



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



LockBit Ransomware

09/23/2021



- Introduction
- LockBit History
- LockBit v1.0 to v2.0
- Affiliate Program
- Interviews
- Victims
- Mitigations

Slides Key:



Non-Technical: Managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



LockBit Overview

- LockBit attack on Accenture
- Claims fastest encryption
- Claims fastest file stealer
- Use RaaS model
- In it for the long haul
- Keep aware of LockBit!





A History of Lockbit

LockBit
(ABCD)
Launched

Jan
2020

Begins
working with
Maze gang

Sep
2020

LockBit v2.0
Debuts

Aug
2021

Sep
2019

Begins RaaS
Affiliate
Program
advertising
on XSS

May
2020

Creates own
Leak Site

Jun
2021

Accenture
Attack





Lockbit v1.1

- IP-based geolocation
- Persistence via COM interface task scheduling and Windows registry hive
- Appending encrypted files with .abcd
- First ransom note version
- Debug file
- High CPU usage during encryption
- Use of exact copy of PhobosImpostor mutex

```
All your important files are encrypted!  
Any attempts to restore your files with the thrid-party software will be fatal for your files!  
RESTORE YOU DATA POSSIBLE ONLY BUYING private key from us.  
There is only one way to get your files back:
```

- ```
| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?E3D94FA5
| This link only works in Tor Browser!
| 3. Follow the instructions on this page
```

```
Attention!
```

```
Do not rename encrypted files.
```

```
Do not try to decrypt using third party software, it may cause permanent data loss.
```

```
Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
```

```
Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
```

```
Tor Browser user manual https://tb-manual.torproject.org/about
```

```
!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.
Don't forget about GDPR.
```





## Lockbit v1.2

- Extension changed from .abcd to .lockbit
- Debug function removed
- Packed ransomware
- Mutexes changed from static to dynamic
- Digitally signed

## Lockbit v1.3

- Ransom note updated

```
All your important files are encrypted!
There is only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

Contact information: pcabcd@countermail.com

Be sure to duplicate your message on the e-mail: recoverymanager@cock.li

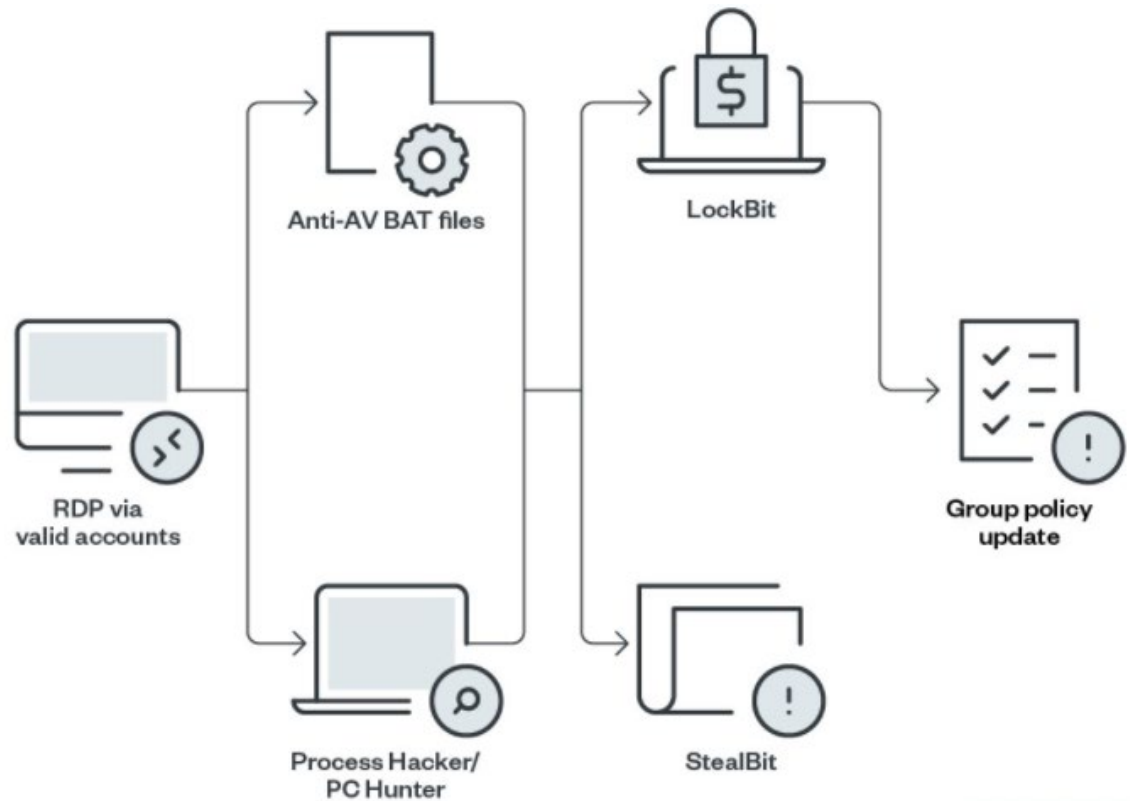
Your personal id:
B1PBs3MJinHk/XLbjMh6VYNN/q/Iq0WqJdHjTvaDCsktCkD0W0pAwdhPyb8RRb3d
3mlHm1AIRbxwA8b1hK50x9f+ehrt8IUVFcVIUfPQgeVXL10gwPhZQDAhcLPH/VD5
NTpA3N+wdJ179J2ynYKiZRz1JmooTt4kvjtp3Mr/kcG7Jd9FUdusTP3dVJla1pQ5
JCpdPtWzEba4CbbYU5k0mLHsw+uQEGUJt0saQzR9+PD7ZS8XMfwkf4VA/LIKYgZK
FRjLHYS8/zX03K0X/ku4XmmqsIfidaAbIAYExrluwU1ptEodLqVfJAK6T62FxFDH
fkmIQ46TEhcXc1a06ctivyMtVLS4LumK1qCUjK1EpBzjb0d6joJ0zUgPh9z5MgtU
bv5I/P4ZCa/8hb74wCYLC70PRaMPtWG7m0js+iPJEzybIH3mU01hc0HvUR8ktewE
lXzmX0DpYAN1/ef5Hw1t0gNTG63mrLXKN75C8+SqA20r3/3D7QCsxXVSmxEpQkKf
eoBrFS0xgirHokSxqIAAT2B2F4TMSq3NbpP5juLeySPE5F34DT1c/thqJVSd5Nsu
8zTs jKJdDoBHUFWVDM/ZwN0/ohC5Mn/EwDDy8a5Tmi0Ihxw6ltB+yuPM6bQDuha8
KreNbTgzJBuZr630mlp764cMdiHF6eWZQB0aFmGeBoy6df0+0zKZCnTs3KrbNdW
H2KR9qIQ5hnhK0AABtb2dfuRCHrKc+rKq4RXsa1DEhXkw1ck1v/nWv+z848sr0rD
mV/Hoyw4ilxiLWI5vsEU8rESUGMaJJTUAKMAVGh78Kkf+Q93bZBqhjmpAcc/PHdV
LQSA7Fesxsn4+5yL4ro364sWlmbFVc9xZpYs0RgKhZw6MQYv0kQnLKialG36KSur
RinffA36CV2NyaANBFxwazhchIACQDrqLpBzz0Xme/v89249qrXDF7W/SUsYHyP4
0zUDv8FI9jthi0K3uL9o+ZdJHSZcTpuw/enZ5eTxxlwfKJ2tJLuDGU1f677D0xAS
Tj20o35H8izESLkrxt/7LmgeSKXjROMKI6AB5jkzoHu5xKtaLiHUwckHwWU7CH+g
Tg5S0G82hXr61A25tTVUBmcm5LcnpYnLp8zkbW1V6+165SWr6ky13WnxJ4XIV1LN
nx9y6uL67580USbH8zCeHBPx0ke7YrsZEN0IuUSJ59+Bso0JBzNMMp5CWV6D1hsp
gJ9MxY9rz1HYvArCpXM2ZyvHhqRgvtDA/tCivzvYZw7venLkix0wNnjA56LLhW7
n1JCZ2KDcjEvKwWxuVQUf2a3IrVZNY3o/UVj66gjxr0opj0/KCpGp94khVRwA6BF
WqwJLxiK2lzmW8Rv4nD52kt9pi5JZ0kyEuorTeSPmV+7w9PL70YSWf/zNntc3Ezq
LIorjIcLSpSQfaP4tptN5lcmfB6ELw5+I90nCrqG+CgxoYS31CnY+KkKhuM54ft
ST32PHE6P/bU0LZ8q17IsLInkzuxXEsrmjvuxMbxax0KmjwzkkQ8riZL8B2Cq5JQ
8XPJc2e5B7hvX+8rvC2LUVXdo5Kzz+CwZUT0KNKsLf/viTEEFczf8u0gdhzbCUME
HUxCWwqbRH5FFmYKyqSsBPz6bw7ZzqPNEKJpCLa8E669tRzRs67eq2sGfwhwTh6
+fgaTMYCVfPxm8qe9yg3toGEQ8uUy5d21HLJHhlgzqc=
```



## Lockbit v2.0

- Released June 2021
- Now uses double extortion via StealBit malware
- Uses group policy update to encrypt networks
- Faster encryption
- Print bombing
- Wake-on-LAN feature
- New desktop wallpaper
- UAC bypass

### Standard LockBit v2.0 infection chain



©2021 TREND MICRO



## Restarted Affiliated Program

- Affiliates set own ransom
- Choose method of payment
- Collect 80% of ransom
- Don't work in Commonwealth of Independent States (CIS) countries
- Only experienced pentesters (penetration testers) need apply
- Affiliate receives payment directly from victim, then pays LockBit gang







## [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;

\*Actor's claims



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 computer 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:

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



# Encryption Speed Chart from the Affiliate Program



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

PC for testing: Windows Server 2016 x64 | 8 core Xeon E5-2680@2.40GHz | 16 GB RAM | SSD

| Name of the ransomware | Date of a sample    | Speed in megabytes per second | Time spent for encryption of 100 GB | Time spent for encryption of 10 TB | Self spread | Size sample in KB | The number of the encrypted files (All file in a system 257472) |
|------------------------|---------------------|-------------------------------|-------------------------------------|------------------------------------|-------------|-------------------|-----------------------------------------------------------------|
| <b>LOCKBIT 2.0</b>     | <b>5 Jun, 2021</b>  | <b>373 MB/s</b>               | <b>4M 28S</b>                       | <b>7H 26M 40S</b>                  | <b>Yes</b>  | 855 KB            | 109964                                                          |
| <b>LOCKBIT</b>         | <b>14 Feb, 2021</b> | <b>266 MB/s</b>               | <b>6M 16S</b>                       | <b>10H 26M 40S</b>                 | <b>Yes</b>  | 146 KB            | 110029                                                          |
| <b>Cuba</b>            | 8 Mar, 2020         | 185 MB/s                      | 9M                                  | 15H                                | No          | 1130 KB           | 110468                                                          |
| <b>BlackMatter</b>     | 2 Aug, 2021         | 185 MB/s                      | 9M                                  | 15H                                | No          | 67 KB             | 111018                                                          |
| <b>Babuk</b>           | 20 Apr, 2021        | 166 MB/s                      | 10M                                 | 16H 40M                            | <b>Yes</b>  | 79 KB             | 109969                                                          |
| <b>Sodinokibi</b>      | 4 Jul, 2019         | 151 MB/s                      | 11M                                 | 18H 20M                            | No          | 253 KB            | 95490                                                           |
| <b>Ragnar</b>          | 11 Feb, 2020        | 151 MB/s                      | 11M                                 | 18H 20M                            | No          | 40 KB             | 110651                                                          |
| <b>NetWalker</b>       | 19 Oct, 2020        | 151 MB/s                      | 11M                                 | 18H 20M                            | No          | 902 KB            | 109892                                                          |
| <b>MAKOP</b>           | 27 Oct, 2020        | 138 MB/s                      | 12M                                 | 20H                                | No          | 115 KB            | 111002                                                          |
| <b>RansomEXX</b>       | 14 Dec, 2020        | 138 MB/s                      | 12M                                 | 20H                                | No          | 156 KB            | 109700                                                          |
| <b>Pysa</b>            | 8 Apr, 2021         | 128 MB/s                      | 13M                                 | 21H 40M                            | No          | 500 KB            | 108430                                                          |
| <b>Avaddon</b>         | 9 Jun, 2020         | 119 MB/s                      | 14M                                 | 23H 20M                            | No          | 1054 KB           | 109952                                                          |
| <b>Thanos</b>          | 23 Mar, 2021        | 119 MB/s                      | 14M                                 | 23H 20M                            | No          | 91 KB             | 81081                                                           |
| <b>Ranzy</b>           | 20 Dec, 2020        | 111 MB/s                      | 15M                                 | 1D 1H                              | No          | 138 KB            | 109918                                                          |
| <b>PwndLocker</b>      | 4 Mar, 2020         | 104 MB/s                      | 16M                                 | 1D 2H 40M                          | No          | 17 KB             | 109842                                                          |
| <b>Sekhmet</b>         | 30 Mar, 2020        | 104 MB/s                      | 16M                                 | 1D 2H 40M                          | No          | 364 KB            | random extension                                                |
| <b>Sun Crypt</b>       | 26 Jan, 2021        | 104MB/s                       | 16M                                 | 1D 2H 40M                          | No          | 1422 KB           | random extension                                                |
| <b>REvil</b>           | 8 Apr, 2021         | 98 MB/s                       | 17M                                 | 1D 4H 20M                          | No          | 121 KB            | 109789                                                          |
| <b>Conti</b>           | 22 Dec, 2020        | 98 MB/s                       | 17M                                 | 1D 4H 20M                          | <b>Yes</b>  | 186 KB            | 110220                                                          |
| <b>Hive</b>            | 17 Jul, 2021        | 92 MB/s                       | 18M                                 | 1D 6H                              | No          | 808 KB            | 81797                                                           |
| <b>Ryuk</b>            | 21 Mar, 2021        | 92 MB/s                       | 18M                                 | 1D 6H                              | <b>Yes</b>  | 274 KB            | 110784                                                          |
| <b>Zeppelin</b>        | 8 Mar, 2021         | 92 MB/s                       | 18M                                 | 1D 6H                              | No          | 813 KB            | 109963                                                          |
| <b>DarkSide</b>        | 1 May, 2021         | 83 MB/s                       | 20M                                 | 1D 9H 20M                          | No          | 30 KB             | 100549                                                          |
| <b>DarkSide</b>        | 16 Jan, 2021        | 79 MB/s                       | 21M                                 | 1D 11H                             | No          | 59 KB             | 100171                                                          |
| <b>Nephilim</b>        | 31 Aug, 2020        | 75 MB/s                       | 22M                                 | 1D 12H 40M                         | No          | 3061 KB           | 110404                                                          |
| <b>DearCry</b>         | 13 Mar, 2021        | 64 MB/s                       | 26M                                 | 1D 19H 20M                         | No          | 1292 KB           | 104547                                                          |
| <b>MountLocker</b>     | 20 Nov, 2020        | 64 MB/s                       | 26M                                 | 1D 19H 20M                         | <b>Yes</b>  | 200 KB            | 110367                                                          |
| <b>Nemty</b>           | 3 Mar, 2021         | 57 MB/s                       | 29M                                 | 2D 0H 20M                          | No          | 124 KB            | 110012                                                          |
| <b>MedusaLocker</b>    | 24 Apr, 2020        | 53 MB/s                       | 31M                                 | 2D 3H 40M                          | <b>Yes</b>  | 661 KB            | 109615                                                          |
| <b>Phoenix</b>         | 29 Mar, 2021        | 52 MB/s                       | 32M                                 | 2D 5H 20M                          | No          | 1930 KB           | 110026                                                          |
| <b>Hades</b>           | 29 Mar, 2021        | 47 MB/s                       | 35M                                 | 2D 10H 20M                         | No          | 1909 KB           | 110026                                                          |
| <b>DarkSide</b>        | 18 Dec, 2020        | 45 MB/s                       | 37M                                 | 2D 13H 40M                         | No          | 17 KB             | 114741                                                          |
| <b>Babuk</b>           | 4 Jan, 2021         | 45 MB/s                       | 37M                                 | 2D 13H 40M                         | <b>Yes</b>  | 31 KB             | 110760                                                          |
| <b>REvil</b>           | 7 Apr, 2021         | 37 MB/s                       | 45M                                 | 3D 3H                              | No          | 121 KB            | 109790                                                          |
| <b>BlackKingdom</b>    | 23 Mar, 2021        | 32 MB/s                       | 52M                                 | 3D 14H 40M                         | No          | 12460 KB          | random extension                                                |
| <b>Avos</b>            | 18 Jul, 2021        | 29 MB/s                       | 59M                                 | 4D 2H                              | No          | 402 KB            | 79486                                                           |

\*Actor's claims





## StealBit performance comparison chart

### Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

| Downloading method        | Speed in megabytes per second | Compression in real time | Hidden mode | drag'n'drop | Time spent for downloading of 10 GB | Time spent for downloading of 100 GB | Time spent for downloading of 10 TB |
|---------------------------|-------------------------------|--------------------------|-------------|-------------|-------------------------------------|--------------------------------------|-------------------------------------|
| <b>Stealer - StealBIT</b> | <b>83,46 MB/s</b>             | <b>Yes</b>               | <b>Yes</b>  | <b>Yes</b>  | <b>1M 59S</b>                       | <b>19M 58S</b>                       | <b>1D 9H 16M 57S</b>                |
| Rclone pcloud.com free    | 4,82 MB/s                     | No                       | No          | No          | 34M 34S                             | 5H 45M 46S                           | 24D 18M 8S                          |
| Rclone pcloud.com premium | 4,38 MB/s                     | No                       | No          | No          | 38M 3S                              | 6H 20M 31S                           | 26D 10H 11M 45S                     |
| Rclone mail.ru free       | 3,56 MB/s                     | No                       | No          | No          | 46M 48S                             | 7H 48M 9S                            | 32D 12H 16M 28S                     |
| Rclone mega.nz free       | 2,01 MB/s                     | No                       | No          | No          | 1H 22M 55S                          | 13H 48M 11S                          | 57D 13H 58M 44s                     |
| Rclone mega.nz PRO        | 1,01 MB/s                     | No                       | No          | No          | 2H 45M                              | 1D 03H 30M 9S                        | 114D 14H 16M 30S                    |
| Rclone yandex.ru free     | 0,52 MB/s                     | No                       | No          | No          | 5H 20M 30S                          | 2D 05H 25M 7S                        | 222D 13H 52M 49S                    |

\*Actor's claims





# Interview with a LockBit ransomware operator

By Azim Khodjibaev,  
Dmytro Korzhevin and Kendall McKay





## Key Takeaways by Cisco Talos

- Threat actors continue to view unpatched systems as an easy, if not preferred, method of intrusion.
- Many cybercriminals rely almost exclusively on common open-source tools that are readily available on the internet and easy to use.
- Cybercriminals are avid consumers of security news and remain up to date on the latest research and vulnerabilities, weaponizing that information to use in future attacks.
- While threat actors may state publicly that their personal ethics influence their target selection, many adversaries go after the easiest victims regardless of any moral obligation, based on our experience.





## LockBit Affiliate Claims

- The actor appears to have a contradictory code of ethics, portraying a strong disdain for those who attack health care entities, while displaying conflicting evidence about whether he targets them himself.
- Hospitals are considered easy targets.
- Maze formerly kept up to 35% of ransom profits earned by its affiliates.
- The EU's General Data Protection Regulation (GDPR) law plays to adversaries' favor.
- The U.S. also has lucrative targets, but with data privacy laws requiring victim companies to report all breaches, the incentive for such entities to pay the ransom is likely somewhat reduced.



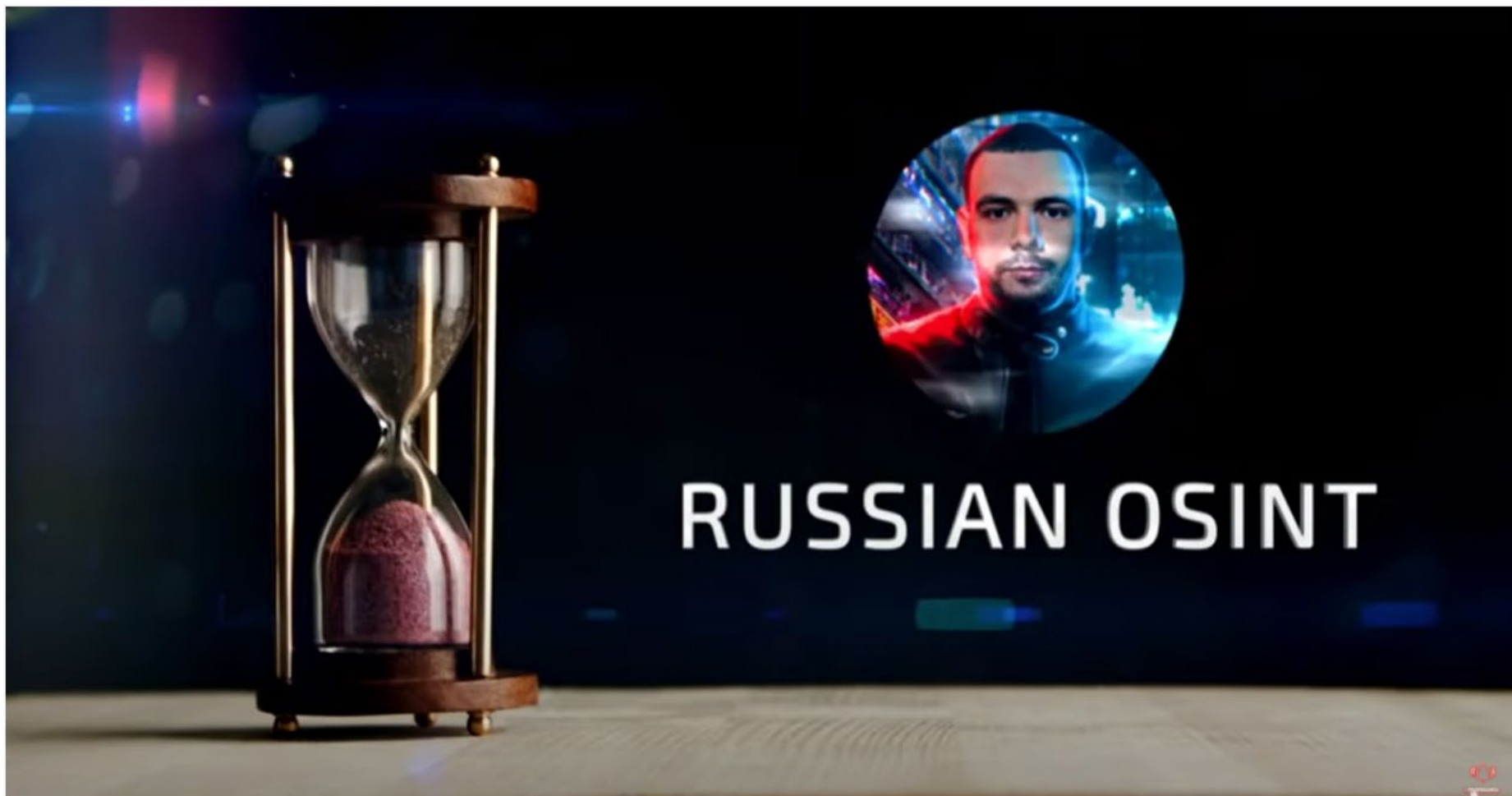




### Confirmed Theories

- Maze was once a franchise/affiliate program.
- A selection process existed for Maze and still does for LockBit.
- LockBit has a profit-sharing requirement that the affiliate has to meet for the first four or five ransoms.
- Keeping your word to the victim is an important part of LockBit's business model.

A large, 3D-style red stamp with the word "ANSWERS" in white, bold, capital letters. The stamp is tilted slightly upwards to the right and has a black pushpin pinned to its top edge.





## Key Takeaways

1. The U.S. and EU remain top targets.
2. The pandemic has been a boon.
3. Why victims choose to pay a ransom.
4. Expect more supply chain attacks.
5. Victims without backups are more likely to pay.
6. Ransomware bans have not disrupted established operations.
7. Multiple cryptocurrencies are accepted.
8. Criminals prefer public silence.
9. Attacks are now more automated.

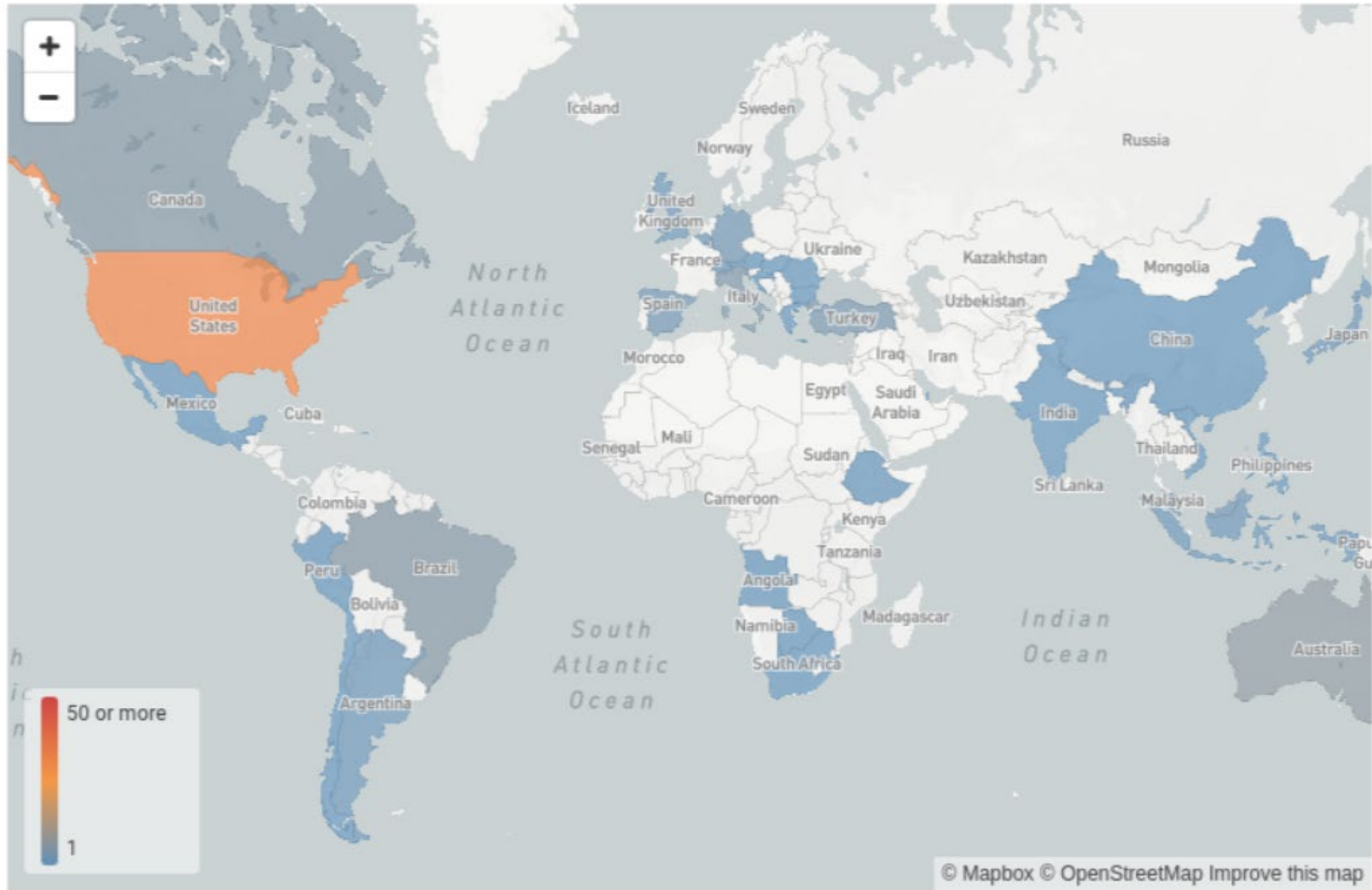
“We do not attack healthcare, education, charitable organizations, social services – everything that contributes to the development of personality and sensible values from the survival of the species perspective.” - LockBitSupp



“Employ a full-time red team, regularly update all software, perform preventive talks with a company's employees to thwart social engineering and ... use the best ransomware-fighting antivirus.”

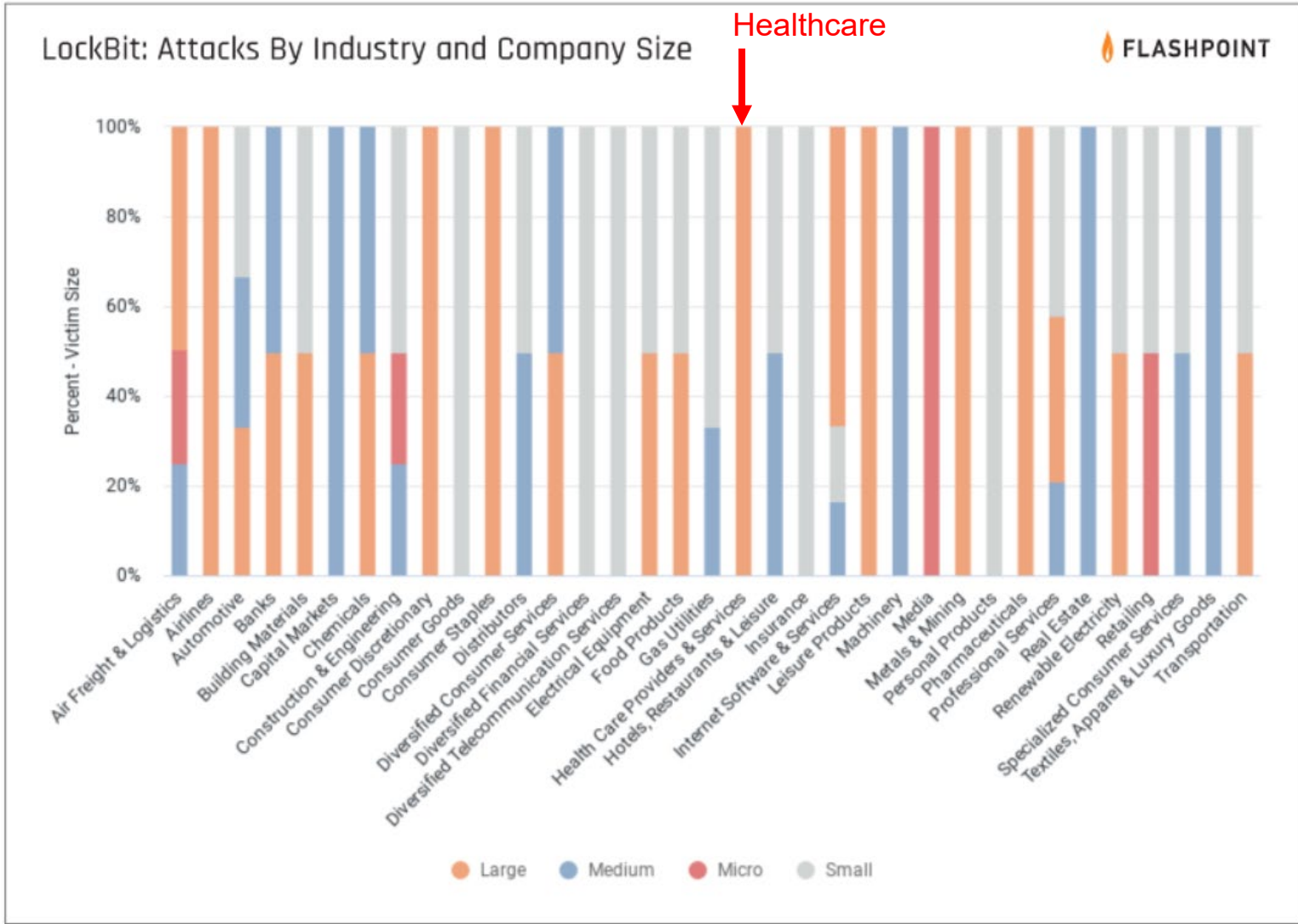


## LockBit: Attacks By Country



© Mapbox © OpenStreetMap Improve this map







"Through our security controls and protocols, we identified irregular activity in one of our environments. We immediately contained the matter and isolated the affected servers.



We fully restored our affected systems from backup, and there was no impact on Accenture's operations, or on our clients' systems." – Accenture



## General efforts to help prevent ransomware attacks include:

1. Maintain offline, encrypted backups of data and regularly test your backups.
2. Create, maintain, and exercise a basic cyber incident response plan, resiliency plan, and associated communications plan.
3. Mitigate internet-facing vulnerabilities and misconfigurations.
4. Reduce the risk of phishing emails from reaching end users.
5. Practice good cyber hygiene.

## Specific efforts to help prevent LockBit ransomware attacks include:

1. Monitoring for, and alerting on, the anomalous execution of legitimate Windows command line tools such as the use of net.exe, taskkill.exe, vssadmin.exe and wmic.exe.
2. Making use of network segregation to limit communications between nodes, especially endpoints, to provide damage limitation and limit the propagation of threats.

CISA ransomware tips: [https://www.cisa.gov/sites/default/files/publications/CISA\\_Fact\\_Sheet-Protecting\\_Sensitive\\_and\\_Personal\\_Information\\_from\\_Ransomware-Caused\\_Data\\_Breaches-508C.pdf](https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf)



# Reference Materials





- Abrams, Lawrence. “LockBit ransomware now encrypts Windows domains using group policies,” Bleeping Computer. 27 July 2021. <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/>
- Abrams, Lawrence. “LockBit ransomware recruiting insiders to breach corporate networks,” Bleeping Computer. 4 August 2021. <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/>
- Bernardo, Jett Paulo, et al. “LockBit Resurfaces With Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK,” Trend Micro. 16 August 2021. [https://www.trendmicro.com/de\\_de/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html](https://www.trendmicro.com/de_de/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html)
- Blackberry. “Threat Spotlight: LockBit 2.0 Ransomware Takes on Top Consulting Firm,” 12 August 2021. <https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm>
- Curated Intelligence. “LockBit 2.0 ransomware attack analysis,” 11 September 2021. <https://www.curatedintel.org/2021/09/lockbit-20-ransomware-attack-analysis.html>
- Cyberint. “LockBit Ransomware hits again,” 26 August 2021. <https://blog.cyberint.com/lockbit-ransomware>
- Emsisoft. “Ransomware Profile: LockBit,” 21 July 2021. <https://blog.emsisoft.com/en/38915/ransomware-profile-lockbit/>
- Flashpoint. “What Does LockBit Want? Decrypting an Interview With the Ransomware Collective,” 31 August 2021. <https://www.flashpoint-intel.com/blog/what-does-lockbit-want-decrypting-an-interview-with-the-ransomware-collective/>



- Gallagher, Sean. “LockBit uses automated attack tools to identify tasty targets,” Sophos. 21 October 2021. <https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/>
- Heinemeyer, Max. “LockBit ransomware analysis: Rapid detonation using a single compromised credential,” Darktrace. 25 February 2021. <https://www.darktrace.com/en/blog/lock-bit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential/>
- Herjavec Group. “Herjavec Group LockBit 2.0 Ransomware Profile,” 23 August 2021. <https://www.herjavecgroup.com/herjavec-group-lockbit-2-0-ransomware-profile/>
- KELA. “LockBit 2.0 Interview with Russian OSINT,” 24 August 2021. <https://ke-la.com/lockbit-2-0-interview-with-russian-osint/>
- Khodjibaev, Azim, Korzhevin, Dmytro, and McKay, Kendall. “Interview with a LockBit ransomware operator,” Talos Intelligence Site. 4 January 2021. [https://talos-intelligence-site.s3.amazonaws.com/production/document\\_files/files/000/095/481/original/010421\\_LockBit\\_Interview.pdf](https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf)
- Nocturnus, Cybereason. “Cybereason vs. LockBit2.0 Ransomware,” Cybereason. 24 August 2021. <https://www.cybereason.com/blog/cybereason-vs.-lockbit2.0-ransomware>
- Paganini, Pierluigi. “The LockBit 2.0 ransomware attack against Accenture - time is running out,” CyberNews. 25 August 2021. <https://cybernews.com/security/the-lockbit-2-0-ransomware-attack-against-accenture-time-is-running-out/>
- Prodaft. “LockBit RaaS In-Depth Analysis,” 19 June 2021. [https://www.prodaft.com/m/reports/LockBit\\_Case\\_Report\\_TLPWHITE.pdf](https://www.prodaft.com/m/reports/LockBit_Case_Report_TLPWHITE.pdf)



- RiveroLopez, Marc. “Tales From the Trenches; a Lockbit Ransomware Story,” McAfee. 30 April 2020. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/>
- Roddie, Megan. “LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment,” Security Intelligence. 9 September 2021. <https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/>
- Russian OSINT. “INTERVIEW WITH LOCKBIT 2.0: SECRET BUSINESS OF COMPANIES WITH RANSOMWARE GROUPS / RUSSIAN OSINT,” YouTube. 23 August 2021. <https://www.youtube.com/watch?v=ldgmx4ZCfFg>
- Schwartz, Mathew J. “9 Takeaways: LockBit 2.0 Ransomware Rep 'Tells All',” Bank Info Security. 25 August 2021. <https://www.bankinfosecurity.com/blogs/9-takeaways-lockbit-20-ransomware-rep-tells-all-p-3098>
- Seals, Tara. “LockBit 2.0 Ransomware Proliferates Globally,” Threatpost. 17 August 2021. <https://threatpost.com/lockbit-ransomware-proliferates-globally/168746/>
- Sumeetha, Surojoy. “CSW Analysis: Accenture attacked by LockBit 2.0 Ransomware,” Cyber Security Works. 19 August 2021. <https://cybersecurityworks.com/blog/ransomware/csw-analysis-accenture-attacked-by-lockbit-2-0-ransomware.html>
- Zsigovits, Albert. “LockBit ransomware borrows tricks to keep up with REvil and Maze,” Sophos. 24 April 2020. <https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/>



**Questions**



## Upcoming Briefs

- 10/7 – Blockchain for Healthcare

## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the [HC3 Customer Feedback Survey](#).

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

## Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.



*HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector*

### Products



#### Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.



#### White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.



#### Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV), or visit us at [www.HHS.Gov/HC3](http://www.HHS.Gov/HC3).



# Contact



[www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)



[HC3@HHS.GOV](mailto:HC3@HHS.GOV)