Ransomware Groups to Watch: Emerging Threats

unit42.paloaltonetworks.com/emerging-ransomware-groups/

Doel Santos, Ruchna Nigam August 24, 2021

By Doel Santos and Ruchna Nigam

August 24, 2021 at 3:00 AM

Category: Malware, Ransomware, Unit 42

Tags: Avos, AvosLocker, Cybercrime, HelloKitty, Hive, Hive Leaks, LockBit 2.0

This post is also available in: 日本語 (Japanese)

Executive Summary

As part of Unit 42’s commitment to stop ransomware attacks, we conduct ransomware hunting operations to ensure our customers are protected against new and evolving ransomware variants. We monitor the activity of existing groups, search for dark web leak sites and fresh onion sites, identify up-and-coming players and study tactics, techniques and procedures. During our operations, we have observed four emerging ransomware groups that are currently affecting organizations and show signs of having the potential to become more prevalent in the future:

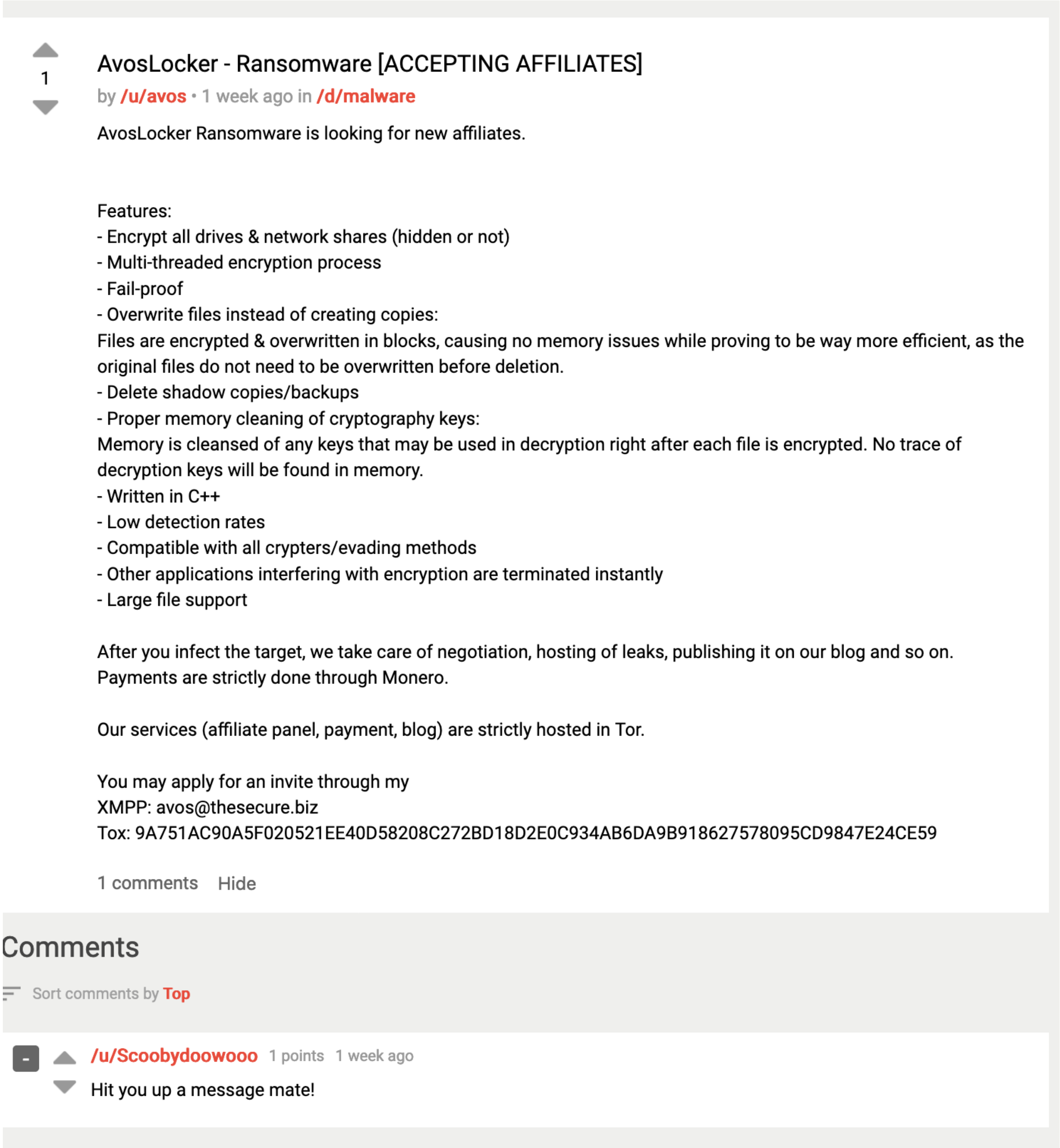
- AvosLocker is ransomware as a service (RaaS) that started operations in late June, using a blue beetle logo to identify itself in communications with victims and “press releases” aimed at recruiting new affiliates. AvosLocker was observed promoting its RaaS program and looking for affiliates on dark web discussion forums and other forums. Like many of its competitors, AvosLocker offers technical support to help victims recover after they’ve been attacked with encryption software that the group claims is “fail-proof,” has low detection rates and is capable of handling large files. This ransomware also has an extortion site, which claims to have impacted six organizations in the following countries: the U.S., the U.K., the U.A.E., Belgium, Spain and Lebanon. We have observed initial ransom demands ranging from $50,000 to $75,000.
- Hive Ransomware is double-extortion ransomware that started operations in June. Since then, Hive has impacted 28 organizations that are now listed on the group’s extortion site, including a European airline company and three U.S.-based organizations. Hive uses all tools available in the extortion toolset to create pressure on the victim, including the date of initial compromise, countdown, the date the leak was actually disclosed on their site, and even the option to share the disclosed leak on social media.
- HelloKitty is not a new ransomware group; it can be tracked as early as 2020, mainly targeting Windows systems. However, in July, we observed a Linux variant of HelloKitty targeting VMware’s ESXi hypervisor, which is widely used in cloud and on-premises data centers. We also observed two clusters of activity. Across the observed samples, some threat actors preferred email communications, while others used TOR chats for communication with the victims. The observed variants impacted five organizations in Italy, Australia, Germany, the Netherlands and the U.S. The highest ransom demand observed from this group was $10 million, but at the time of writing, the threat actors have only received three transactions that sum up to about $1.48 million.
- LockBit 2.0 (previously known as ABCD ransomware) is a three-year-old RaaS operator that has been linked to some high-profile attacks lately following the June launch of a slick marketing campaign to recruit new affiliates. It claims to offer the fastest encryption on the ransomware market. LockBit 2.0 has impacted multiple industries – 52 victims are listed on the group’s leak site. Its victims include organizations in the U.S., Mexico, Belgium, Argentina, Malaysia, Australia, Brazil, Switzerland, Germany, Italy, Austria, Romania and the U.K.

Here, we share information we've gathered from our observations of the behavior of these ransomware groups to help organizations defend against them.

Palo Alto Networks Next-Generation Firewall customers are protected from these threats with Threat Prevention and WildFire security subscriptions. Customers are also protected with Cortex XDR and can use AutoFocus for tracking related entities.

AvosLocker

AvosLocker is new ransomware that was first observed on July 4, 2021, and follows the RaaS model. The ransomware operator of the same name, avos, advertised their affiliate program on Dread (Figure 1). Dread is a Reddit-like dark web discussion forum featuring news and sub-dreads around darknet markets. The announcement of the program includes information about features of the ransomware and lets affiliates know that AvosLocker operators will take care of negotiation and extortion practices. The user Avos has also been observed trying to recruit individuals on the Russian forum XSS.



AvosLocker - Ransomware [ACCEPTING AFFILIATES]

by /u/avos • 1 week ago in /d/malware

AvosLocker Ransomware is looking for new affiliates.

Features:
- Encrypt all drives & network shares (hidden or not)
- Multi-threaded encryption process
- Fail-proof
- Overwrite files instead of creating copies:
Files are encrypted & overwritten in blocks, causing no memory issues while proving to be way more efficient, as the original files do not need to be overwritten before deletion.
- Delete shadow copies/backups
- Proper memory cleaning of cryptography keys:
Memory is cleansed of any keys that may be used in decryption right after each file is encrypted. No trace of decryption keys will be found in memory.
- Written in C++
- Low detection rates
- Compatible with all crypters/evading methods
- Other applications interfering with encryption are terminated instantly
- Large file support

After you infect the target, we take care of negotiation, hosting of leaks, publishing it on our blog and so on.
Payments are strictly done through Monero.

Our services (affiliate panel, payment, blog) are strictly hosted in Tor.

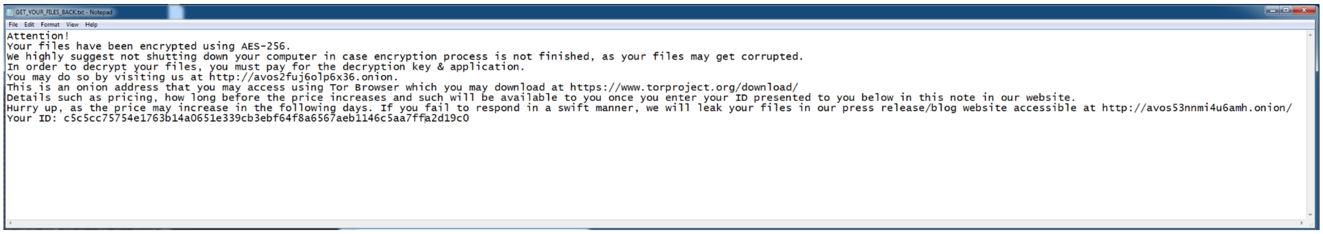
You may apply for an invite through my
XMPP: avos@thesecure.biz
Tox: 9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095CD9847E24CE59

/u/Scoobydoowooo 1 points 1 week ago

Hit you up a message mate!

Figure 1. AvosLocker announcement in Dread.AvosLocker, when executed, first opens a Windows shell showing the progress of the encryption process. After encryption is complete,

it then appends the .avos extension to the encrypted files and drops the ransom note GET_YOUR_FILES_BACK.TXT in every encrypted directory (Figure 2). We observed another AvosLocker sample that behaves exactly the same way as the initial observed sample, but also included a string called “Message from the agent” letting the victim know their files were exfiltrated.



```
Attention!
Your files have been encrypted using AES-256.
We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key & application.
You may do so by visiting us at http://avos2fuj6olp6x36.onion.
This is an onion address that you may access using Tor Browser which you may download at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.
Hurry up, as the price may increase in the following days. If you fail to respond in a swift manner, we will leak your files in our press release/blog website accessible at http://avos53nnmi4u6amh.onion/
Your ID: c5c5cc75754e1763b14a0651e339cb3ebf64f8a6567aeb1146c5aa7ffa2d19c0
```

Figure 2a. AvosLocker ransom note

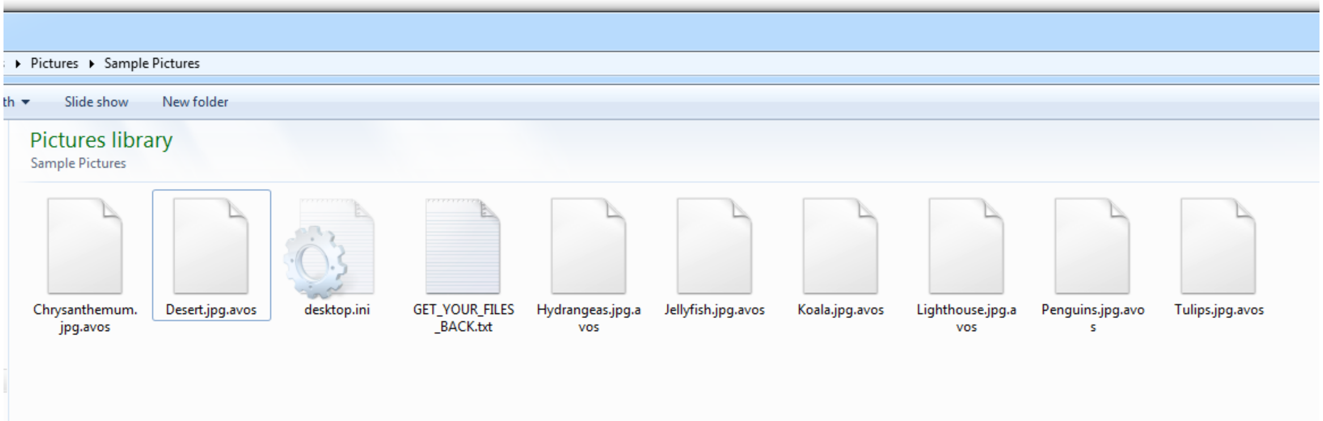
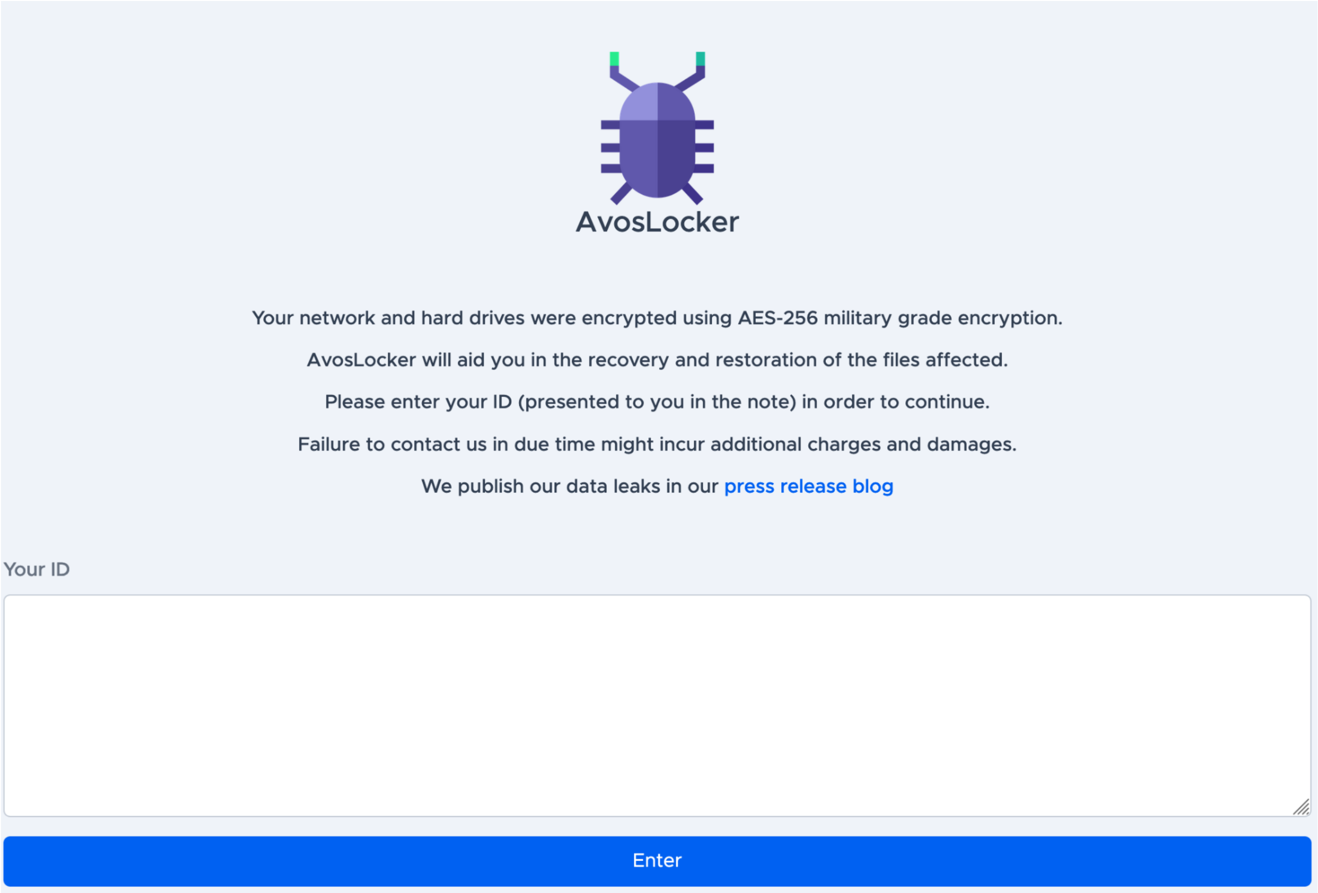


Figure 2b. Encrypted files.

The ransom note includes information and an ID used to identify victims, and instructs the victim to visit the AvosLocker TOR site (Figure 3).



Your network and hard drives were encrypted using AES-256 military grade encryption.

AvosLocker will aid you in the recovery and restoration of the files affected.

Please enter your ID (presented to you in the note) in order to continue.

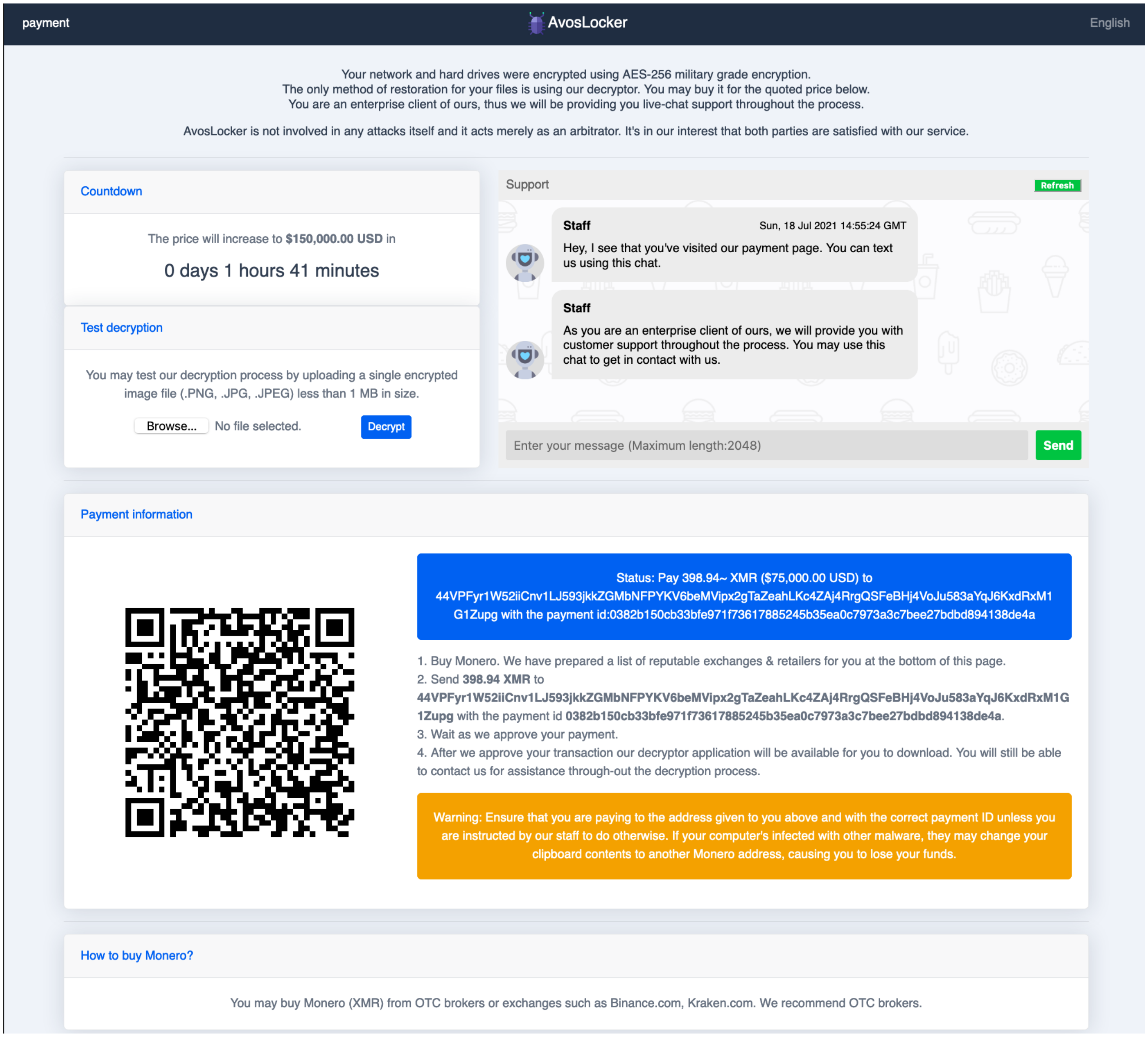
Failure to contact us in due time might incur additional charges and damages.

We publish our data leaks in our press release blog

Your ID

Figure 3. AvosLocker landing page.

After submitting the ID, the victim will encounter a support chat and the request for ransom. From the available instances observed, we have seen payment requests as low as $50,000 and as high as $75,000 in Monero (XMR). As seen with other ransomware groups, AvosLocker increases the ransom price if the victim doesn't pay in the designated time period, as shown in Figure 4.



Your network and hard drives were encrypted using AES-256 military grade encryption.
The only method of restoration for your files is using our decryptor. You may buy it for the quoted price below.
You are an enterprise client of ours, thus we will be providing you live-chat support throughout the process.

AvosLocker is not involved in any attacks itself and it acts merely as an arbitrator. It's in our interest that both parties are satisfied with our service.

The price will increase to **$150,000.00 USD** in

0 days 1 hours 41 minutes

You may test our decryption process by uploading a single encrypted image file (.PNG, .JPG, .JPEG) less than 1 MB in size.

Staff Sun, 18 Jul 2021 14:55:24 GMT

Hey, I see that you've visited our payment page. You can text us using this chat.

Staff

As you are an enterprise client of ours, we will provide you with customer support throughout the process. You may use this chat to get in contact with us.

Status: Pay 398.94~ XMR ($75,000.00 USD) to 44VPFyr1W52iiCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFeBHj4VoJu583aYqJ6KxdRxM1G1Zupg with the payment id:0382b150cb33bfe971f73617885245b35ea0c7973a3c7bee27bdbd894138de4a

1. Buy Monero. We have prepared a list of reputable exchanges & retailers for you at the bottom of this page.
2. Send **398.94 XMR** to **44VPFyr1W52iiCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFeBHj4VoJu583aYqJ6KxdRxM1G1Zupg** with the payment id **0382b150cb33bfe971f73617885245b35ea0c7973a3c7bee27bdbd894138de4a**.
3. Wait as we approve your payment.
4. After we approve your transaction our decryptor application will be available for you to download. You will still be able to contact us for assistance through-out the decryption process.

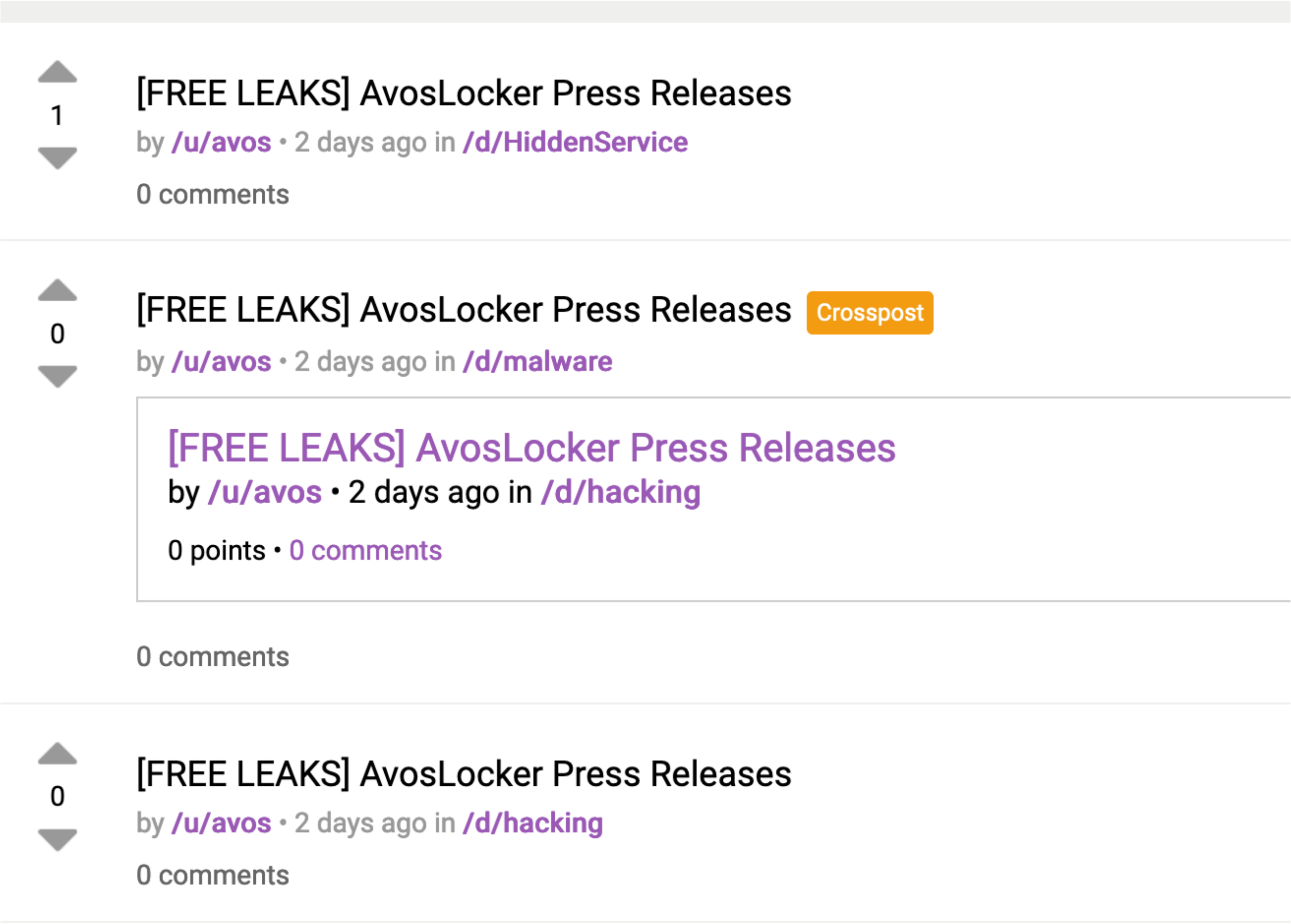
Warning: Ensure that you are paying to the address given to you above and with the correct payment ID unless you are instructed by our staff to do otherwise. If your computer's infected with other malware, they may change your clipboard contents to another Monero address, causing you to lose your funds.

You may buy Monero (XMR) from OTC brokers or exchanges such as Binance.com, Kraken.com. We recommend OTC brokers.

Figure 4. AvosLocker support page.

While exploring their site, we discovered that this group has already affected seven organizations: two law firms, one in the U.K. and one in the U.S.; a logistics company in Spain; a real estate agency in Belgium; a holdings company in Turkey; a Syrian transportation organization and a city in the U.S. Some of the leaked data displayed on their site include private organization documents and personal identifiable information.

AvosLocker's first site post, on Jan. 1, 2021, was an announcement that the site was officially online (Figure 5). The user avos also announced they started leaking data on multiple sub-dreads as well. We believe this was done to attract more affiliates and traffic to their site.



1

[FREE LEAKS] AvosLocker Press Releases

by /u/avos • 2 days ago in /d/HiddenService

0 comments

0

[FREE LEAKS] AvosLocker Press Releases Crosspost

by /u/avos • 2 days ago in /d/malware

[FREE LEAKS] AvosLocker Press Releases

by /u/avos • 2 days ago in /d/hacking

0 points • 0 comments

0 comments

0

[FREE LEAKS] AvosLocker Press Releases

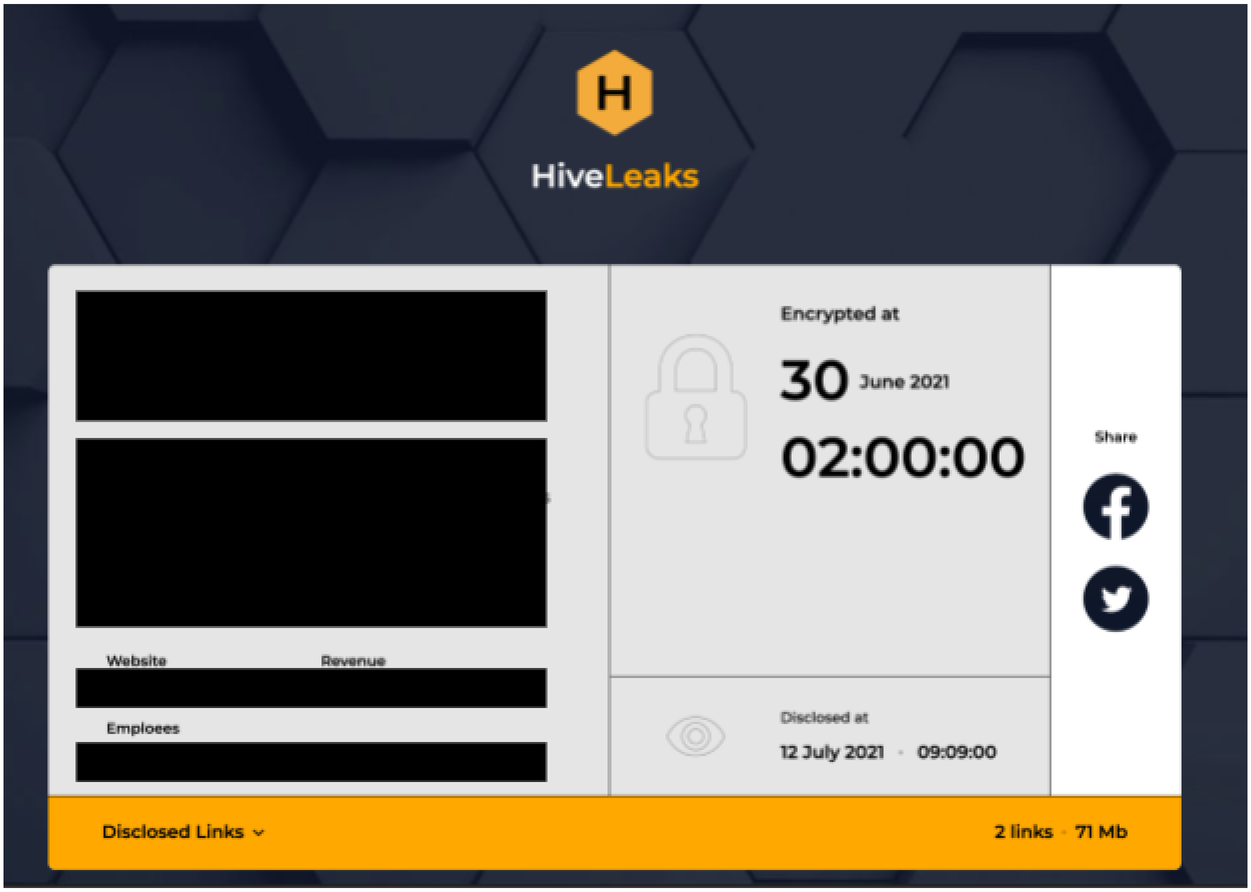
by /u/avos • 2 days ago in /d/hacking

0 comments

Figure 5. AvosLocker leak site and multiple advertisements on Dread.

Hive Ransomware

Hive ransomware began operations in June 2021 and has already shown notable disregard for its victims' welfare, attacking organizations including healthcare providers and mid-size organizations ill-equipped for managing a ransomware attack. Hive published their first victim on their leak site, Hive Leaks, in late June (Figure 6). Since then, 28 victims have been published on the Hive Leaks site, including a European airline company and three U.S.-based organizations, one each in hardware retail, manufacturing and law. The posts include the date and time the victim was affected.



HiveLeaks

[redacted]

[redacted]

Website Revenue

[redacted]

Emploees

[redacted]

Encrypted at

30 June 2021

02:00:00

Disclosed at

12 July 2021 · 09:09:00

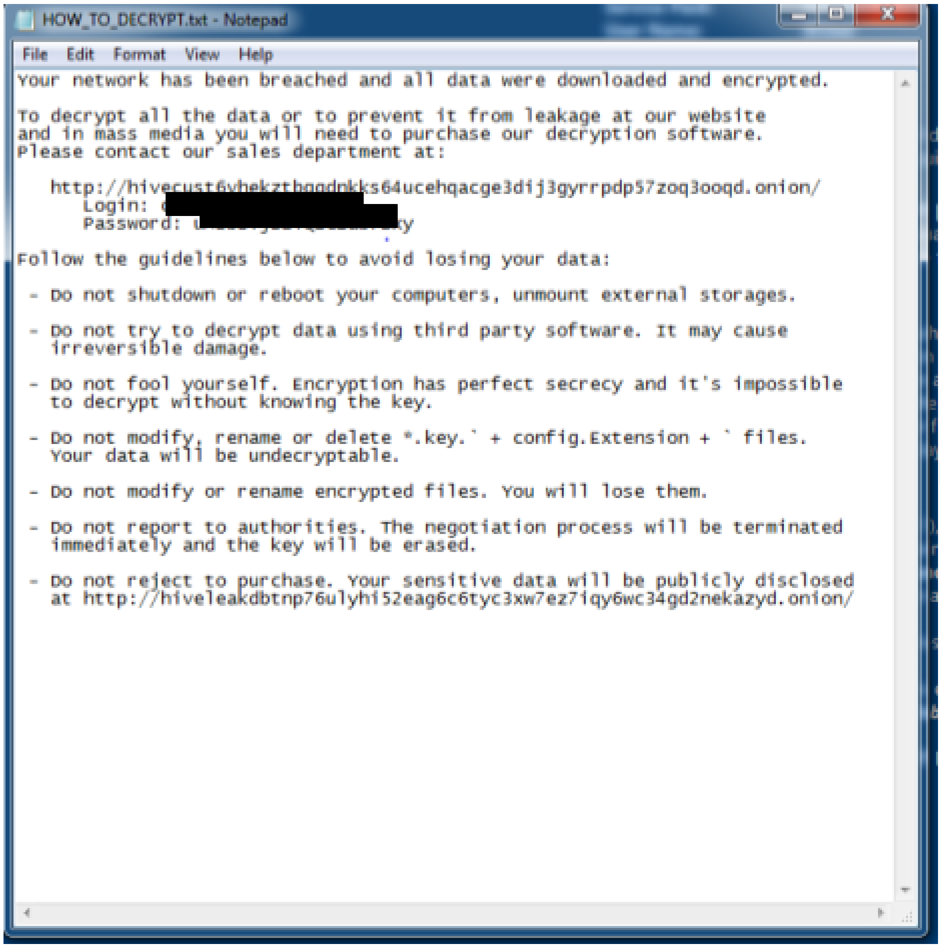
Share

Disclosed Links

2 links · 71 Mb

Figure 6. Hive Leaks.

When this ransomware is executed, it drops two batch scripts. The first script, hive.bat, tries to delete itself, and the second script is in charge of deleting the shadow copies of the system (shadow.bat). Hive ransomware adds the [randomized characters].hive extension to the encrypted files and drops a ransom note titled HOW_TO_DECRYPT.txt containing instructions and guidelines to prevent data loss (Figure 7). The ransom note includes a generated login credential for the victim to chat with what the threat actors claim is their “sales” department. The TOR link directs the “customer” to a login page, and after the credentials are submitted, it opens up a chat room for communication between the operators and the victim (Figure 8).



```
Your network has been breached and all data were downloaded and encrypted.

To decrypt all the data or to prevent it from leakage at our website
and in mass media you will need to purchase our decryption software.
Please contact our sales department at:

   http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/
      Login: [redacted]
      Password: [redacted]

Follow the guidelines below to avoid losing your data:

 - Do not shutdown or reboot your computers, unmount external storages.

 - Do not try to decrypt data using third party software. It may cause
   irreversible damage.

 - Do not fool yourself. Encryption has perfect secrecy and it's impossible
   to decrypt without knowing the key.

 - Do not modify, rename or delete *.key.` + config.Extension + ` files.
   Your data will be undecryptable.

 - Do not modify or rename encrypted files. You will lose them.

 - Do not report to authorities. The negotiation process will be terminated
   immediately and the key will be erased.

 - Do not reject to purchase. Your sensitive data will be publicly disclosed
   at http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/
```

Figure 7. Hive ransom note.

We noticed that the login credentials provided by the ransom note were for a specific victim. With this in mind, we then hunted for additional samples and found two more victims that were affected but not yet listed on the leak site at the time of writing. After logging in, the victim will see a chat where they can talk to the operators and get their decryptors (Figure 8).

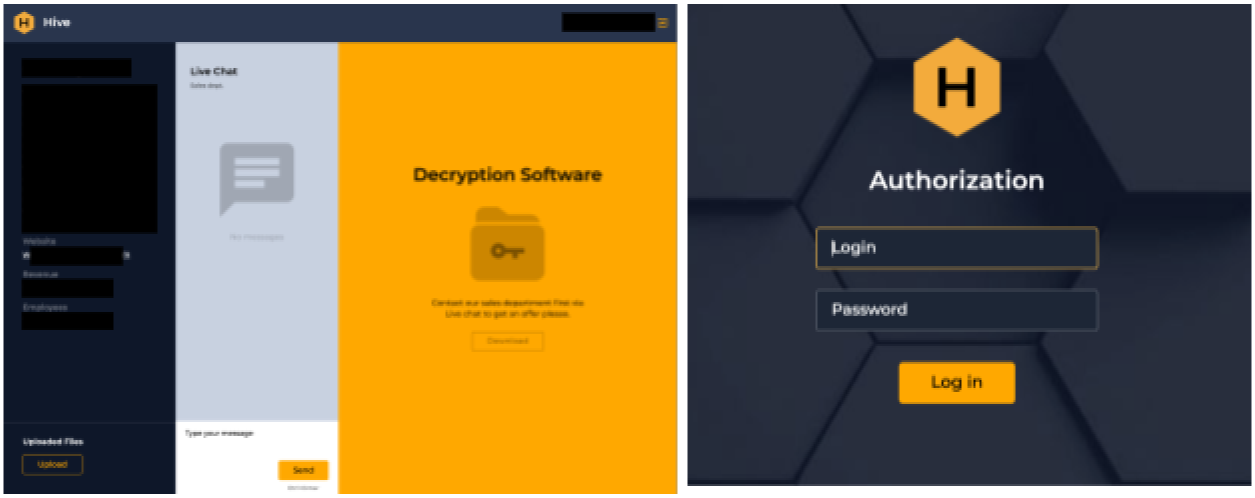


Figure 8. Hive chat (left) and login page (right).

We don't yet have information on how Hive ransomware is being delivered, but ransomware operators are known for buying access to certain networks, brute-forcing credentials or spear-phishing for initial access.

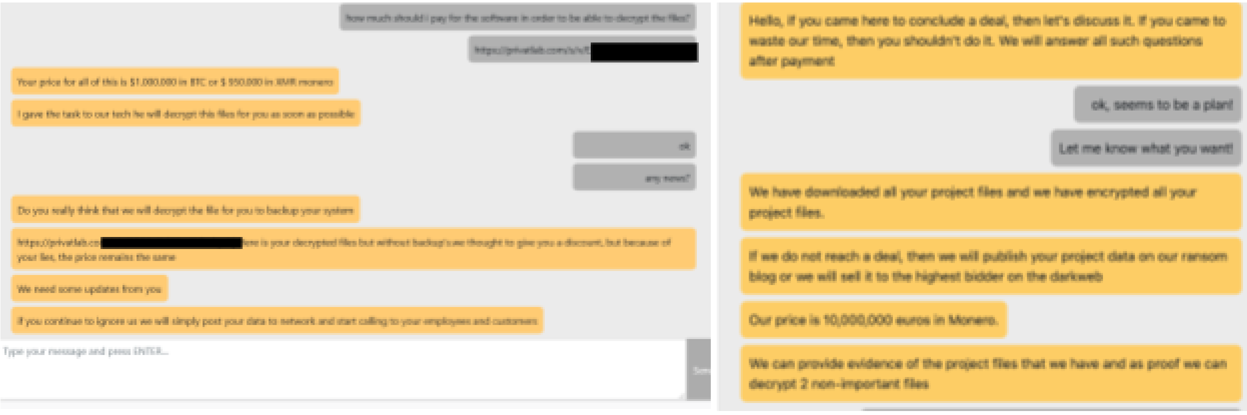
HelloKitty: Linux Edition

HelloKitty is a ransomware family that first surfaced at the end of 2020, primarily targeting Windows systems. The malware family got its name due to its use of a Mutex with the same name: HelloKittyMutex. The ransomware samples seem to evolve quickly and frequently, with different versions making use of the .crypted or .kitty file extensions for encrypted files. Some newer samples make use of a Golang packer that ensures the final ransomware code is only loaded in memory, most likely to evade detection by security solutions.

In July 2021, we came across a Linux (ELF) sample with the name funny_linux.elf containing a ransom note with verbiage that directly matched ransom notes seen in later samples of HelloKitty for Windows. This led to the discovery of other samples of this Linux strain of the HelloKitty ransomware, dating as far back as October 2020. However, starting in March, the samples began targeting ESXi, a target of choice for recent Linux ransomware variants.

Oddly enough, the preferred mode of communication shared by attackers in the ransom notes across the different samples is a mix between TOR URLs and victim-specific Protonmail email addresses. This could indicate different campaigns or even entirely different threat actors making use of the same malware codebase. Since the samples we found contained victim-specific ransom notes, we were able to get an idea of the ransomware's targets. We observed six organizations impacted by Hello Kitty, including Italian and Dutch pharmaceutical organizations, a Germany-based manufacturer, an Australian industrial automation solutions organization, and a medical office and a stock broker in the U.S. One sample, oddly enough, didn't contain any contact information in its ransom note.

We also observed that the ransom demanded by the operator varies depending on the impacted organization; we saw demands as high as $10 million and as low as $950,000 in Monero (Figure 9). The operators behind HelloKitty are also open to using bitcoin (BTC), but they charge higher for bitcoin transactions due to its associated fees. We were able to look up the BTC wallet address they provided for victims (bc1ql5f3m75qx3ueu2pz5eeveyqsw6pdjs3ufk8r20) and confirm that three transactions were made to that address, summing up to $1,477,872.41.



how much should i pay for the software in order to be able to decrypt the files?

https://privatlab.com/s/s/[redacted]

Your price for all of this is $1.000.000 in BTC or $ 950.000 in XMR monero

I gave the task to our tech he will decrypt this files for you as soon as possible

ok

any news?

Do you really think that we will decrypt the file for you to backup your system

https://privatlab.co[redacted]ere is your decrypted files but without backup's we thought to give you a discount, but because of your lies, the price remains the same

We need some updates from you

If you continue to ignore us we will simply post your data to network and start calling to your employees and customers

Hello, if you came here to conclude a deal, then let's discuss it. If you came to waste our time, then you shouldn't do it. We will answer all such questions after payment

ok, seems to be a plan!

Let me know what you want!

We have downloaded all your project files and we have encrypted all your project files.

If we do not reach a deal, then we will publish your project data on our ransom blog or we will sell it to the highest bidder on the darkweb

Our price is 10,000,000 euros in Monero.

We can provide evidence of the project files that we have and as proof we can decrypt 2 non-important files

Figure 9 HelloKitty chats.

The samples found primarily made use of different combinations of the arguments described in Table 1.

Argument	Description	Value(s)
v	Verbose mode	0 or 1
d	Run the process as a daemon	0 or 1
e	When the flag is set, the ransomware only encrypts files with the extensions .vmdk, .vmx, .vmsd and .vmsn It is not set by default, which means that all files under the start path that don’t match certain ransomware-specific file extensions will be encrypted	0 or 1
k	When this flag is set, the ransomware tries to kill VMs running on the host using the esxcli tool. It is not set by default	0 or 1
m	Mode	5 (default) or 10 or 20 or 25 or 33 or 50
c	(Unsure of purpose)	

Table 1. Arguments accepted by the Linux HelloKitty ransomware.

The following esxcli commands are executed to kill running VMs, when the k flag is set:

```
esxcli vm process list
esxcli vm process kill -t=soft -w=%d %(PID)
esxcli vm process kill -t=force -w=%d %(PID)
```

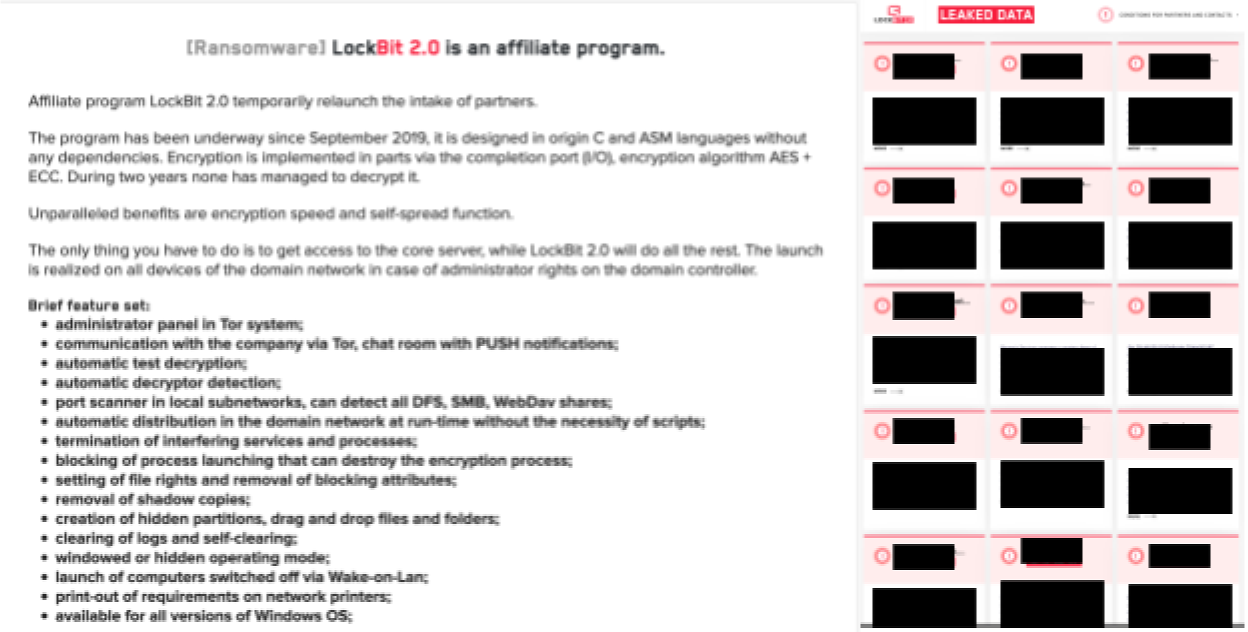
The malware samples log their output to a work.log file in their execution path.

Finally, the ransomware makes use of the Elliptic Curve Digital Signature Algorithm (ECDSA) for encrypting files using functions from the shared library libcrypto.so for encryption. The encrypted file is saved with the extension .crypt. Each encrypted file has a corresponding file with the extension .README_TO_RESTORE containing the ransom note. Additional details can be found in the appendix of this report.

LockBit 2.0

LockBit is another ransomware group that follows the RaaS model. According to their website, this ransomware affiliate program has been active since September 2019. While LockBit has been known for some time, we included this group in this blog because of their recent evolution to LockBit 2.0. In June 2021, the operators behind this ransomware revamped their site and rebranded as LockBit 2.0.

Since June 2021, they have compromised 52 organizations in accounting ,automotive, consulting, engineering, finance, high tech, hospitality, insurance, law enforcement,l egal services, manufacturing, non-profit energy, retail, transportation and logistics industries, utilities in the following countries: Argentina, Australia, Austria, Belgium, Brazil, Germany, Italy, Malaysia, Mexico, Romania, Switzerland, the U.K. and the U.S. All the posts by the threat actors on their leak site include a countdown until confidential information is released to the public, which creates additional pressure on the victim (Figure 10).



[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.

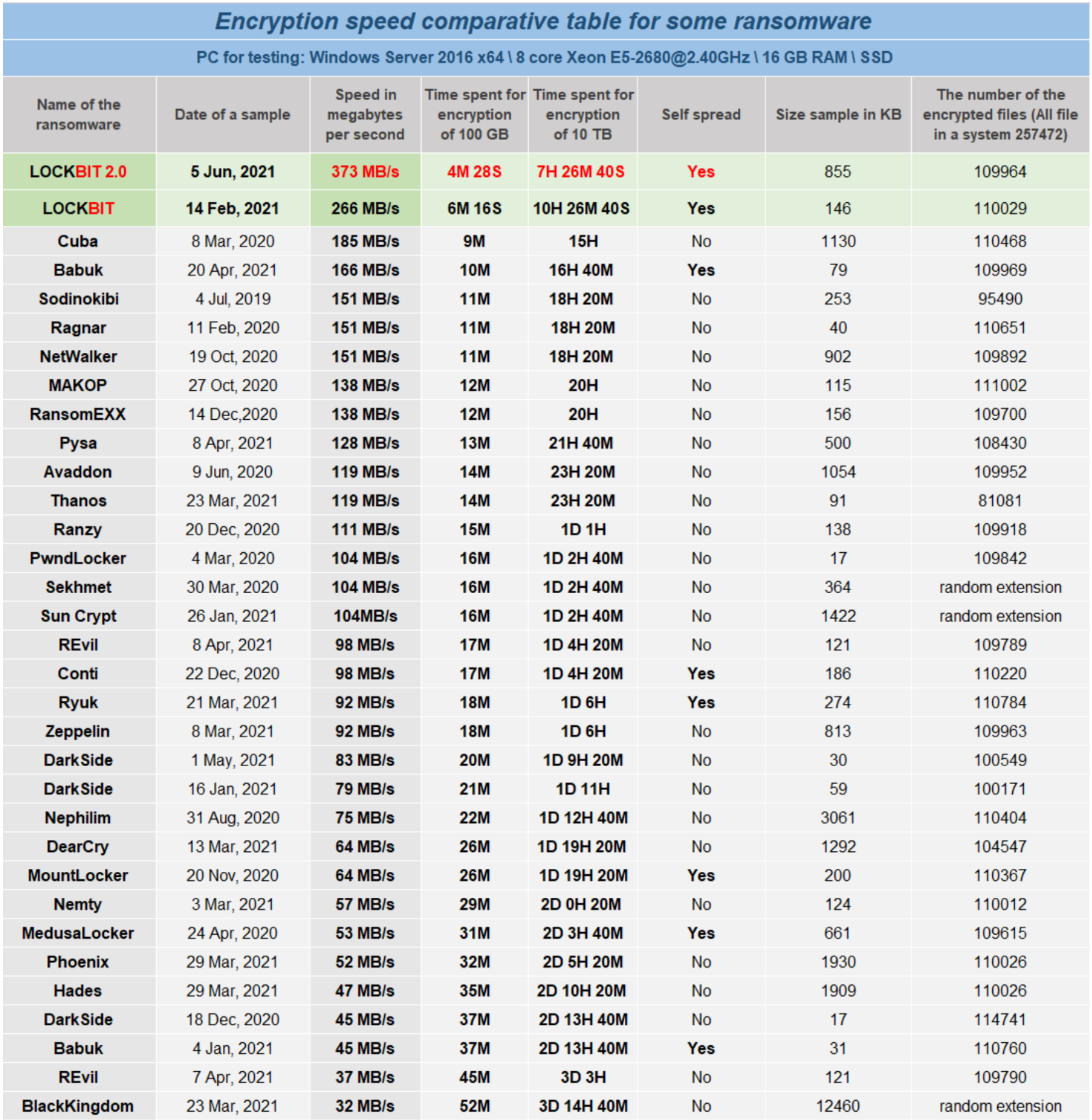
Brief feature set:

- **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;**

[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]
[redacted] [redacted] [redacted]

Figure 10. Affiliation program description (left) and leak site (right).

The threat actors behind this ransomware claim that their current variant is the fastest encryption software in operation. To attract more affiliates, they include a table comparing different ransomware families, including their previous variant (Figure 11).



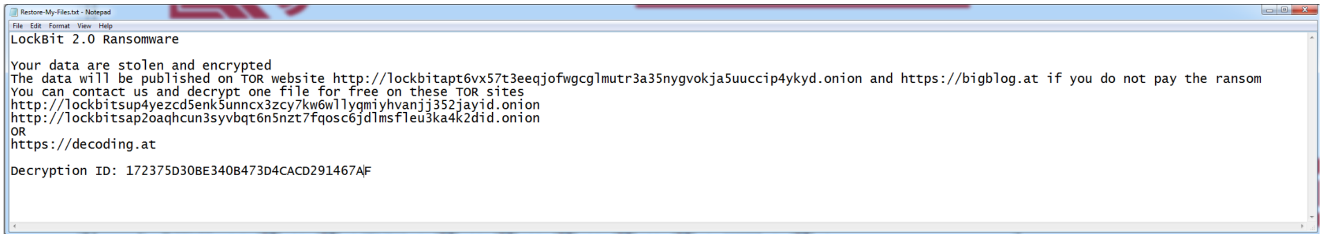
Encryption speed comparative table for some ransomware

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	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension

Figure 11. Encryption speeds comparison released by LockBit.

When LockBit is executed, it starts encrypting files and appends the .lockbit extension. Additionally, the ransomware changes the icon of the encrypted file to the LockBit 2.0 logo (Figure 12.b). After encryption is complete, LockBit then drops the ransom note titled, Restore-My-Files.txt (Figure 12.a).



```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and https://bigblog.at if you do not pay the ransom
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: 172375D30BE340B473D4CACD291467AF
```

Figure 12a. Ransom Note.

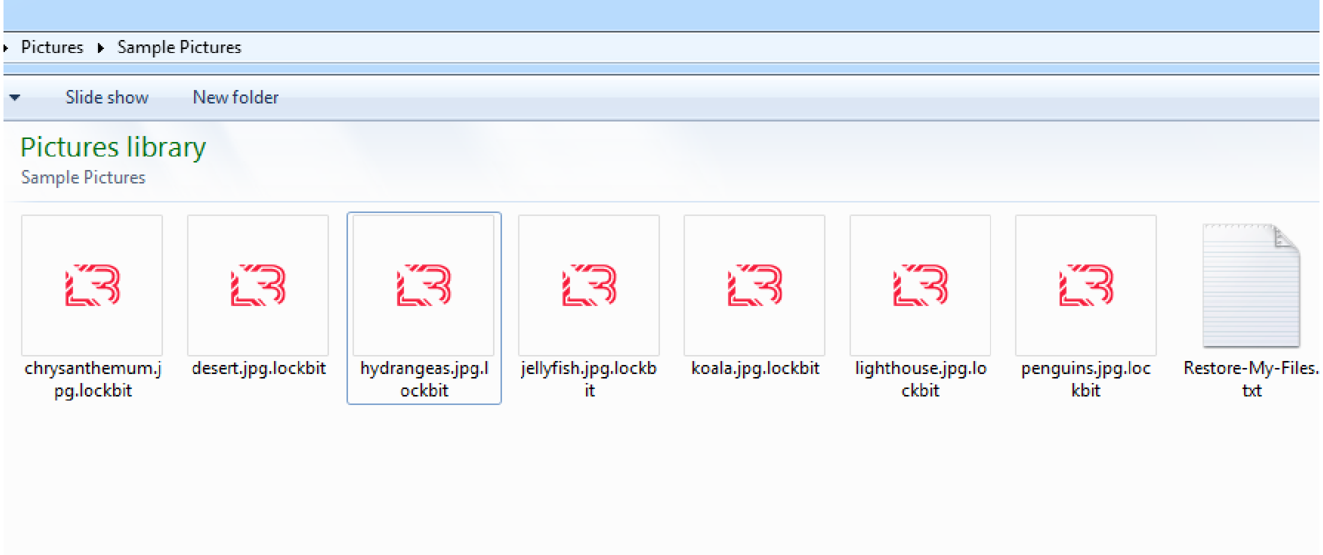
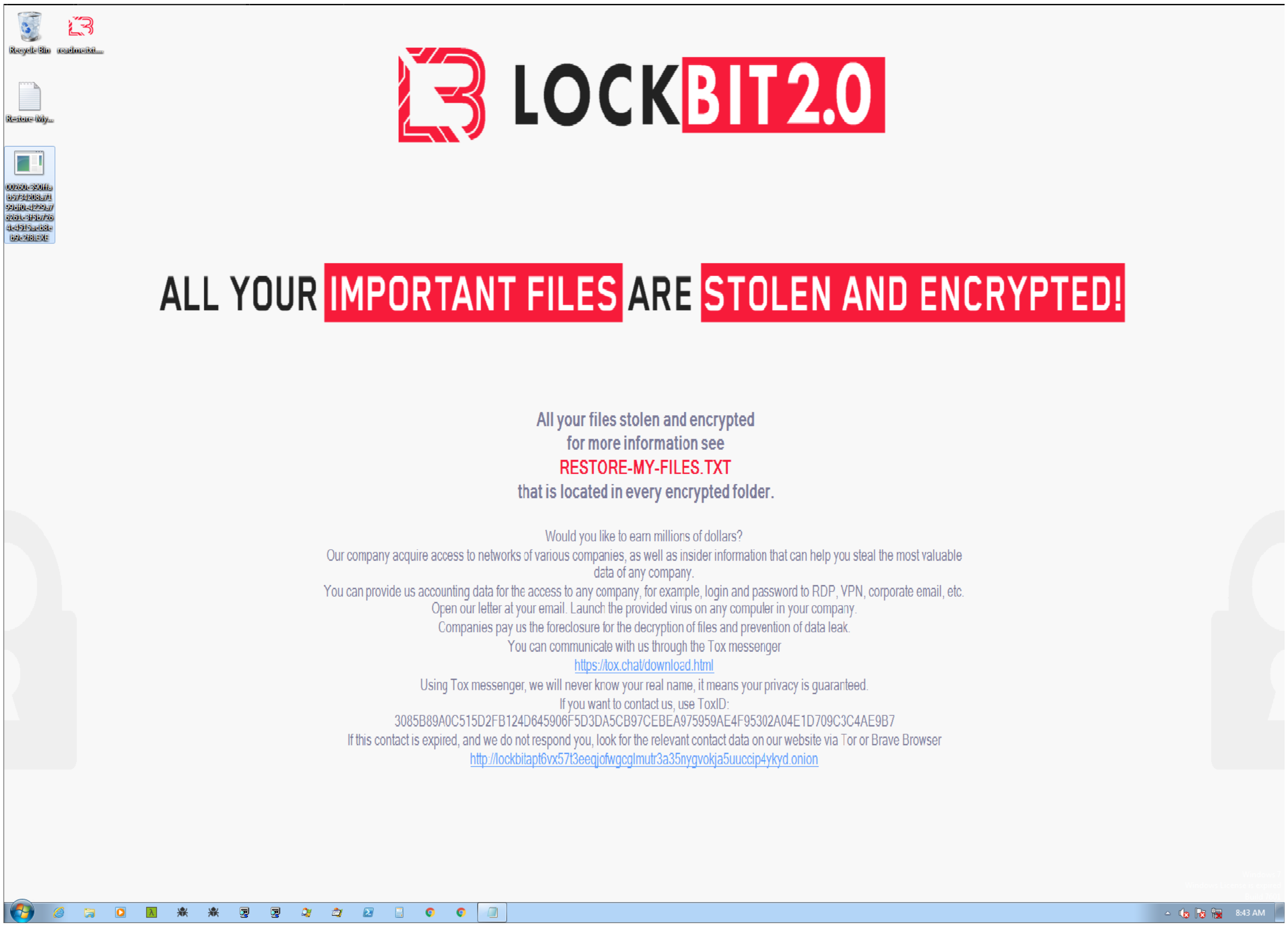


Figure 12b. Encrypted files.

Similar to REvil, LockBit 2.0 ransomware modifies the victim's desktop wallpaper if the encryption process is successful, making the victim aware of their compromise. The wallpaper also includes an advertisement aimed at encouraging insider threats that all organizations could fall prey to. (Figure 13).



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

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 compuler in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
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, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
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
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

Figure 13. Modified LockBit 2.0 wallpaper.

The advertisement states that the threat actors are interested in methods of access, such as RDP, VPN and corporate email credentials. In exchange, they offer a cut of paid ransom.

If the victim wants to communicate with Lockbit operators to get their data back, the operators include a “Decryption ID” and a TOR link (and their clearnet mirror: decoding[.]at) on the ransom note. This information allows the user to log in and start the negotiation process (Figure 14).

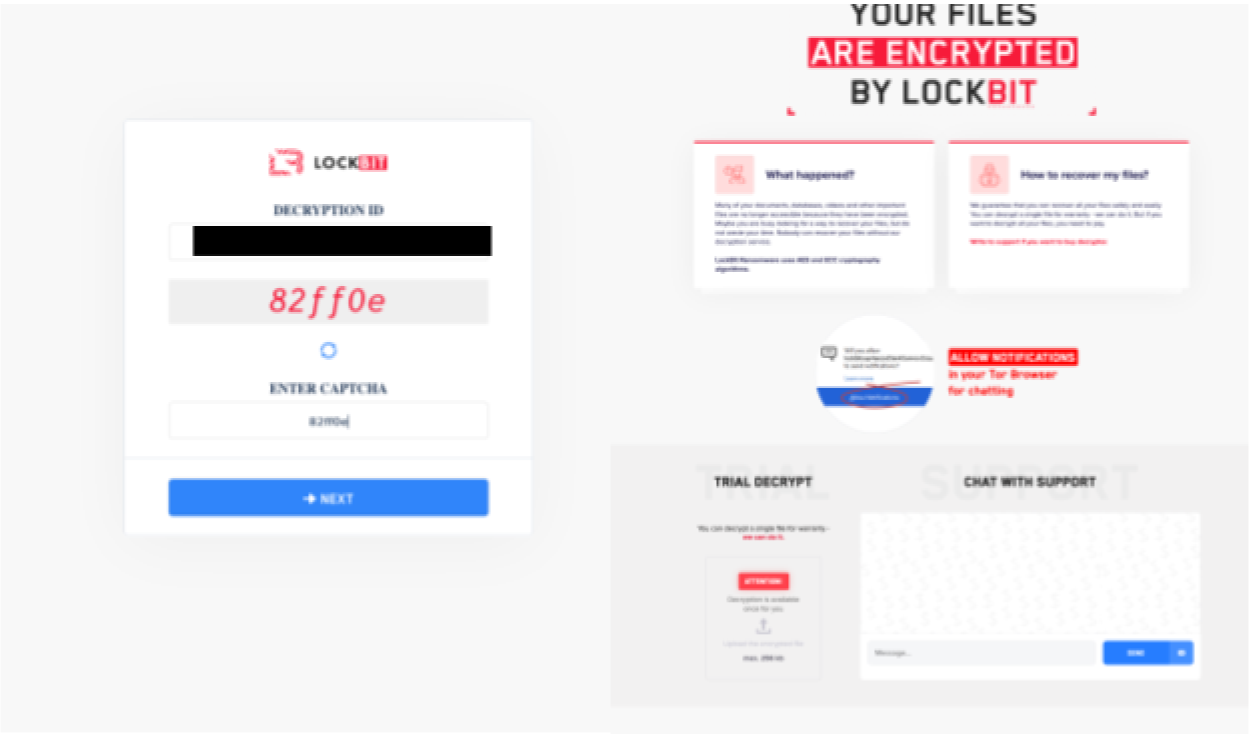


Figure 14. Support site login (left) and LockBit Support chat (right).

Conclusion

With major ransomware groups such as REvil and Darkside lying low or rebranding to evade law enforcement heat and media attention, new groups will emerge to replace the ones that are no longer actively targeting victims. Here, we shared information on some of the observed malicious activity of the ransomware groups trying to become the next key players. While LockBit and HelloKitty have been previously active, their recent evolution makes them a good example of how old groups can re-emerge and remain persistent threats. Unit 42 will continue to monitor these ransomware families – and new ones that may emerge in the future.

Palo Alto Networks customers are protected against these ransomware families with Cortex XDR or the Next-Generation Firewall with Threat Prevention and WildFire security subscriptions. Customers can use AutoFocus for tracking related entities using the AvosLocker, Hive, LockBit and HelloKitty tags, respectively. Full visualization of the techniques observed can be seen in the Unit 42 ATOM viewer.

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 systematically disrupt malicious cyber actors. Visit the Cyber Threat Alliance for more information.

If you think you may have been impacted by any of these ransomware families, please email unit42-investigations@paloaltonetworks.com or call (866) 486-4842 – (866) 4-UNIT42 – for U.S. toll-free; (31-20) 299-3130 in EMEA; or (65) 6983-8730 in JAPAC. The Unit 42 Incident Response team is available 24/7/365. You can also take preventative steps by requesting a Ransomware Readiness Assessment.

Indicators of Compromise

AvosLocker

43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856
fb544e1f74ce02937c3a3657be8d125d5953996115f65697b7d39e237020706f
3984968230c96d52d78af1905ea1b224e7de36776a6af398a0462321f3c22020
01792043e07a0db52664c5878b253531b293754dc6fd6a8426899c1a66ddd61f

Hive Ransomware

A0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749
1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff
Fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf
88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1

Hello Kitty (Linux)

16a0054a277d8c26beb97850ac3e86dd0736ae6661db912b8782b4eb08cfd36e
556e5cb5e4e77678110961c8d9260a726a363e00bf8d278e5302cb4bfccc3eed
9f82f22c137688d0b3e7912d415605d2bbc56478311fd0b3dc265f8d0006aa8c
8f3db63f70fad912a3d5994e80ad9a6d1db6c38d119b38bc04890dfba4c4a2b2
bedf30bbcefc54bc48432674255856f47c0ba2ec46e913d078a53e66ac9dcff8
Ca607e431062ee49a21d69d722750e5edbd8ffabcb54fa92b231814101756041
b4f90cff1e3900a3906c3b74f307498760462d719c31d008fc01937f5400fb85

Lockbit 2.0

F32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202
4de287e0b05e138ab942d71d1d4d2ad5fb7d46a336a446f619091bdace4f2d0a
F3e891a2a39dd948cd85e1c8335a83e640d0987dbd48c16001a02f6b7c1733ae
Ea028ec3efaab9a3ce49379fef714bef0b120661dcbb55fcfab5c4f720598477
Bcdb59232137e570d4afb3c635f8df19ceb03e3f57fe558f4fc69a0be778c6ab
4efcd774d9d224137c5840e9a2d0f9e56c976e8e7a49158e3c15135dd9fbae9c
00260c390ffab5734208a7199df0e4229a76261c3f5b7264c4515acb8eb9c2f8
E32dc551a721b43da44a068f38928d3e363435ce0e4d2e0479c0dfdb27563c82
16a707a3965ebd71ebc831b68863b855b2c8d60aef8efdef1e0c0a6cc28e9bc7
Bc0b54c19949f407da972f0bedf7f429c0fe25181564d1fb6d053b989925898f
Acad2d9b291b5a9662aa1469f96995dc547a45e391af9c7fa24f5921b0128b2c
0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049
Bcbb1e388759eea5c1fbb4f35c29b6f66f3f4ca4c715bab35c8fc56dcf3fa621
717585e9605ac2a971b7c7537e6e311bab9db02ecc6451e0efada9b2ff38b474

73406e0e7882addf0f810d3bc0e386fd5fd2dd441c895095f4125bb236ae7345

90af3848d5a0c5eb9c6ddc1ee2e6c539dd6cb5ec5a433d00a6dae22fb221c446

4bb152c96ba9e25f293bbc03c607918a4452231087053a8cb1a8accb1acc92fd

21879b5a8a84c5fe5e009c85744caf74b817c57203020bf919037d7ccb6b6a58

56fd91787c641c2329a86813497d0e6ff219c81a4d61ac10fedef9cd68c3baed

9dd6cc25b2f920b825e15682a4d06435a42b281674ba6e99c8e2b2222c9d638f

23984141a918be3345296bb6bf50d8d356229cb832c726833499fbb950037d00

91d1ab6c305552685996f4d80c44cc1c694355ae7d09243df027827d1df61631

1dbe9f956514460774290197ffccb11d817d1a5a5aeab81877ae7b74daa1b592

1e3bf358c76f4030ffc4437d5fcd80c54bd91b361abb43a4fa6340e62d986770

69d9dd7fdd88f33e2343fb391ba063a65fe5ffbe649da1c5083ec4a67c525997

26b6a9fecfc9d4b4b2c2ff02885b257721687e6b820f72cf2e66c1cae2675739

Ca57455fd148754bf443a2c8b06dc2a295f014b071e3990dd99916250d21bc75

5072678821b490853eff0a97191f262c4e8404984dd8d5be1151fef437ca26db

410c884d883ebe2172507b5eadd10bc8a2ae2564ba0d33b1e84e5f3c22bd3677

0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76

286bffaa9c81abfb938fe65be198770c38115cdec95865a241f913769e9bfd3f

E3f236e4aeb73f8f8f0caebe46f53abbb2f71fa4b266a34ab50e01933709e877

0f178bc093b6b9d25924a85d9a7dde64592215599733e83e3bbc6df219564335

1b109db549dd0bf64cadafec575b5895690760c7180a4edbf0c5296766162f18

Ffbb6c4d8d704a530bdd557890f367ad904c09c03f53fda5615a7208a0ea3e4d

76a77def28acf51b2b7cdcbfaa182fe5726dd3f9e891682a4efc3226640b9c78

faa3453ceb1bd4e5b0b10171eaa908e56e7275173178010fcc323fdea67a6869

12a435aa3fe7fc3fa531b9e02ee63b907f343b4aa7acc137105e48eb7b32075a

e32dc551a721b43da44a068f38928d3e363435ce0e4d2e0479c0dfdb27563c82

bc0b54c19949f407da972f0bedf7f429c0fe25181564d1fb6d053b989925898f

14b3827e821ee2d719d20c265d873e7e1471df40df1089175adbbe31a83fc0eb

acad2d9b291b5a9662aa1469f96995dc547a45e391af9c7fa24f5921b0128b2c

bcbb1e388759eea5c1fbb4f35c29b6f66f3f4ca4c715bab35c8fc56dcf3fa621

d089d57b8b2b32ee9816338e96680127babc5d08a03150740a8459c29ab3ba78

32f8eed5b2ada44b51cb251bce22355604d8cafef77e33bce769469926dc8cd7

92ec3373b528e0040fae1c34b6edc8d623d03eac84267bd3ed408fe547b9c944

f32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202

f3e891a2a39dd948cd85e1c8335a83e640d0987dbd48c16001a02f6b7c1733ae

d52f0647e519edcea013530a23e9e5bf871cf3bd8acb30e5c870ccc8c7b89a09

ea028ec3efaab9a3ce49379fef714bef0b120661dcbb55fcfab5c4f720598477

bcdb59232137e570d4afb3c635f8df19ceb03e3f57fe558f4fc69a0be778c6ab

1008af117f3f9f5c2d7f634c7c88fdb2af0dc2a8d01be203f0d69897559d3e05

60b5aa993eaef3342252f8cb3f4c9d7c6272ebf2180a27bac8db516af32e8393

459e6ff44674568233b2b2fbfd56e1456e5d72147fe919c063b5fc87d8fb3365

0bbd59147cf0893d16829d705dcb6bed82487efc77c78fb17c1f2dcffa08875e

a8dfd303f2ff18416ccb88a815629889268976712 1206b137a92ece8577e7403

ebe038b29b9f535f975ac7e6c256b7b0597ff93710c2328e8c43a63c750b441d
b0ae47c915e7ed46e7badb3ed3888debf505c0a9f0a88e1ee18757df74cecb5f
0b856337d9d3255fc3b07635fdadecbe83e23eb5c205eccab83c21c2fb76edc9
3dcb5aa76118a5af24c3e01290d2ad0f71adcc21d3e2b337210bbeb97f73881a
ade83273f178c3dd5f82c22f42015dcf1aa1a2c961b6e4bf80068b7b5986cc2f
b2b29c358242d49da3c9ef237695e02817b3e5b3fbb75fa94b5762e2a4210f8f
d2ab5785e0dcf9c7657d960b7b7e86f1373408226a95946400f98e5957faf631
aa727a827c9e978520f5703e9100b52551b97cfc1e15e683cf27ce5212035548
5b9e6d9275e9523aa3945be891745442a07b936ee5236e23934250ba3844f65f
3e3801d5441c63661aca495f3e540ff77c669437924aff64dc340f594fbb185a
99d781a0e9ac3dfaa7f9958cc62051f47ba116835e75b5d61835ff63afc98571
e2e140d6d84e377c313006ae8d0848583f74a1ee7aad0fcd758a1888f9b04694
b2f1ec9408272cc125b96a4f3b7c06c23742d69845e9b6a24f7eafad4da72faa
e7a81e3c2bd77a237a3b75806197cb18db5cbf06fda246739bb3904ac117d013
e15903faaad61d6d6499148c596d8051a51c80973cc1190336769b84a1eca1c8
743ecc953dcd83a48140c82d8a7dcac1af28e0839aed16628ddfc9454bec8dfa
626a4fa1f52623e89b3011c37c2d3ca4069dc5a4d3f5c4f74d4579c2d3d50356
8013232fb7c254269c1029f91a915b80ed7ded53043d239a4be9a0b1fe37fa2c
953bdc65d1d3316ffb2761da09a3b8587228bd40095d72eae95fc373488732cc
e82315985f8eab415f6fabab7f805f0a76db6ca58b851070c946142f0ba29cbd
fab378dbd88af235421174b73ad06d1e5f2c614c70b9bab318602f51da544d5e
a718c499a7a3c505828f5253862c9b2f3c40e2d80132de96e5cc19e3c161730b
b735c0169ecdddba6676c6c490199358f6ab7cc9724391fee2482676a3efc6e5
a7591e4a248c04547579f014c94d7d30aa16a01bb2a25b77df36e30a198df108
98900768d564c6962981edde2759889fdda11bb1113c851468e5c40ddafe1d4d
6d26226f99724c18faf355a4e07b74bad72f5837e0de8c8361f7d9a18525b5ae
5f99cdba09aa3e03e531fc34bc5fcee96f61ec0b83b575911d79573da7109906
cd2287122277237a9c507ce9ba5f114ddd48faa1b3f87b33ed1a8b19f65c8a14
93b0c6576c73b48dcb47f6572a31defc1304fd3c4464d50592195fa64edbcafe
34e6f4317e223d712a9464cd2e6ba9e6d7915eac75a8c06648813ea1d7a80b80
36446a57a54aba2517efca37eedd77c89dfc06e056369eac32397e8679660ff7
f17ca8f7527669a35eee12edb7050a81ef91e3f0ea7b3935ddf554a6f731e374
4edbf2358a9820e030136dc76126c20cc38159df0d8d7b13d30b1c9351e8b277
0906a0b27f59b6db2a2451a0e0aabf292818e32ddd5404d08bf49c601a466744
0d6524b9a1d709ecd9f19f75fa78d94096e039b3d4592d13e8dbddf99867182d

Domains

Decoding[.]at
bigblog[.]at
lockbit-decryptor[.]com
lockbit-decryptor[.]top

Appendix (Hello Kitty)

Extensions that are ignored for encryption:

.crypt
.README_TO_RESTORE
.tmp_
.a
.so
.la

Directories ignored for encryption:

/bin
/boot
/dev
/etc
/lib
/lib32
/lib64
/lost+found
/proc
/run
/sbin
/usr/bin
/usr/include
/usr/lib
/usr/lib32
/usr/lib64
/usr/sbin
/sys
/usr/libexec
/usr/share
/var/lib