

Analysis and Impact of LockBit Ransomware's First Linux and VMware ESXi Variant

trendmicro.com/en_us/research/22/a/analysis-and-impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html

January 24, 2022



In our monitoring of the LockBit ransomware's intrusion set, we found an announcement for LockBit Linux-ESXi Locker version 1.0 on October 2021 in the underground forum "RAMP," where potential affiliates can find it. This signifies the LockBit ransomware group's efforts to expand its targets to Linux hosts. Since October, we have been seeing samples of this variant in the wild.

This variant could have a big impact on victim organizations because of how ESXi, VMware's hypervisor helps in managing servers.

Analysis of the variant

Lockbit Linux-ESXi Locker version 1.0 uses a combination of Advanced Encryption Standard (AES) and elliptic-curve cryptography (ECC) algorithms for data encryption. From our analysis, we can see that this version of LockBit can accept parameters, as detailed in Figure 1.

```
Usage: %s [OPTION]... -i '/path/to/crypt'
Recursively crypts files in a path or by extention.

Mandatory arguments to long options are mandatory for short options too.
-i, --indir          path to crypt
-m, --minfile        minimal size of a crypted file, no less than 4096
-r, --remove         self remove this file after work
-l, --log            prints the log to the console
-n, --nolog          do not print the log to the file /tmp/locker.log
-d, --daemonize      runs a program as Unix daemon
-w, --wholefile      encrypts whole file
-b, --beginfile      encrypts first N bytes
-e, --extensions     encrypts files by extentions
-o, --nostop         prevent to stop working VM
-p, --wipe           wipe free space
-s, --spot           upper bound limitation value of spot in Mb
```

Figure 1. Parameters accepted by the Linux-ESXi version of LockBit

This version of the ransomware has logging capabilities and can log the following information:

- Processor information
- Volumes in the system
- Virtual machines (VMs) for skipping
- Total files
- Total VMs
- Encrypted files
- Encrypted VMs
- Total encrypted size
- Time spent for encryption

This variant also contains commands necessary for encrypting VM images hosted on ESXi servers, as listed in Table 1.

Command	Description
vm-support --listvms	Obtain a list of all registered and running VMs
esxcli vm process list	Get a list of running VMs
esxcli vm process kill --type force --world-id	Power off the VM from the list
esxcli storage filesystem list	Check the status of data storage
/sbin/vmdumper %d suspend_v	Suspend VM
vim-cmd hostsvc/enable_ssh	Enable SSH

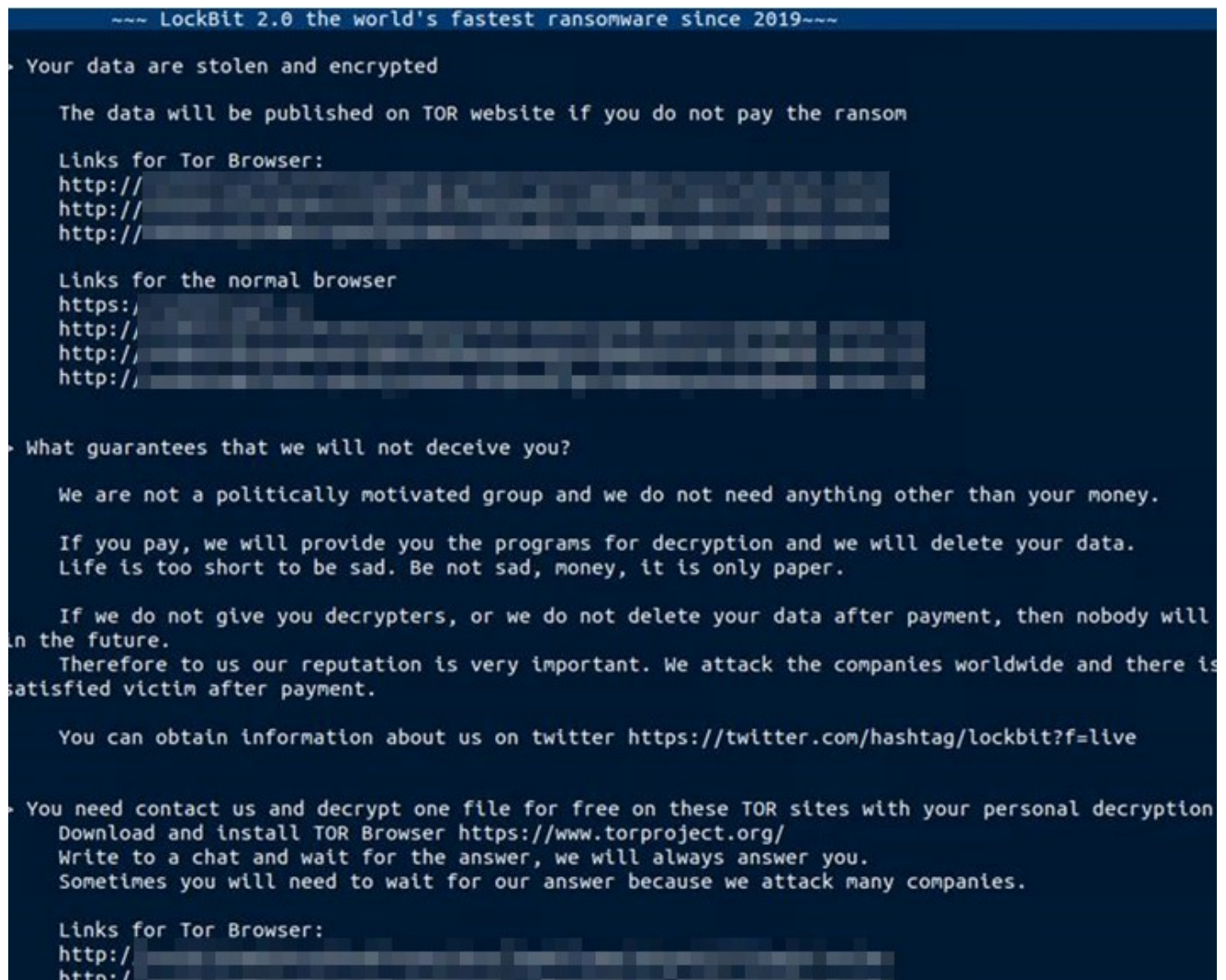
**vim-cmd
hostsvc/autostartmanager/enable_autostart
false**

Disable autostart

vim-cmd hostsvc/hostsummary grep cpuModel Determine ESXi CPU model

Table 1. Commands for encrypting VM images hosted on ESXi servers

The ransom note is typical of LockBit attacks. It advertises the speed of LockBit 2.0, lists down the leak sites where the LockBit group threatens to publish stolen information, and ends with a recruitment ad for potential insiders enticing them with “millions of dollars” in exchange for access to valuable company data.



--- LockBit 2.0 the world's fastest ransomware since 2019---

Your data are stolen and encrypted

The data will be published on TOR website if you do not pay the ransom

Links for Tor Browser:
http://
http://
http://

Links for the normal browser
https://
http://
http://
http://

What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will
in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is
satisfied victim after payment.

You can obtain information about us on twitter <https://twitter.com/hashtag/lockbit?f=live>

You need contact us and decrypt one file for free on these TOR sites with your personal decryption
Download and install TOR Browser <https://www.torproject.org/>
Write to a chat and wait for the answer, we will always answer you.
Sometimes you will need to wait for our answer because we attack many companies.

Links for Tor Browser:
http://
http://


```
>>>> Advertisement

Would you like to earn millions of dollars $$$ ?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.

You can do it both using your work computer or the computer of any other employee in order to divert suspicion of being in collusion with us.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can contact us using Tox messenger without registration and SMS https://tox.chat/download.html.
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, write in jabber or tox.

Tox ID LockBitSupp: [REDACTED]
XMPP (Jabber) Support: [REDACTED]

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave browser

Links for Tor Browser:
http://\[REDACTED\]
http://\[REDACTED\]
http://\[REDACTED\]
```

Figure 2. A ransom note of the Linux-ESXi version of LockBit
LockBit's operators typically threaten to publish data they stole from their victims on their leak site once their targeted organizations have failed to comply with their ransom demands.

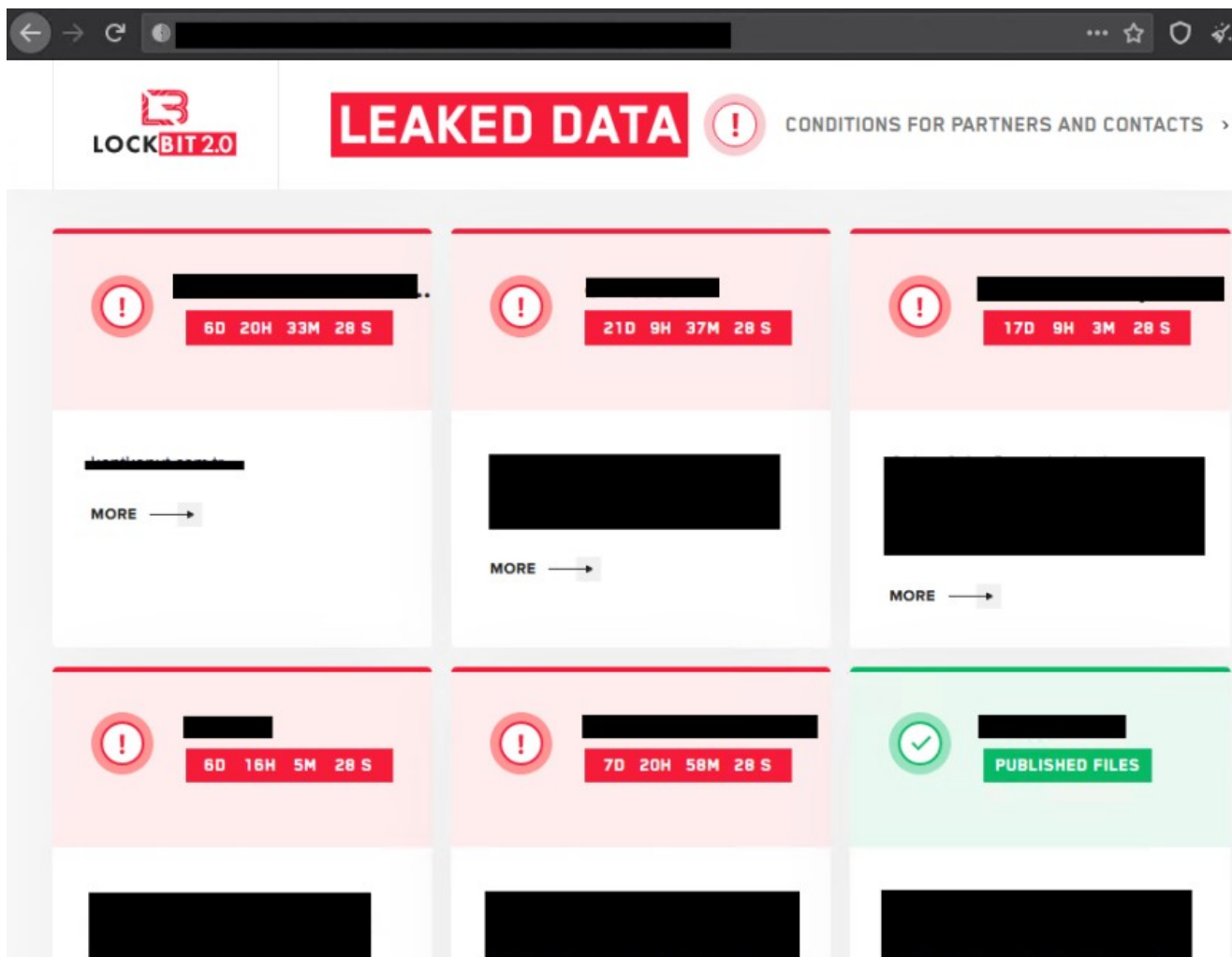


Figure 3. A screenshot of LockBit 2.0's leak site
Impact of the variant

The release of this variant is in line with how modern ransomware groups have been shifting their efforts to target and encrypt Linux hosts such as ESXi servers. An ESXi server typically hosts multiple VMs, which in turn hold important data or services for an organization. The successful encryption by ransomware of ESXi servers could therefore have a large impact on targeted companies. This trend was spearheaded by ransomware families like REvil and DarkSide.

Recommendations

ESXi offers organizations an easier way to manage their servers. But ransomware operators are also mirroring the transition of organizations to platforms such as ESXi. This development adds LockBit to the list of ransomware families capable of targeting Linux hosts in general and the ESXi platform in particular.

While Linux versions are typically harder to detect, implementing security best practices can still help organizations minimize the possibility of a successful attack. In the case of LockBit, keeping systems up to date can prevent intrusions. This is because LockBit has been known

to use access credentials stolen from vulnerable servers and sold in the cybercriminal underground. VMware also provides recommendations for enhancing the security of ESXi.

Organizations should also consider the following steps to mitigate ransomware threats:

- Deploy cross-layered detection and response solutions. Find solutions that can anticipate and respond to ransomware activities, techniques, and movements before the threat culminates. Trend Micro Vision One™, for example, helps detect and block ransomware components to stop attacks before they can affect an enterprise.
- Create a playbook for attack prevention and recovery. Both an incident response (IR) playbook and IR frameworks help organizations plan for different attacks.
- Conduct attack simulations. Expose employees to realistic cyberattack simulations that can help decision-makers, security personnel, and IR teams identify and prepare for potential security gaps and attacks.

Indicators of compromise (IOCs)

SHA256

- f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
- 67df6effa1d1d0690c0a7580598f6d05057c99014fcbfe9c225faae59b9a3224
- ee3e03f4510a1a325a06a17060a89da7ae5f9b805e4fe3a8c78327b9ecae84df

YARA rule:

```
rule Linux_Lockbit_Jan2022 {  
  meta:  
    description = "Detects a Linux version of Lockbit ransomware"  
    author = "TrendMicro Research"  
    date = "2022-01-24"  
    hash1 =  
"038ff8b2fef16f8ee9d70e6c219c5f380afe1a21761791e8cbda21fa4d09fdb4"  
    strings:  
      $xor_string_1 = "LockBit Linux/ESXi locker V:" xor(0x01-0xff)  
      $xor_string_2 = "LockBit 2.0 the world's fastest ransomware since 2019"  
xor(0x01-0xff)  
      $xor_string_3 = "Tox ID LockBitSupp" xor(0x01-0xff)  
    condition:  
      uint16(0) == 0x457f and filesize < 300KB and  
      filesize > 200KB and any of them  
}
```