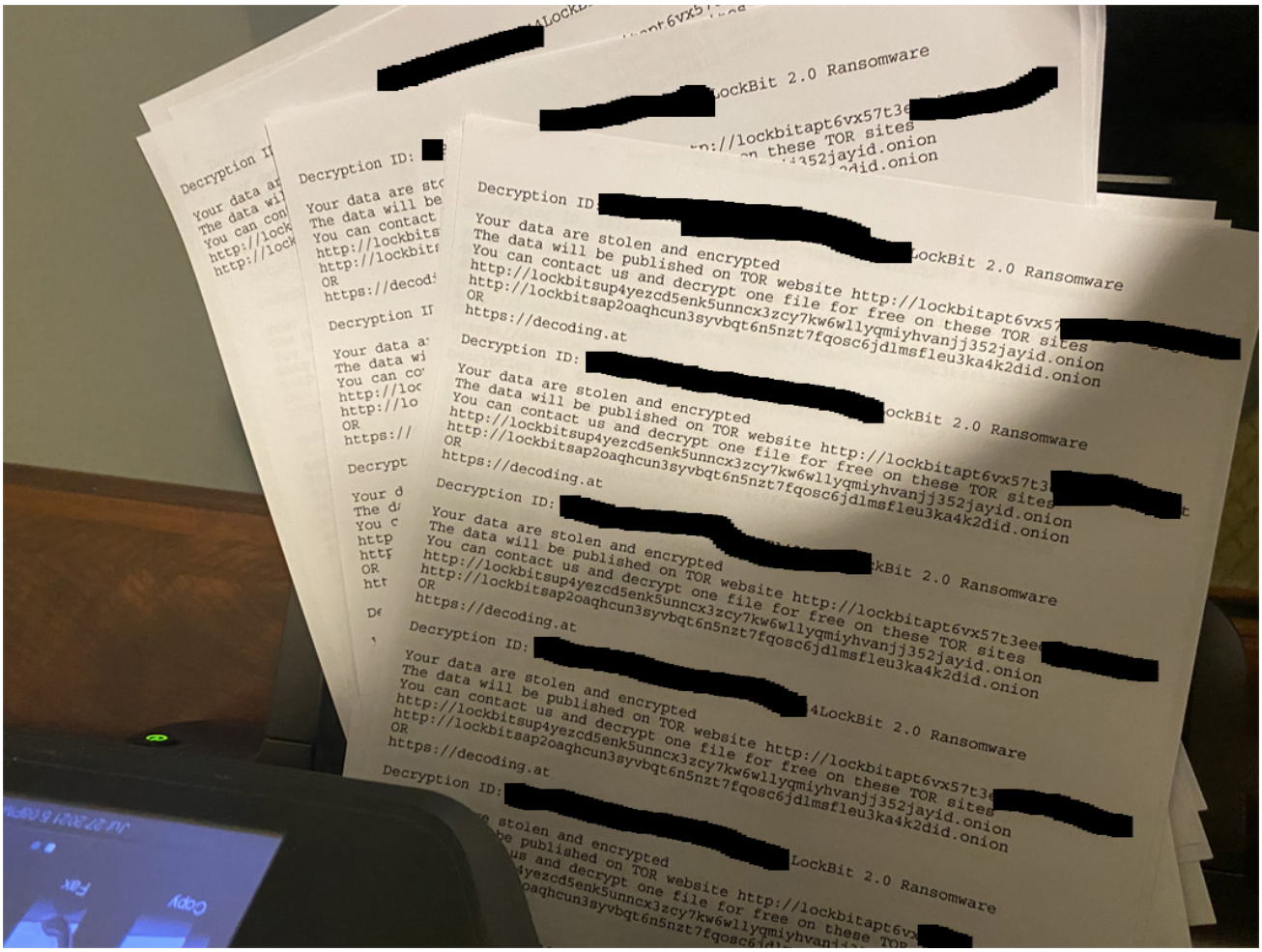
"A new version of the LockBit 2.0 ransomware has been found that automates the interaction and subsequent encryption of a Windows domain using Active Directory group policies."

"The malware added a novel approach of interacting with active directory propagating ransomware to local domains as well as built-in updating global policy with anti-virus disable making "pentester" operations easier for new malware operators."

LockBit 2.0 print bombs network printers

LockBit 2.0 also includes a feature previously used by the Egregor Ransomware operation that print bombs the ransom note to all networked printers.

When the ransomware has finished encrypting a device, it will repeatedly print the ransom note to any connected network printers to get the victim's attention, as shown below.



Print bomb of ransom notes

In an Egregor attack against retail giant Cencosud, this feature caused ransom notes to shoot out of receipt printers after they conducted the attack.

Related Articles:

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

Online library app Onleihe faces issues after cyberattack on provider

The Week in Ransomware - April 15th 2022 - Encrypting Russia

LockBit ransomware gang lurked in a U.S. gov network for months

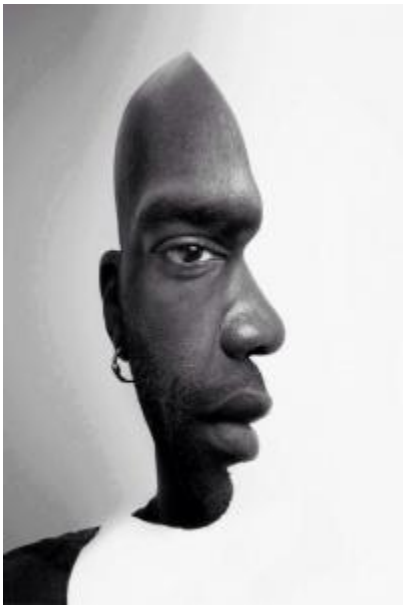
- Domain Controller
- Group Policy
- LockBit
- LockBit 2.0
- Ransomware
- Windows Domain

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments



xXHelperXx - 9 months ago

-
-

This is a serious ransomware. They get better and better every year.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: