Meet LockBit: The Most Prevalent Ransomware in 2022 | FortiGuard Labs

Published: 2023-07-10 · Archived: 2026-04-05 16:32:48 UTC

Affected platforms: Microsoft Windows, Linux, ESXi, MacOS
Impacted parties: Microsoft Windows, Linux, ESXi, and MacOS Users
Impact: Encrypts and exfiltrates victims' files and demands ransom for file decryption and not to leak stolen files
Severity level: High

On June 14th, 2023, the CISA, FBI, MS-ISAC, and multiple international cyber security organizations released a joint advisory for the LockBit ransomware. This ransomware group has been active since early 2020, targeting organizations across numerous industries, including energy and government sectors. According to the advisory, LockBit was the most active ransomware in 2022.

This blog provides insights into the LockBit Group's activities over the past few years.

What is LockBit?

LockBit is a ransomware group that has been active since early 2020 (the active period goes back to 2019 if its predecessor "ABCD ransomware" is included in the "LockBit" family) providing a Ransomware-as-a-Service (RaaS) service to for-hire online criminals known as affiliates. The affiliates' job is to select and infiltrate victim organizations and deploy the ransomware provided by the LockBit developer.

The developer has consistently worked to improve the ransomware: LockBit 2.0 (also known as LockBit Red) was released in mid-2021, and LockBit 3.0 (also known as LockBit Black) became available in early-2022. The latest LockBit ransomware variant, "LockBit Green," appeared in early 2023. While the LockBit ransomware initially only supported the Windows platform, the LockBit threat actor group added support for Linux/VMware/ESXi and macOS platforms in 2021 and 2023, respectively. The group also works with partners who want to sell exfiltrated data but do not want to encrypt victims' files.

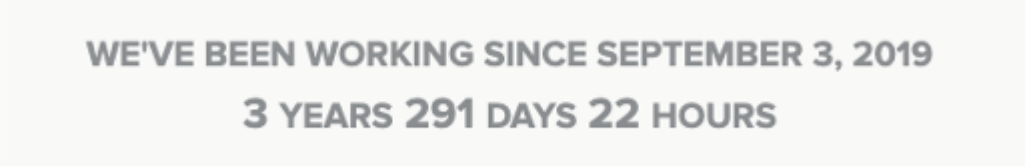


Figure 1. LockBit's active period as of June 21st, 2023, seen on its data leak site

LockBit uses a dual extortion tactic, demanding that victims pay a ransom to recover their files and not release the stolen information to the public. LockBit is also believed to threaten Distributed Denial of Service (DDoS) attacks against victims if the demanded ransom is not paid.

Due to its prevalence and popularity among cybercriminals, FortiGuard Labs has published several blogs and threat signals for LockBit ransomware:

Blog

- Can You See It Now? An Emerging LockBit Campaign
- Ransomware Roundup: LockBit, BlueSky, and More

Threat Signal

- #StopRansomware: LockBit 3.0 (AA23-075A)
- LockBit 2.0 Ransomware as a Service (RaaS) Incorporates Enhanced Delivery Mechanism via Group Policy

As a RaaS, the LockBit operator offers its affiliates a variety of options for splitting the ransom fee. The ransom payment is typically split 1:4 between the LockBit operator and the affiliates.

Using the features provided by the LockBit operator, its affiliates can perform a variety of activities, including:

- Create private chat rooms to communicate with victim organizations
- Use of a custom “StealBit” stealer for data exfiltration
- Upload images, data, and communication history with victim organizations to the LockBit blog (data leak site)
- Set exceptions for computer names, file names, and file extensions that are not to be encrypted
- Shut down and remove Windows Defender
- Run the ransomware in SafeMode
- Delete shadow copies

It also has “do not target” and approved “target” industry lists for file encryption and data exfiltration.

- Affiliates are **NOT** allowed to encrypt files belonging to critical infrastructure, such as nuclear/thermal/hydroelectric power plants, gas and oil pipelines, oil production stations, and refineries. However, affiliates are allowed to steal data from such organizations without encrypting files.
- Affiliates are **NOT** allowed to attack post-Soviet countries: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine, and Estonia.
- Affiliates **ARE** allowed to target non-profit organizations
- Affiliates **ARE** allowed to target private and for-profit educational institutions
- Affiliates **ARE** allowed to attack medical and pharmaceutical institutions/companies, as long as the attack does not result in death. Affiliates are free to steal data without encrypting files.
- Affiliates **ARE** allowed to attack government agencies (as long as they make a profit)
- Affiliates **ARE ENCOURAGED** to attack police stations and law enforcement agencies

Prevalence

Data gathered through Fortinet's FortiRecon service supports the CISA advisory's claim that LockBit was the most active ransomware in 2022. According to our internal research, LockBit ransomware accounted for approximately 50% of the 3,298 ransomware incidents we observed in 2022.

Figure 2. FortiRecon's ransomware trends from January 1st, 2022, to December 31st, 2022

LockBit ransomware victim organizations are spread across several industries. As explained, the LockBit operator imposes "do not attack" rules for specific industries and countries. However, it's up to each affiliate to follow the rules.

History of LockBit Ransomware

ABCD ransomware

ABCD ransomware, which first appeared in September 2019, is believed to be the predecessor of LockBit ransomware. Unlike its slightly more sophisticated successor, ABCD ransomware only allows victims to contact it using email. The ransomware also deletes shadow copies by running the command *vssadmin delete shadows /all /quiet & wmic shadowcopy delete*, making it difficult to recover files.

FortiGuard Labs found what appears to be an even earlier version of the ABCD ransomware (SHA2: 49c0acf512146620dd26f515804324c8e4b4cc8eb8b9ab5d9c57e201241bc7ae). While this variant encrypts files, its ransom note only contains the victim's personal ID.

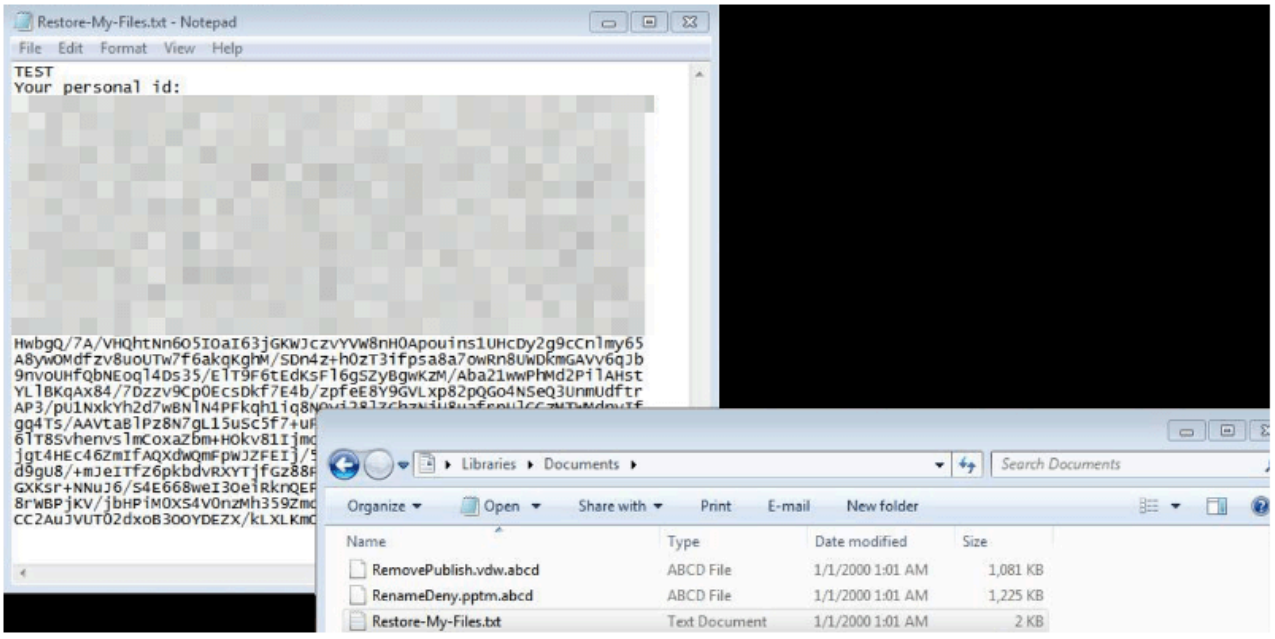


Figure 3. LockBit's encrypted files and test ransom note

The transition can be seen in a subsequent ABCD ransomware sample (SHA2: c8205792fbc0a5efc6b8f0f2257514990bfaa987768c4839d413dd10721e8871). This sample drops a ransom note, "Restore-My-Files.txt," and changes the desktop wallpaper. Both refer to LockBit, but encrypted files still have a ".abcd" extension. It's also worth noting that the LockBit operator set up a data leak site on TOR.

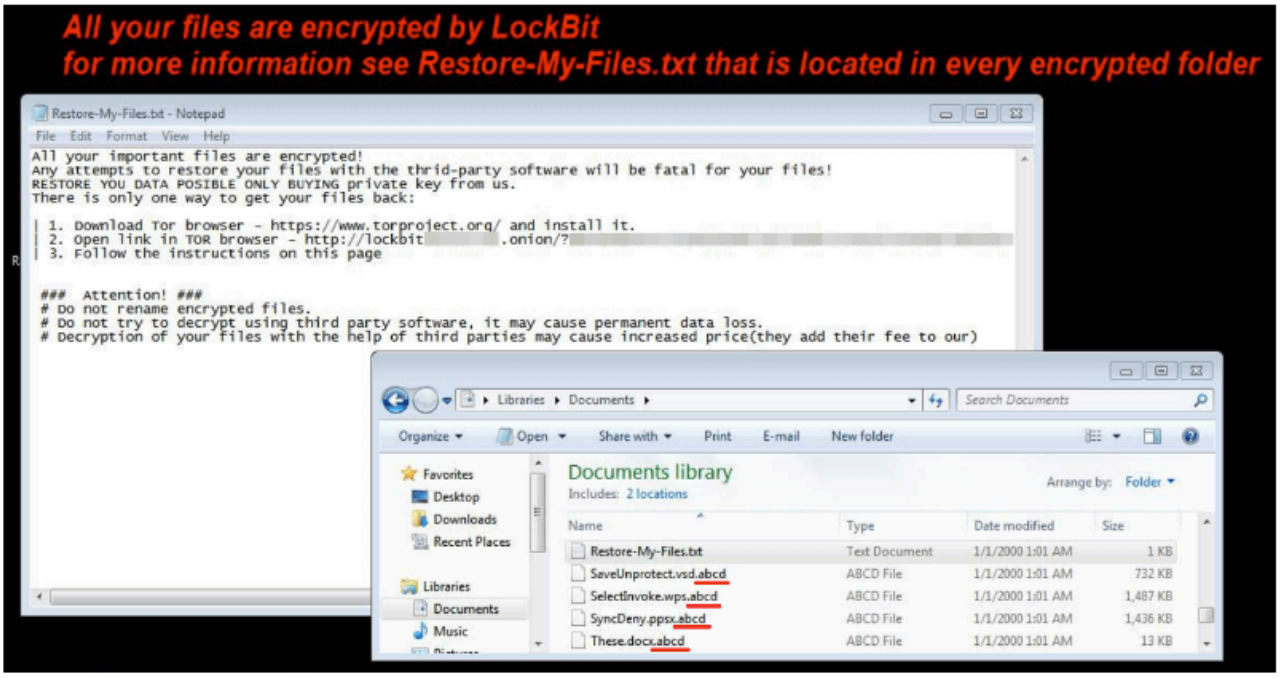


Figure 4. ABCD ransomware sample referencing LockBit

LockBit

ABCD ransomware was rebranded as LockBit in January 2020. This new LockBit variant changes the file extensions of encrypted files to ".lockbit" instead of ".abcd".

Figure 5. Files encrypted by LockBit ransomware

It drops a ransom note with the same name as the ABCD ransomware, and communication was centralized on the TOR website rather than via email.

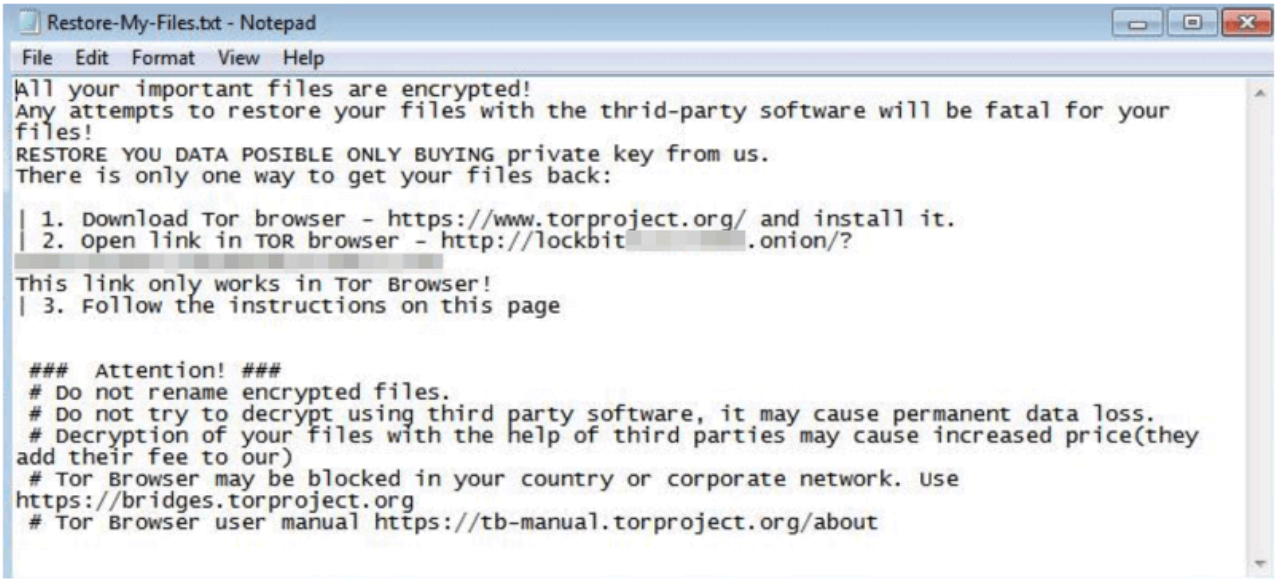


Figure 6. LockBit ransom note

This LockBit variant also replaces the desktop wallpaper on compromised machines to indicate the presence of the ransom note. The threat actor appears to have been using two different wallpapers.

Figure 7. Desktop wallpaper replaced by LockBit ransomware

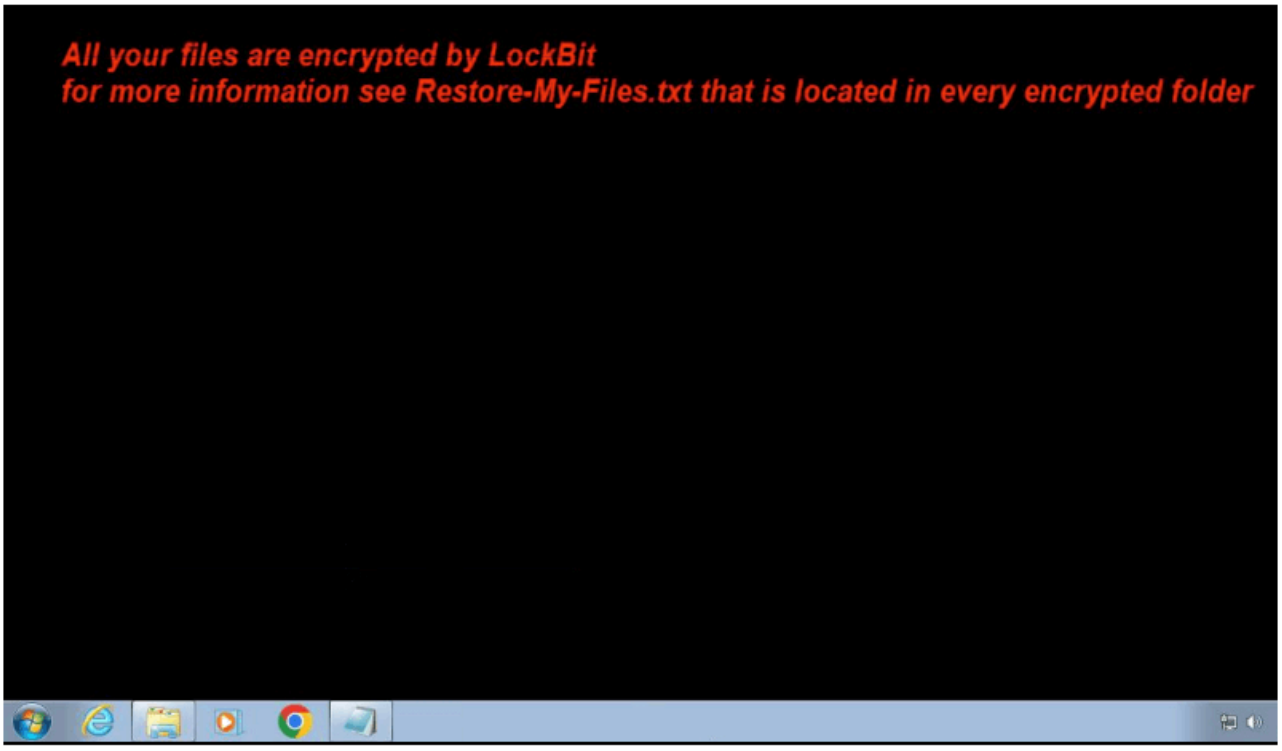


Figure 8. Another desktop wallpaper replaced by LockBit ransomware

LockBit 2.0 (LockBit Red)

LockBit ransomware was updated to LockBit 2.0 (also known as LockBit Red) in mid-2021. This new variant still appends a ".lockbit" extension to the files it encrypts but now uses a red file icon that mimics the shape of a B.

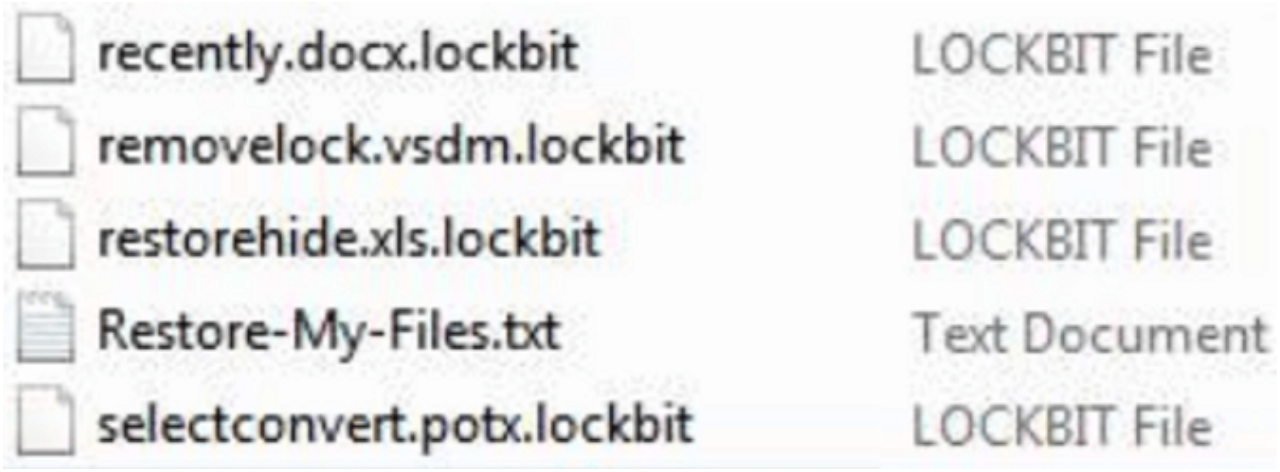


Figure 9. Files encrypted by LockBit 2.0 (LockBit Red)

Figure 10. LockBit 2.0 file icon

LockBit 2.0 displays a ransom note on the desktop and a text file called Restore-My-Files.txt. This time, the LockBit threat actor added an alternate website that can be accessed through regular web browsers.

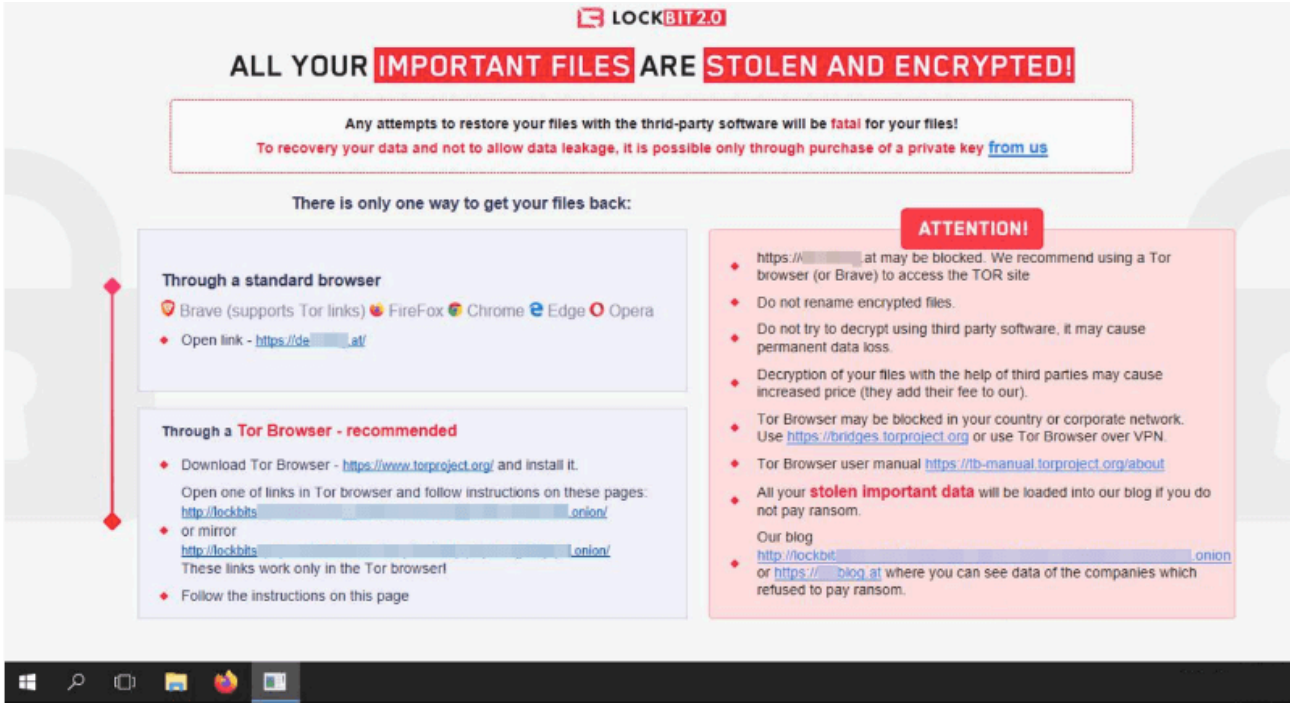


Figure 11. Desktop wallpaper replaced by LockBit 2.0

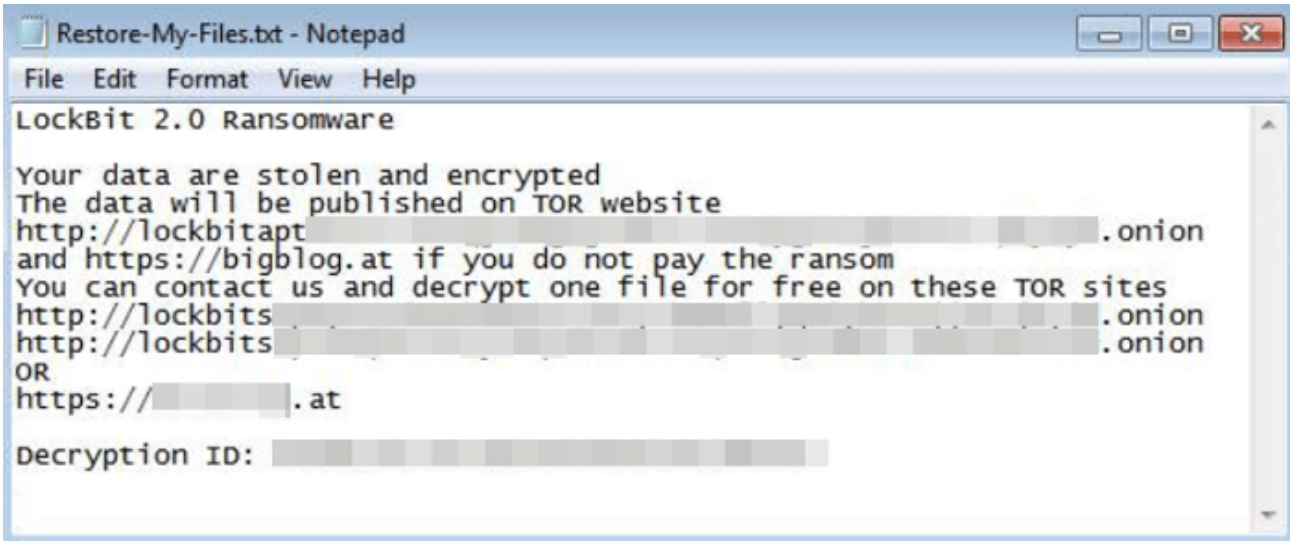


Figure 12. LockBit 2.0 ransom note

LockBit Linux-ESXi Locker

In October 2021, the LockBit developer released a new LockBit ransomware variant designed to work on Linux and ESXi virtual machines. Like the Windows version, this new LockBit variant encrypts files on compromised devices and leaves a ransom note called "restore-my-files.txt."

LockBit 3.0 (March 2022~)

LockBit 3.0 was released in March 2022. This variant appends a random 9-character file extension instead of the ".lockbit" extension used by the two previous LockBit variants. It also changes the file icon of the encrypted files to a black file icon that mimics the shape of a B.

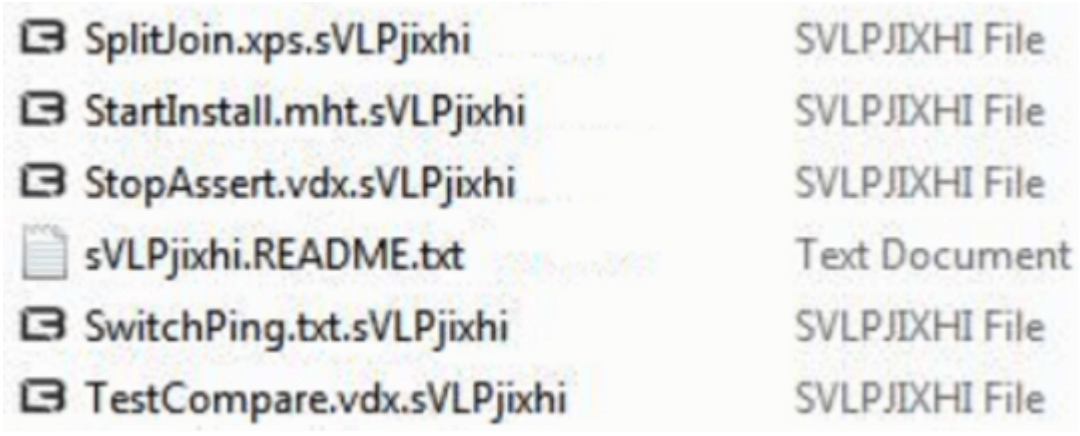
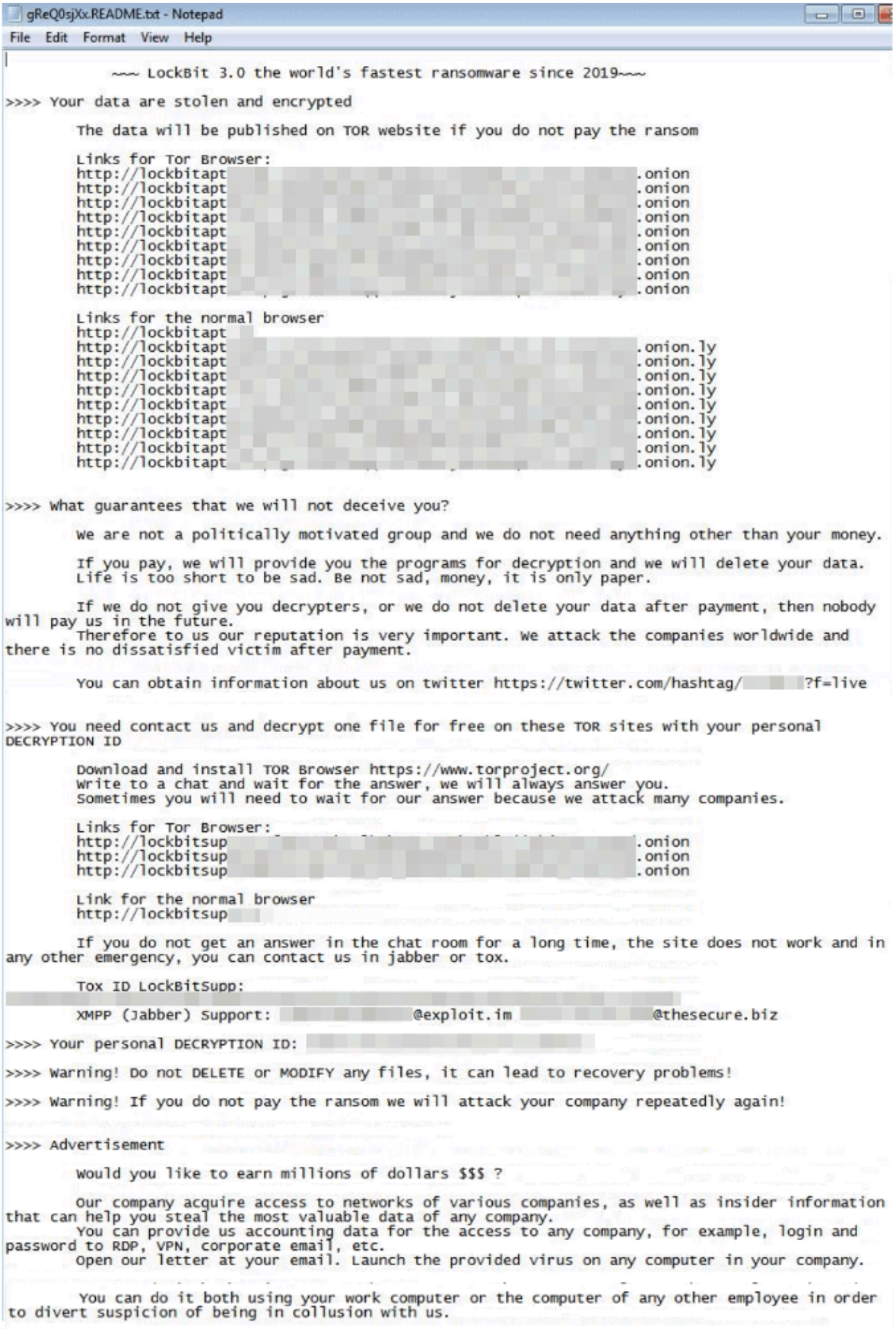


Figure 13. Files encrypted by LockBit 3.0 (LockBit Black)

Figure 14. LockBit 3.0 file icon

LockBit 3.0 drops a ransom note labeled "[random nine letters]_README_txt." The threat actor also set up more mirror TOR and regular websites in case they become inaccessible. This turned out to be the right move, as in mid-2022, reported distributed denial-of-service (DDoS) attacks took down LockBit's leak sites. The group also added 'Tox' and 'Jabber' as alternative communication methods for victims. Another noteworthy addition was an advertisement for victims, in which the LockBit group seeks insiders willing to provide internal information and access to the corporate network.



gReQ0sjXx.README.txt - Notepad

File Edit Format View Help

~~~ LockBit 3.0 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://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion
http://lockbitapt[redacted].onion

Links for the normal browser
http://lockbitapt[redacted]
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly
http://lockbitapt[redacted].onion.ly

>>>> 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 pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

You can obtain information about us on twitter https://twitter.com/hashtag/[redacted]?f=live

>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

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://lockbitsup[redacted].onion
http://lockbitsup[redacted].onion
http://lockbitsup[redacted].onion

Link for the normal browser
http://lockbitsup[redacted]

If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us in jabber or tox.

Tox ID LockBitSupp:
[redacted]

XMPP (Jabber) Support: [redacted]@exploit.im [redacted]@thesecure.biz

>>>> Your personal DECRYPTION ID: [redacted]

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

>>>> 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.
```

Figure 15. LockBit 3.0 ransom note

It also replaces the desktop wallpaper with a reference to the dropped ransom note.

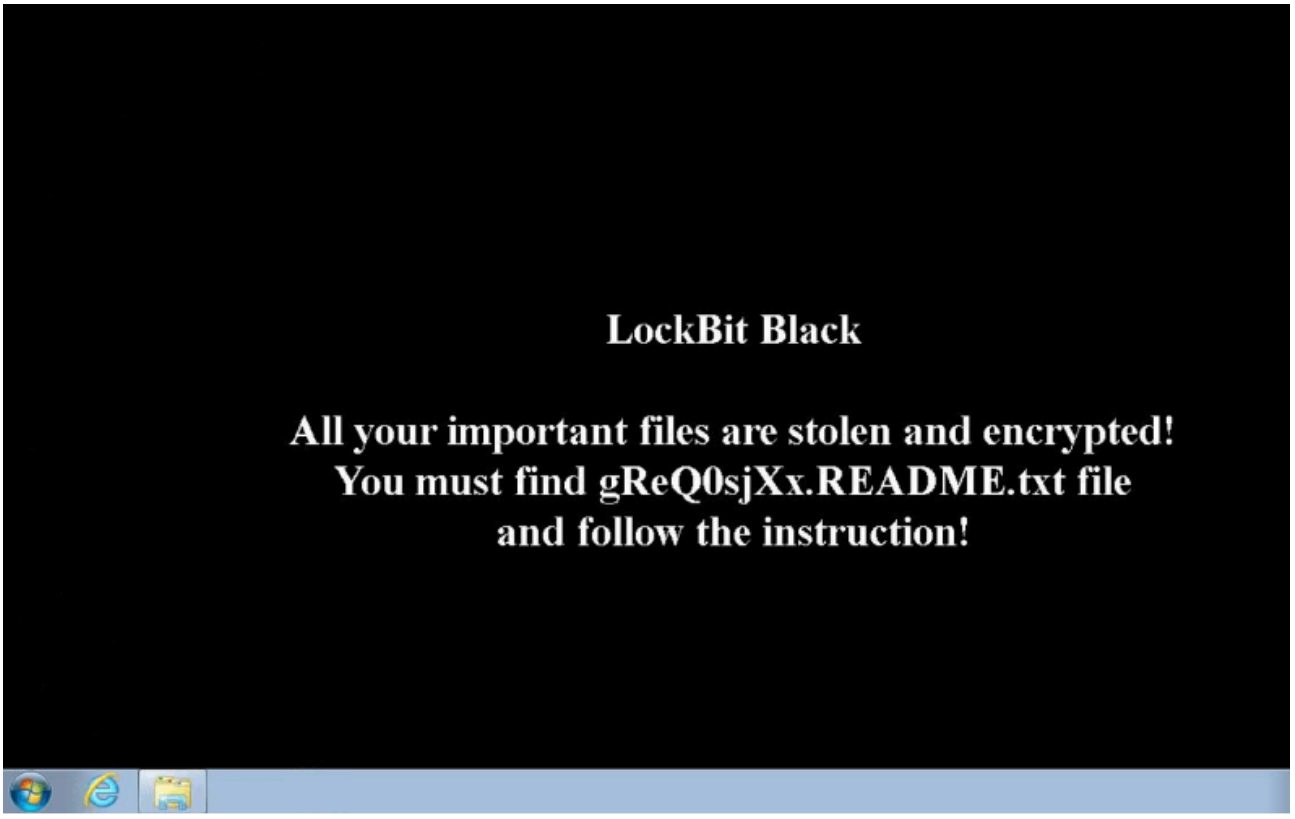


Figure 16. Desktop wallpaper replaced by LockBit 3.0

LockBit Green

The latest LockBit ransomware variant, "LockBit Green," appeared in January 2023. A random 8-character extension is now added to the LockBit Green extension, and LockBit Green leaves a ransom note titled, "!!!-Restore-My-Files-!!!.txt". This new variant also contains a new encryption tool based on the leaked Conti source code.

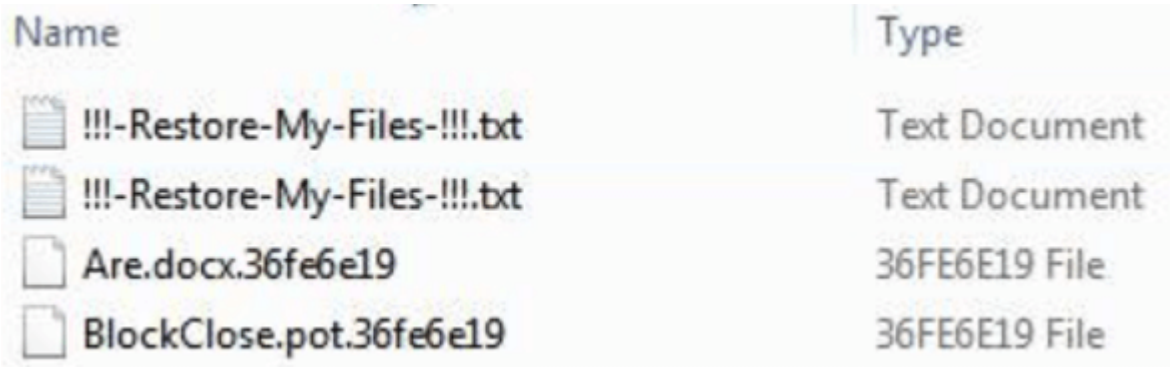


Figure 17. Files replaced by LockBit Green

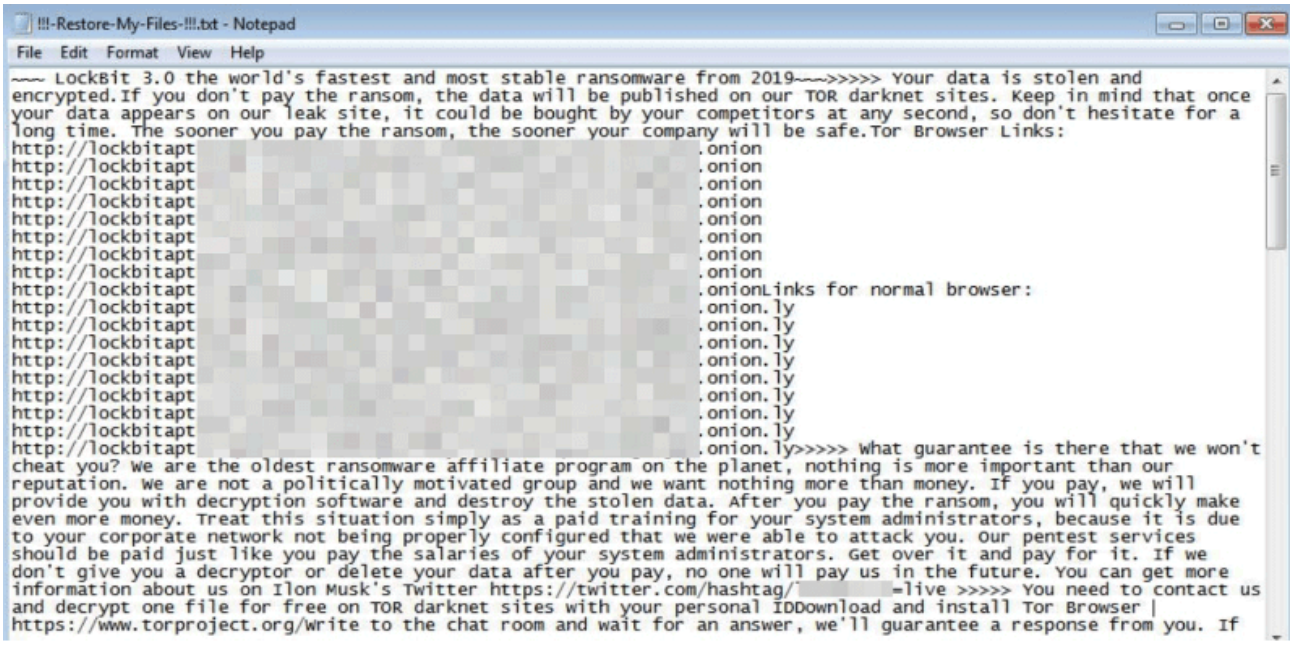


Figure 18. LockBit Green ransom note

The comprehensive LockBit Green ransom note is reproduced below, as the ransom note dropped by the ransomware is badly formatted.

~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion

hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion
hxxp://lockbitapt[redacted][.]onion

Links for normal browser:

hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitap[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly
hxxp://lockbitapt[redacted][.]onion.ly

>>>>> What guarantee is there that we won't cheat you?

We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter hxxps://twitter[.]com/hashtag/[redacted]?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser hxxps://www.torproject[.]org/

Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser personal link available only to you (available during a ddos attack):
hxxp://lockbitsup[redacted][.]onion

Tor Browser Links for chat (sometimes unavailable due to ddos attacks):

hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion

hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsupt[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion
hxxp://lockbitsup[redacted][.]onion

>>

>>>>> Your personal ID: [redacted] <<<<<

>>

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

>>>>> Don’t go to the police or the FBI for help and don’t tell anyone that we attacked you.

They won’t help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave a trail of crime. The police will try to prohibit you from paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and the FBI, they will eat more sweet coffee donuts and get fatter and fatter. The police and the FBI don’t care what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money. Along with this you should know that it is not necessarily your company that has to pay the ransom and not necessarily from your bank account, it can be done by an unidentified person, such as any philanthropist who loves your company, for example, Elon Musk, so the police will not do anything to you if someone pays the ransom for you. If you’re worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom. The police and FBI will not be able to stop lawsuits from your customers for leaking personal and private information. The police and FBI will not protect you from repeated attacks. Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.

>>>>> What are the dangers of leaking your company’s data.

First of all, you will receive fines from the government such as the GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the planet for various unpleasant things. For example, social engineering, your employees’ personal data can be used to re-infiltrate your company. Bank details and passports can be used to create bank accounts and online wallets through which criminal money will be laundered. On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your personal information could be used to make loans or buy appliances.

You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan. Your competitors may use the stolen information to steal technology or to improve their processes, your working methods, suppliers, investors, sponsors, employees, it will all be in the public domain. You won't be happy if your competitors lure your employees to other firms offering better wages, will you? Your competitors will use your information against you. For example, look for tax violations in the financial documents or any other violations, so you have to close your firm. According to statistics, two thirds of small and medium-sized companies close within half a year after a data breach. You will have to find and fix the vulnerabilities in your network, work with the customers affected by data leaks. All of these are very costly procedures that can exceed the cost of a ransomware buyout by a factor of hundreds. It's much easier, cheaper and faster to pay us the ransom. Well and most importantly, you will suffer a reputational loss, you have been building your company for many years, and now your reputation will be destroyed.

Read more about the GDRP legislation:
hxxps://en.wikipedia[.]org/wiki/General_Data_Protection_Regulation
hxxps://gdpr[.]eu/what-is-gdpr/
hxxps://gdpr-info[.]eu/

>>>>> Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.

We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.

>>>> Very important! For those who have cyber insurance against ransomware attacks.

Insurance companies require you to keep your insurance information secret, this is to never pay the maximum amount specified in the contract or to pay nothing at all, disrupting negotiations. The insurance company will try to derail negotiations in any way they can so that they can later argue that you will be denied coverage because your insurance does not cover the ransom amount. For example your company is insured for 10 million dollars, while negotiating with your insurance agent about the ransom he will offer us the lowest possible amount, for example 100 thousand dollars, we will refuse the paltry amount and ask for example the amount of 15 million dollars, the insurance agent will never offer us the top threshold of your insurance of 10 million dollars. He will do anything to derail negotiations and refuse to pay us out completely and leave you alone with your problem. If you told us anonymously that your company was insured for $10 million and other important details regarding insurance coverage, we would not demand more than $10 million in correspondence with the insurance agent. That way you would have avoided a leak and decrypted your Information. But since the sneaky insurance agent purposely negotiates so as not to pay for the insurance claim, only the insurance company wins in this situation. To avoid all this and get the money on the insurance, be sure to inform us anonymously about the availability and terms of insurance coverage, it benefits both you and us, but it does not benefit the insurance company. Poor multimillionaire insurers will not starve and will not become poorer from the payment of the maximum amount specified in the contract, because everyone knows that the contract is more expensive than money, so let them fulfill the conditions prescribed in your insurance contract, thanks to our interaction.

LockBit for MacOS

In April 2023, samples of LockBit for MacOS were submitted to a public file scanning service. Now that LockBit covers all major platforms (Windows, Linux, ESXi, and MacOS), LockBit developers look to stay one step ahead of competitors and further expand their influence.

Evidence that they plan to take their efforts further was uncovered in late 2022 when a post offering to purchase the Raccoon Stealer source code was discovered. This addition to their arsenal would enable them to integrate known infostealer code into the LockBit ransomware.

Infection Vector

LockBit's initial access vectors include exploiting vulnerabilities and exposed Remote Access Protocol (RDP), drive-by compromise, and the use of phishing and spear-phishing emails. The LockBit group is also known to purchase existing access to targeted organizations from initial access brokers on the dark web.

According to the CISA advisory, the LockBit ransomware group is reportedly exploiting the following N-day vulnerabilities:

- CVE-2023-0669 (Fortra GoAnywhere MFT License Response Servlet Command Injection)
- CVE-2023-27350 (PaperCut NG SetupCompleted Authentication Bypass Vulnerability)
- CVE-2021-44228 (Apache Log4j Error Log Remote Code Execution)
- CVE-2021-22986 (F5 iControl REST Interface Remote Command Execution Vulnerability)
- CVE-2020-1472 (Microsoft Windows Server Netlogon Elevation of Privilege Vulnerability)
- CVE-2019-0708 (Microsoft Windows Remote Desktop Services Remote Code Execution Vulnerability)
- CVE-2018-13379 (FortiOS SSL VPN Web Portal Pathname Information Disclosure Vulnerability)

Please note that there are patches available for all of these security vulnerabilities.

Post-Infection Activities

After LockBit affiliates gain access to victim environments, the attackers move laterally across compromised networks and exfiltrate information using various custom and dual-use tools, such as Stealbit and rclone, living-off-the-land tactics, and publicly available file-sharing services.

LockBit Data Leak Site

LockBit has a data leak site on TOR where LockBit affiliates can post information about victims and their stolen data.

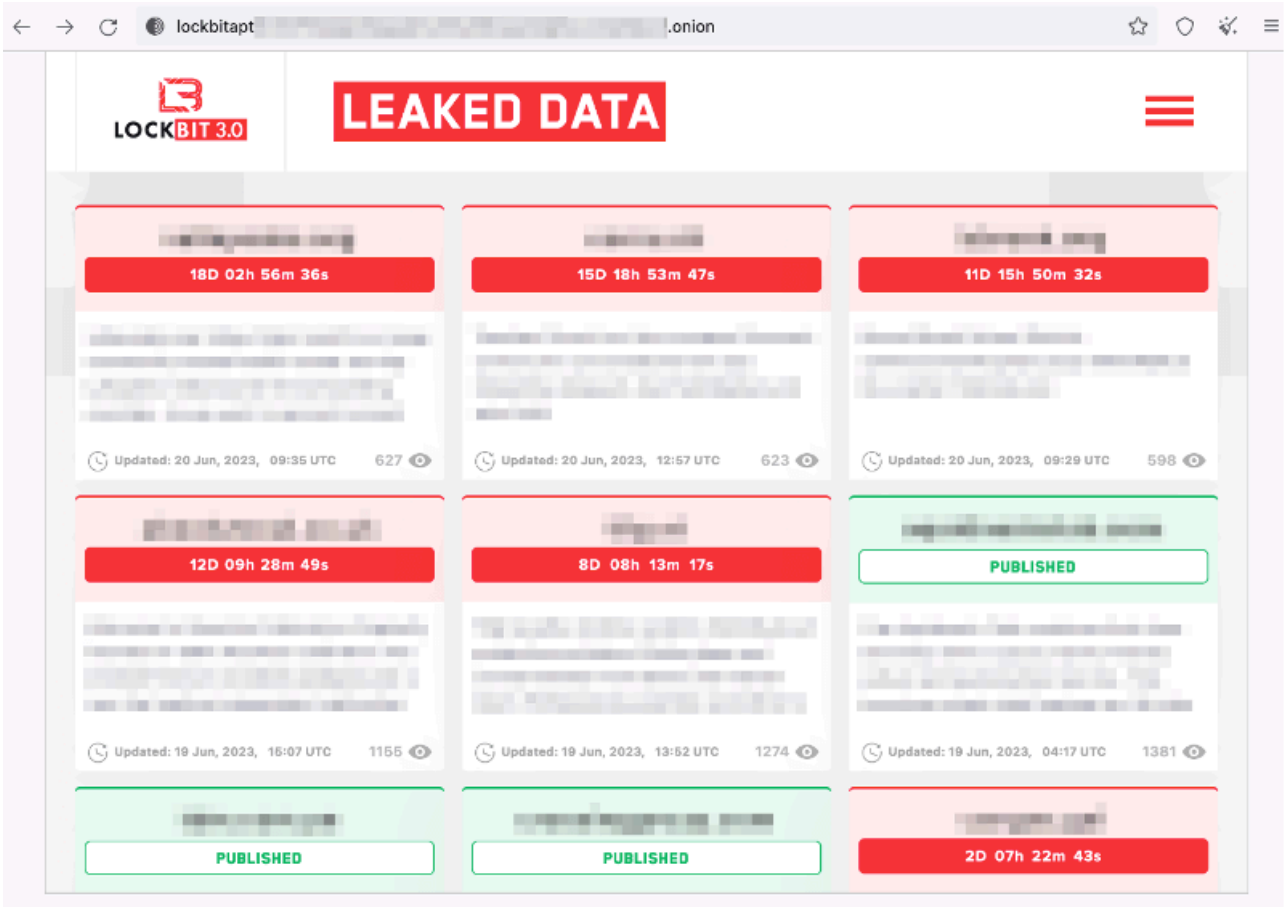


Figure 19. LockBit 3.0 data leak site

Each victim has their own page with a countdown timer and examples of stolen information. In some cases, LockBit threat actors offer to extend the ransom deadline, download stolen information, and destroy all copies for a fee.

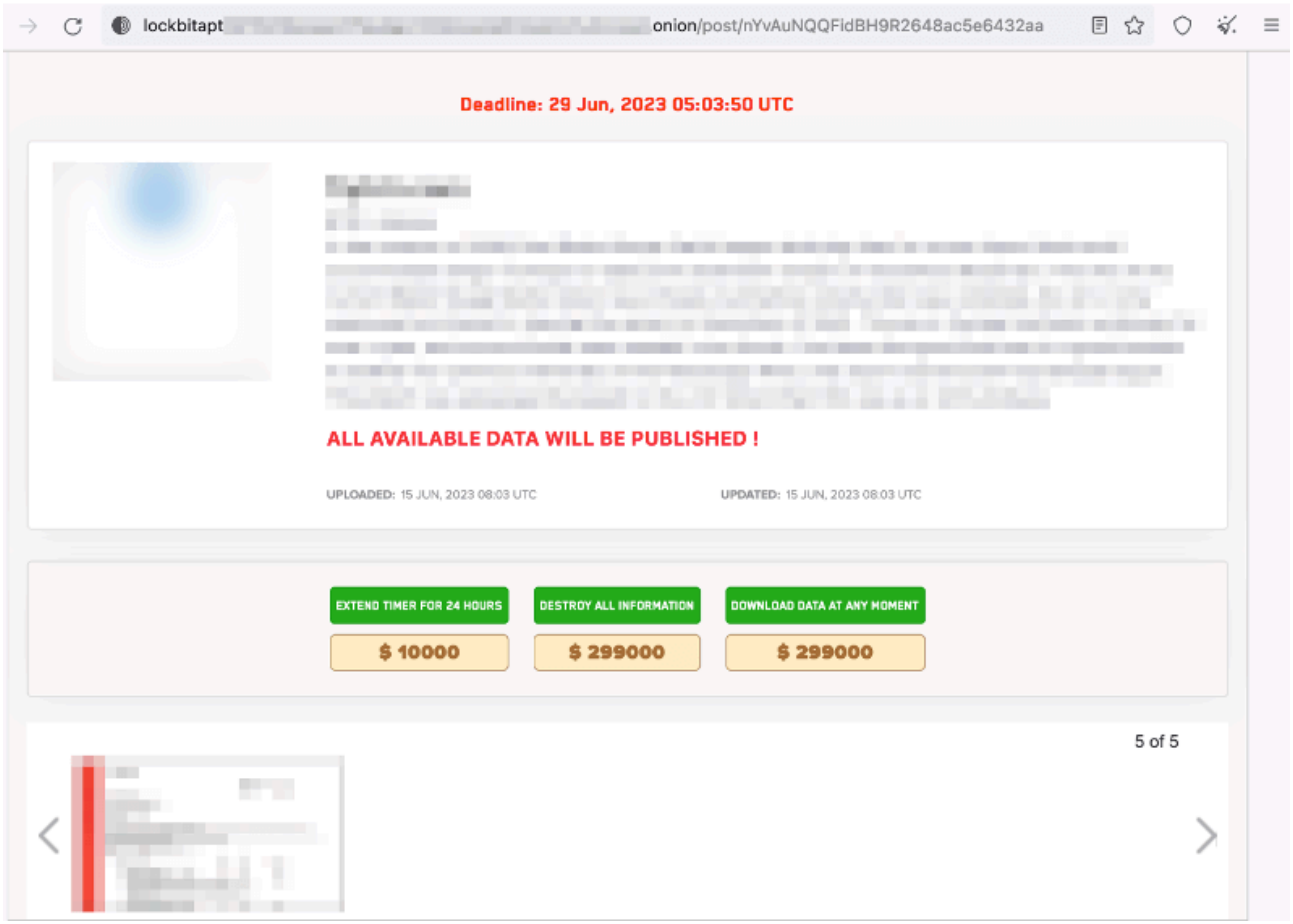


Figure 20. LockBit 3.0 data leak page

The LockBit group also offers a file-sharing service that supports files up to 2GB. The service also has options to automatically remove uploaded files after 24 hours, seven days, or on the first download, as well as a password setting.

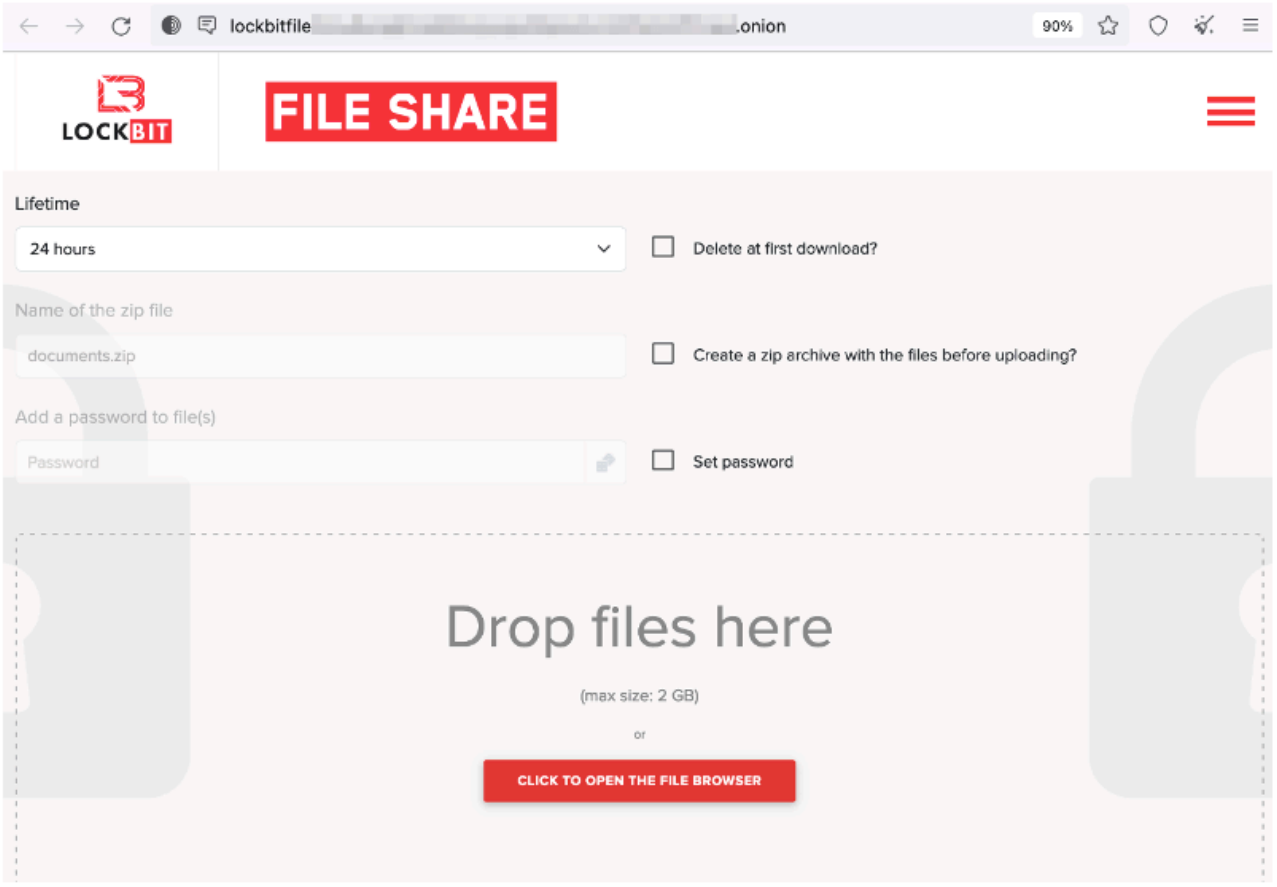


Figure 21. LockBit file-sharing service

A data leak page with search functionality is also available.

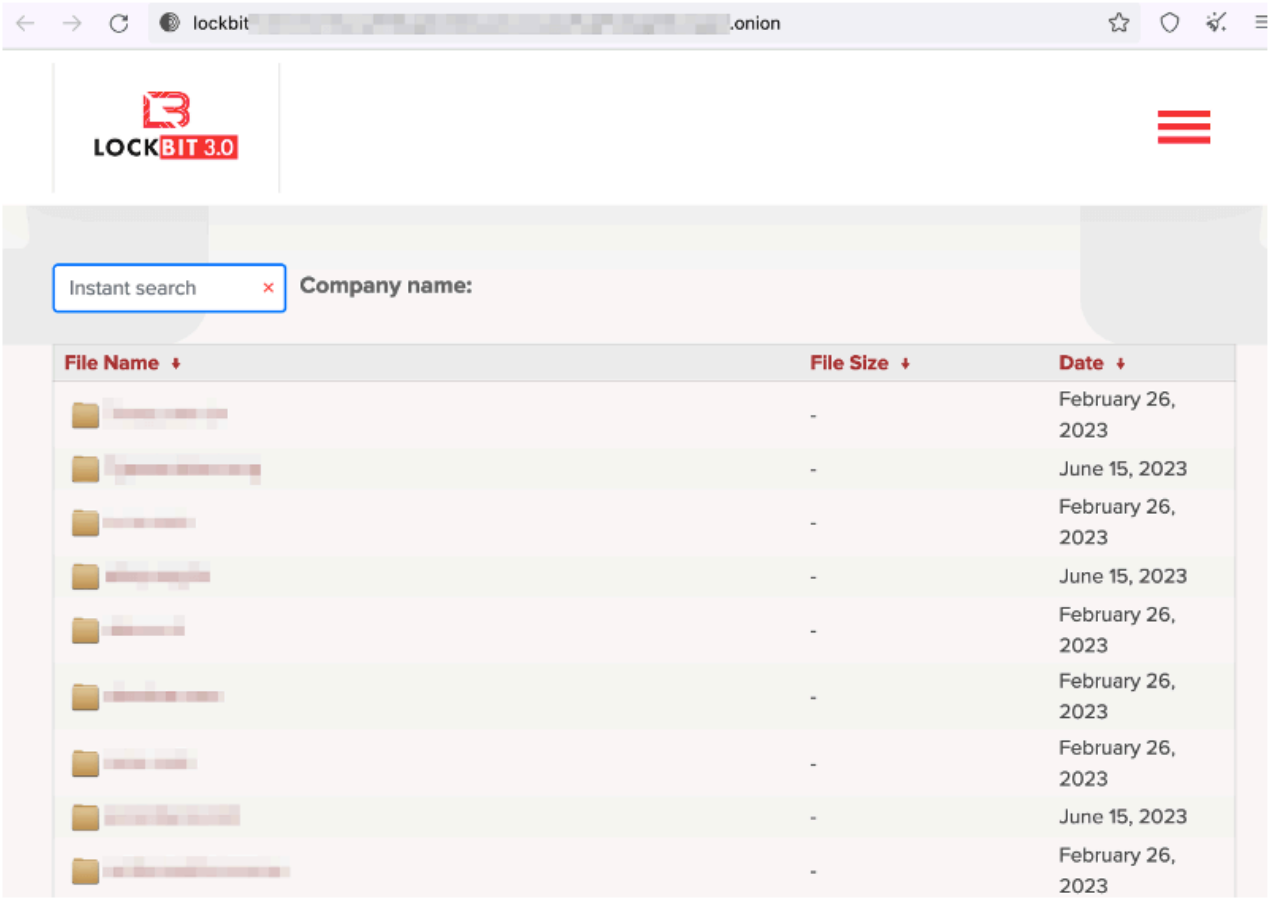


Figure 22. LockBit 3.0 data leak page

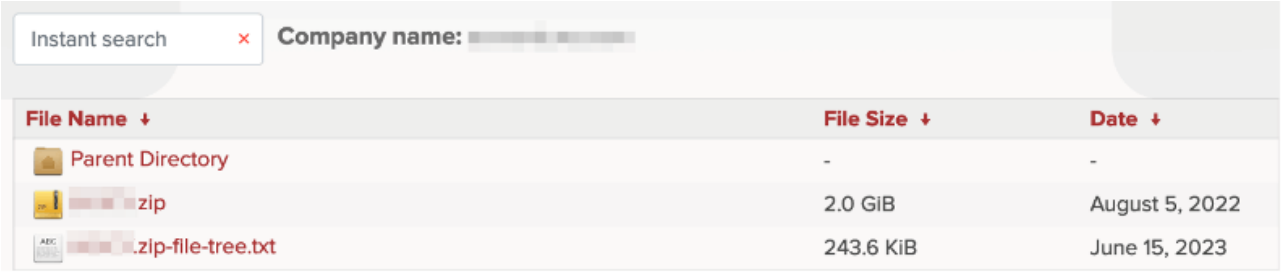


Figure 23. LockBit 3.0 data leak page for the victim company

The LockBit leak site was initially not as sophisticated as it is today—proof that the LockBit developer has put much effort into improving the site along with improvements to the ransomware code over the years. The below figure of the LockBit Data Leak site is courtesy of id-ransomware.

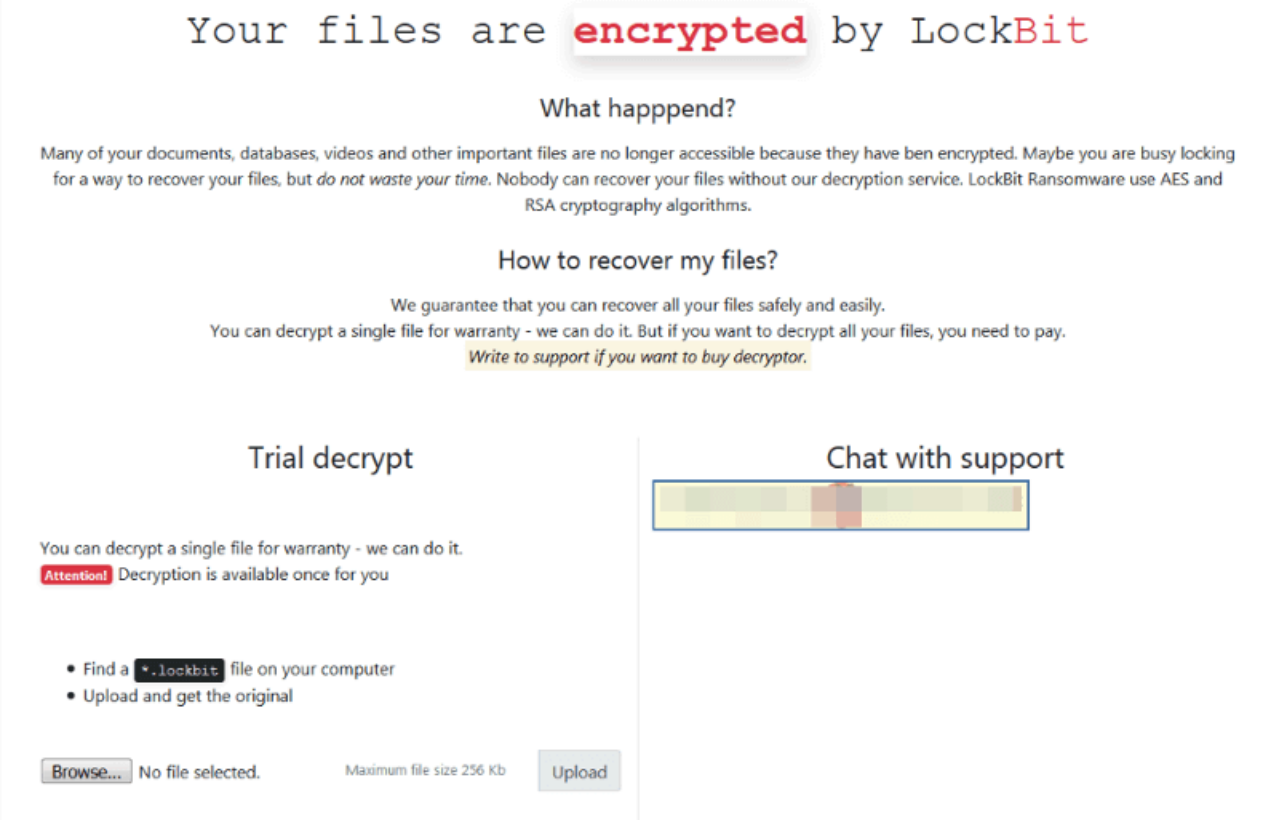


Figure 24. LockBit Data Leak Site in 2019 (courtesy of id-ransomware)

Conclusion

The LockBit Group has worked hard to improve its services to those who work with them. These efforts have enabled LockBit to remain at the forefront of the ransomware realm in terms of popularity and prevalence.

IOCs

Note that many LockBit ransomware samples exist due to the high prevalence of the ransomware over several years. Because of this, this section only contains up to 10 samples from each LockBit generation.

SHA2	Malware
13849c0c923bfed5ab37224d59e2d12e3e72f97dc7f539136ae09484cbe8e5e0	ABCD ransomware
49c0acf512146620dd26f515804324c8e4b4cc8eb8b9ab5d9c57e201241bc7ae	ABCD ransomware
4d0113884f70ddbbaf1ee0365602124ba91c11a76ff7bff5908d310aa9d3dfe9	ABCD ransomware

6fedf83e76d76c59c8ad0da4c5af28f23a12119779f793fd253231b5e3b00a1a	ABCD ransomware
70cb1a8cb4259b72b704e81349c2ad5ac60cd1254a810ef68757f8c9409e3ea6	ABCD ransomware
9595abf24d1fa80a476c2711cd788820e9f75da015c2c8726a0a44bca0444ddf	ABCD ransomware
b02d57f1c4f7f233044a56fdc57c89b6cc3661479dccc3b4cfa1f6f9d20cd893	ABCD ransomware
c8205792fbc0a5efc6b8f0f2257514990bfaa987768c4839d413dd10721e8871	ABCD ransomware
cff048ed06cf900170562906bded4a8fd166185a1b785f5ece0e2a842cf52d46	ABCD ransomware
ec88f821d22e5553afb94b4834f91ecdedeb27d9ebfd882a7d8f33b5f12ac38d	ABCD ransomware
0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76	LockBit ransomware
0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f	LockBit ransomware
0f178bc093b6b9d25924a85d9a7dde64592215599733e83e3bbc6df219564335	LockBit ransomware
0f5d71496ab540c3395cfc024778a7ac5c6b5418f165cc753ea2b2befbd42d51	LockBit ransomware
15a7d528587ffc860f038bb5be5e90b79060fbba5948766d9f8aa46381ccde8a	LockBit ransomware
286bffaa9c81abfb938fe65be198770c38115cdec95865a241f913769e9bfd3f	LockBit ransomware
410c884d883ebe2172507b5eadd10bc8a2ae2564ba0d33b1e84e5f3c22bd3677	LockBit ransomware
76a77def28acf51b2b7cdcbfaa182fe5726dd3f9e891682a4efc3226640b9c78	LockBit ransomware

e3f236e4aeb73f8f8f0caebe46f53abbb2f71fa4b266a34ab50e01933709e877	LockBit ransomware
faa3453ceb1bd4e5b0b10171eaa908e56e7275173178010fcc323fdea67a6869	LockBit ransomware
3f8ab65e3733ca62001500f7fcb83057869c869345affa4701fbd4d7207e6899	LockBit 2.0
4b09da2f1d94bc0fd2fd8be7b723172349e03e71117dfe483da06ac207f3e124	LockBit 2.0
5b5f3fc7bd943bd6bb575406018bf6401c6e6956ed92d54f634ba754e993d2d2	LockBit 2.0
897b23cc1af331a972da64e298163fbe0f1fd4d6bd983d452a889c1d285a1a27	LockBit 2.0
f35ba7686462a868a90bb8d9567e42e34064f91f54aeb5ed74b0d0b0e19badac	LockBit 2.0
059399f01e9bd588b42dbaf61c7a3b5aa6a48ba15a3ed13bdca7ce13a71a8526	LockBit 2.0
161c951e6d2e8d07571fc451a28a9feafb672c1f05586768f8178f33a9d74efb	LockBit 2.0
329e77a8a304e38ce4c4ed8906f9a7594377a3da64505fd1935b58acfc9ab4b9	LockBit 2.0
c6d3ff77910e991c6d782a3961c58ef69643c7d000b9c2d31e19904f2020dc6c	LockBit 2.0
ef870afba5951592f7d2964613a7819b9c92c7c6f6bd5c6fd2aa46978deaca34	LockBit 2.0
6aee637b88a06f7cc4813b47719717a64e39047f33617930a6cd11fc25fbca0a	LockBit 3.0
7d7357e4963c7d6f087a11e22d683cacf614dc7f269c2907bbb12ae30f2b007d	LockBit 3.0
97320395d90b28ad3d5cd0ed0416b0fe379cc0cc3d65f0b27e50db4da5902ec2	LockBit 3.0

cb537a122fb0531f14c76dfd0a87cc304c26a9ab01aec46a5fd17f268ac80854	LockBit 3.0
f1ecb57988caf26216683b1314607f06f8bf051632ff7ba73f17c2dc9b3aafcc	LockBit 3.0
072d0633006eeafc77c0b0144fdac84a57fa1e4f8b96d9aa33d377bd789bc533	LockBit 3.0
12b6fead37cca9d8ca4c00c2a9d56c0a402e760ab309356f078587acb7f33396	LockBit 3.0
58729cd09a74e3f69d26653b71412f9c9285ffaba52a9beb5b6d634014c98e1a	LockBit 3.0
aa0d0c6dcb69623ac4cfd87ecd991d8fe55807cec6628b92ba698844a24ba58e	LockBit 3.0
f02cf38d417fc6e3d5f9fc05ebf49ca37e6106ffc62ce21145888338598e0c70	LockBit 3.0
102679330f1e2cbf41885935ceeb2ab6596dae82925deec1aff3d90277ef6c8c	LockBit Green
32eb4b7a4d612fac62e93003811e88fbc01b64281942c25f2af2a0c63cdbe7fa	LockBit Green
5c5c5b25b51450a050f4b91cd2705c8242b0cfc1a0eaeb4149354dbb07979b83	LockBit Green
7509761560866a2f7496eb113954ae221f31bc908ffcbacad52b61346880d9f3	LockBit Green
924ec909e74a1d973d607e3ba1105a17e4337bd9a1c59ed5f9d3b4c25478fe11	LockBit Green
ac49a9ecd0932faea3659d34818a8ed4c48f40967c2f0988eeda7eb089ad93ca	LockBit Green
fc8668f6097560f79cea17cd60b868db581e51644b84f5ad71ba85c00f956225	LockBit Green
ffa0420c10f3d0ffd92db0091304f6ed60a267f747f4420191b5bfe7f4a513a9	LockBit Green

472836ed669d3927d50055e801048696375b37fce03b2f046e3e1039fb88e048	LockBit for Linux
dc3d08480f5e18062a0643f9c4319e5c3f55a2e7e93cd8eddd5e0c02634df7cf	LockBit for Linux
052716d193fc11c2f0deb67e35e580db335368d53cdd486f9cb1598c7021be8e	LockBit for Linux
2f31962c5e89917f6df87babd836840042b7ea7ea01763cff1bf645878a2ab47	LockBit for Linux
719e1e9289c78ed9ee5000bffdd26bc2a4473f966091e321919e333d81e8b1e6	LockBit for Linux
624188b7b839afe83d2cc6593448b73e94c40085671f967846ac3901c9f75249	LockBit for Linux
6a6c3a6eec55a1ec47badd05d6cfe6b4f8680c7f7bc6ee571c330a5b1ffdbc3a	LockBit for Linux
a0b36376ab6c54540d10e5d549049622096d121abec6f760e0452a535c1675f3	LockBit for Linux
3e4bbd21756ae30c24ff7d6942656be024139f8180b7bddd4e5c62a9dfbd8c79	LockBit for MacOS
0be6f1e927f973df35dad6fc661048236d46879ad59f824233d757ec6e722bde	LockBit for MacOS

Protection

FortiGuard Labs has the following AV signatures in place for the LockBit samples in the IOC section:

- W32/Filecoder.NXQ!tr.ransom
- W32/LockBit.29EA!tr.ransom
- W32/Filecoder.OAN!tr.ransom
- W32/Lockbit.C2F8!tr.ransom
- W32/Lockbit.K!tr.ransom
- W64/GenKryptik.FSFZ!tr.ransom
- Linux/Filecoder_LockBit.D!tr
- ELF/LockBit.D!tr.ransom
- Linux/Filecoder.BU!tr
- Linux/Filecoder_LockBit.B!tr

- Linux/Filecoder_LockBit_AGen.A!tr
- Linux/Filecoder_LockBit.A!tr
- OSX/Filecoder_Lockbit.A!tr

Additionally, the following AV signatures are available for LockBit samples:

- W32/Filecoder_Lockbit.A!tr
- W32/Filecoder_Lockbit.BHHHVJJ!tr.ransom
- W32/Filecoder_Lockbit.E!tr
- W32/Filecoder_Lockbit.E!tr.ransom
- W32/Filecoder_Lockbit.H!tr
- W32/Filecoder_Lockbit.H!tr.ransom
- W32/Filecoder_Lockbit.I!tr
- W32/Filecoder_Lockbit.I!tr.ransom
- W32/Filecoder_Lockbit.P!tr.ransom
- W32/Filecoder_Lockbit.Q!tr
- W32/Filecoder_Lockbit.Q!tr.ransom
- W32/Filecoder_Lockbit.R!tr
- W32/Filecoder_Lockbit.R!tr.ransom
- W32/Filecoder.LOCKBIT!tr
- W32/Filecoder.LOCKBIT!tr.ransom
- W32/LockBit.20D4!tr.ransom
- W32/LockBit.2513!tr.ransom
- W32/LockBit.29FC!tr.ransom
- W32/Lockbit.2D74!tr.ransom
- W32/LockBit.323D!tr.ransom
- W32/Lockbit.82C9!tr.ransom
- W32/LockBit.921B!tr.ransom
- W32/LockBit.B8275!tr.ransom
- W32/Lockbit.D!tr.ransom
- W32/Lockbit.E!tr.ransom
- W32/LockBit.E755!tr.ransom
- W32/LockBit.F84F!tr.ransom
- W32/Lockbit.P!tr.ransom
- W32/Lockbit.R!tr.ransom
- W32/Lockbit.VHO!tr.ransom
- W32/Predator.LOCKBIT!tr.ransom
- W32/Ransom_Lockbit.R002C0DD823
- W32/Ransom_Lockbit.R002C0DDP23
- W32/Ransom_Lockbit.R002C0DEB23
- W32/Ransom_Lockbit.R002C0DEC23
- W32/Ransom_Lockbit.R002C0DED23
- W32/Ransom_Lockbit.R002C0DF223!tr.ransom

- W32/Ransom_Lockbit.R023C0DEA23
- W32/Ransom_Win32_LOCKBIT.ENC
- W32/Ransom_Win32_LOCKBIT.EOD
- W32/Ransom_Win32_LOCKBIT.YXCGT
- W32/Ransom_Win32_LOCKBIT.YXCGUT
- W32/Ransom_Win32_LOCKBIT.YXCLQZ!tr.ransom
- W64/Lockbit.886F!tr.ransom
- W64/Lockbit.A!tr.ransom
- W64/LockBit.EF55!tr.ransom
- HTML/Lockbit.FCBE!tr.ransom
- MSIL/Lockbit.96B2!tr.ransom
- Data/Lockbit!tr.ransom
- Data/Lockbit.9AFA!tr.ransom

FortiGuard Labs has put the following IPS signatures in place for the vulnerabilities reportedly exploited by LockBit ransomware threat actors:

- Fortra.GoAnywhere.MFT.LicenseResponseServlet.Command.Injection (CVE-2023-0669)
- PaperCut.NG.SetupCompleted.Authentication.Bypass (CVE-2023-27350)
- Apache.Log4j.Error.Log.Remote.Code.Execution (CVE-2021-44228)
- F5.iControl.REST.Interface.Remote.Command.Execution (CVE-2021-22986)
- MS.Windows.Server.Netlogon.Elevation.of.Privilege (CVE-2020-1472)
- MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution (CVE-2019-0708)
- MS.Windows.Server.NTLM.Relay.Spoofing (CVE-2021-36942)
- ZK.Framework.Remote.Code.Execution (CVE-2022-36537)
- MS.Exchange.Server.Autodiscover.Remote.Code.Execution (CVE-2021-34473)
- MS.Exchange.Server.Common.Access.Token.Privilege.Elevation (CVE-2021-34523)
- MS.Exchange.MailboxExportRequest.Arbitrary.File.Write (CVE-2021-31207)
- FortiOS.SSL.VPN.Web.Portal.Pathname.Information.Disclosure (CVE-2018-13379)

Note: For more information on CVE-2018-13379, see the blog "Prioritizing Patching is Essential for Network Integrity."

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is generally delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted

phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations also need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Organizations are encouraged to implement cloud-based security solutions, such as SASE, to protect off-network devices, advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack, and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context. These solutions are proven to minimize risk and reduce the impact of a successful ransomware attack.

By operating these solutions as part of the industry's only fully integrated Security Fabric, organizations can also take advantage of native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings that can be deployed independently or as part of the Fortinet Security Fabric. These services are powered by advanced AI-enabled technologies and our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because the payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.
