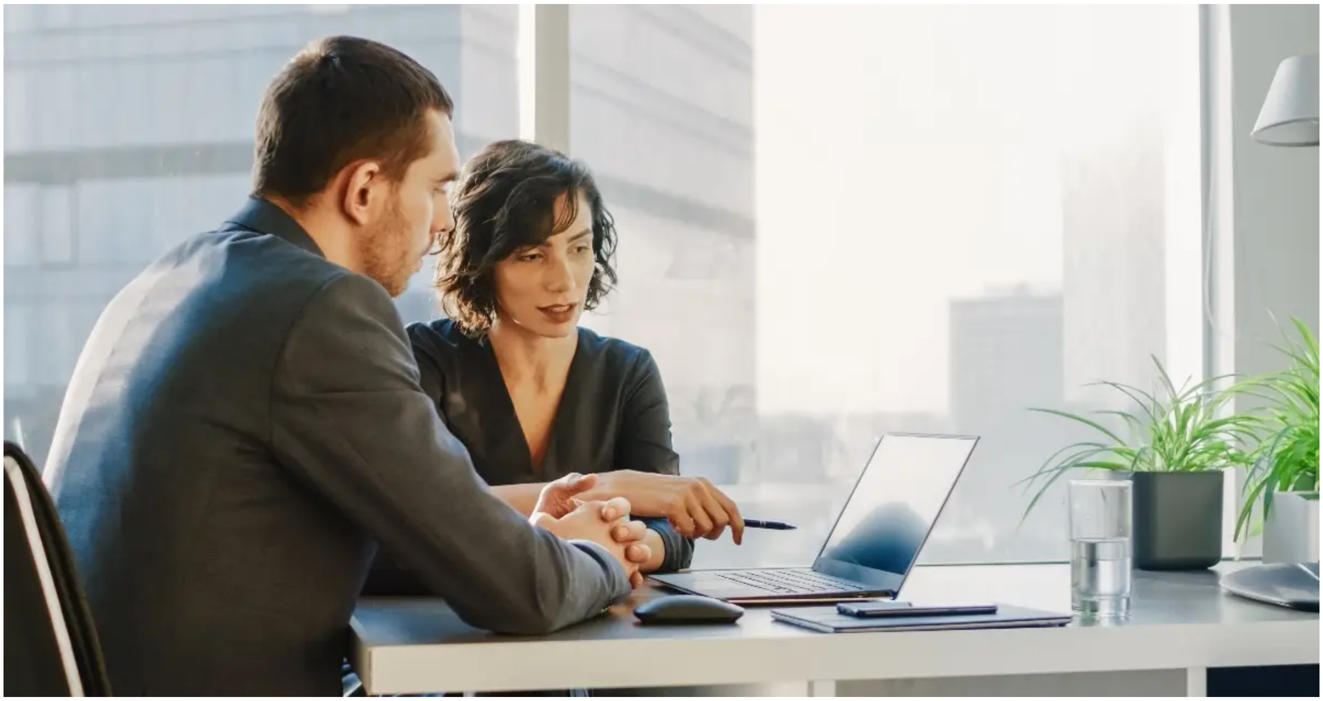
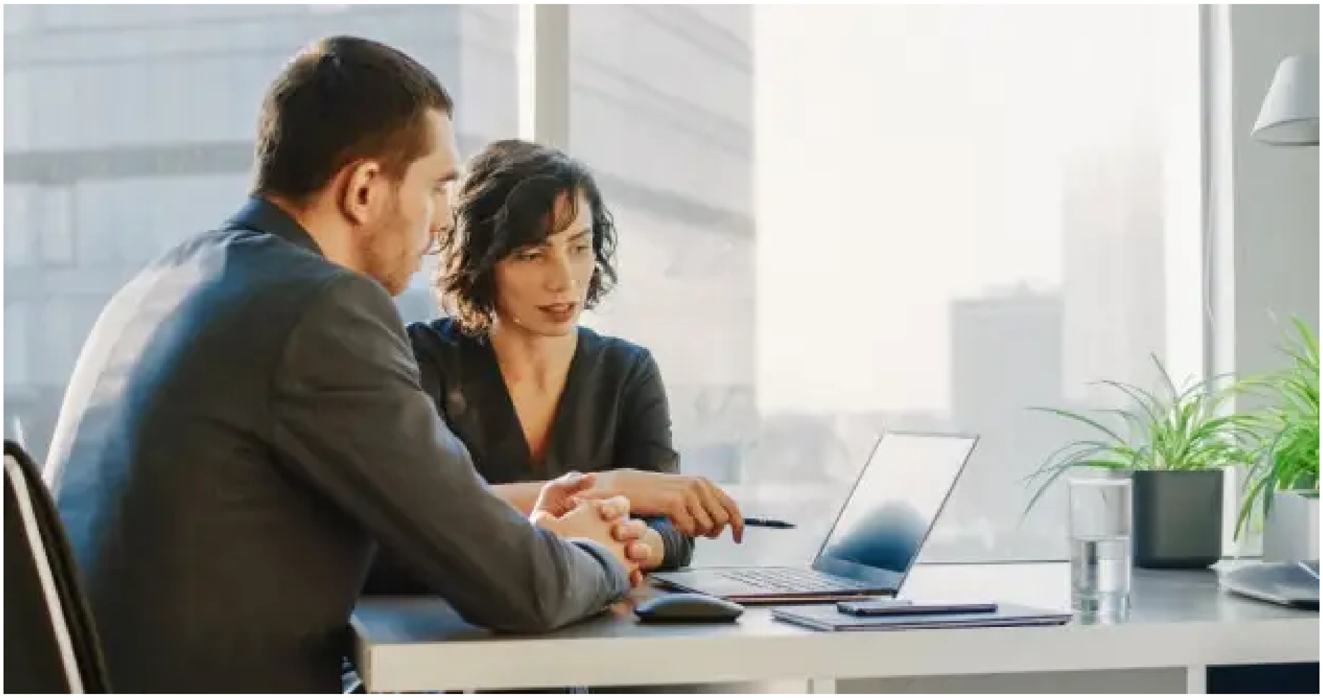
Ransomware Attacks Surge After Successful Affiliate Recruitment

securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/



Home&nbsp/ Malware

LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment



Malware September 9, 2021

By Megan Roddie 7 min read

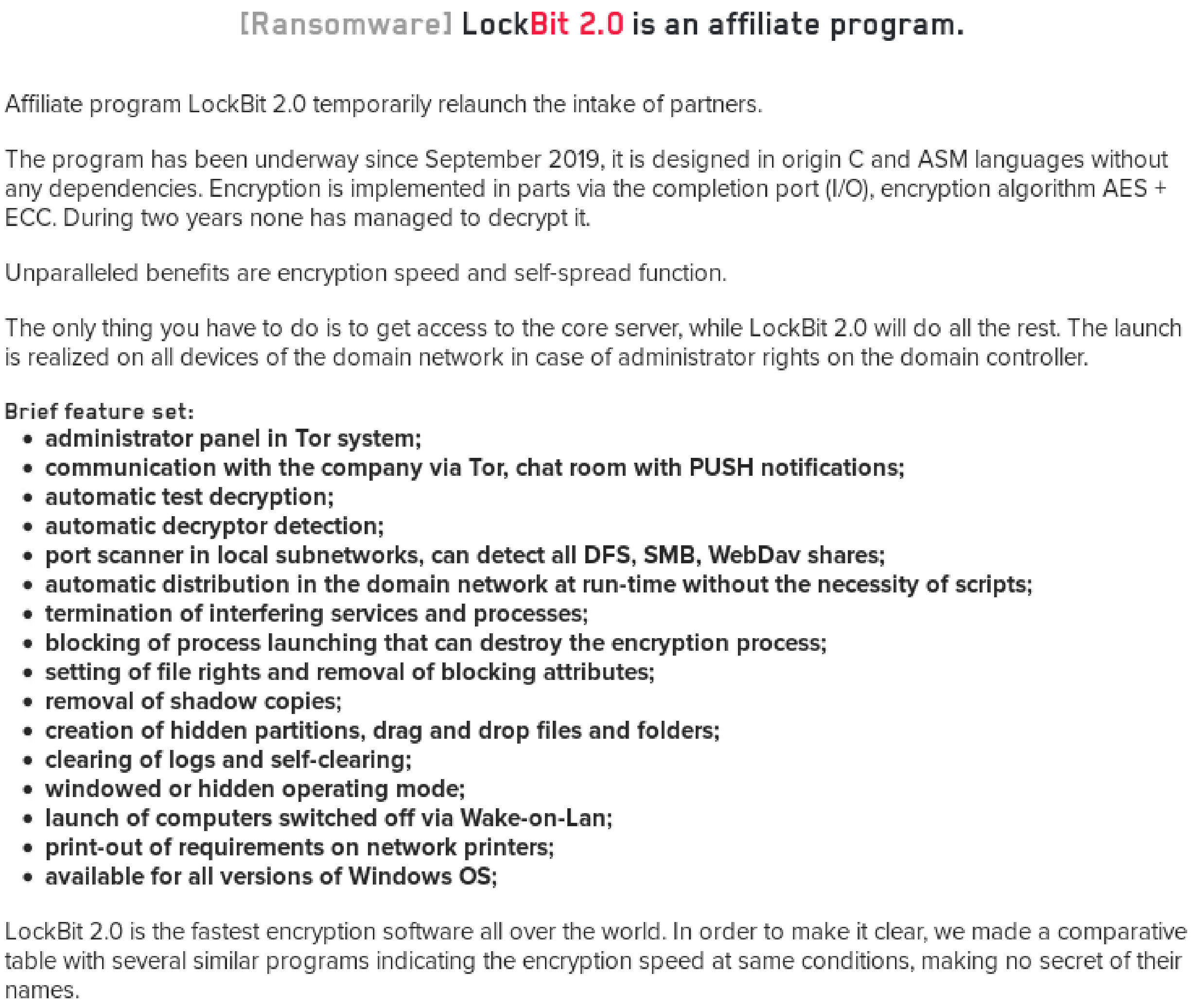
After a brief slowdown in activity from the LockBit ransomware gang following increased attention from law enforcement, LockBit is back with a new affiliate program, improved payloads and a change in infrastructure. According to IBM X-Force, a major spike in data leak activity on the gang's new website indicates that their recruitment attempts have been successful. IBM's data shows that LockBit is nearly six times more active than other groups, such as the Conti ransomware operators. This blog post delves into LockBit's 2.0 version, its recent activity and an analysis of the new payloads.

LockBit is a ransomware-as-a-service (RaaS) gang that writes and distributes its malware through affiliates. RaaS has become an increasingly popular business model for ransomware operators in the past few years, helping gangs expand their reach without growing their core team or their expenses. These groups are able to make a profit while turning over the actual deployment of their ransomware payloads to affiliates, who also shoulder part of the risk of being exposed by law enforcement.

Announcing LockBit 2.0

The LockBit gang was first found advertising their affiliate program in January 2020 on a well-known, Russian-speaking forum known as XSS. This underground forum has been used by many RaaS gangs in the past to advertise their malware and hunt for new affiliates. That includes gangs like REvil/Sodinokibi, DarkSide, Netwalker and others. But with increased attention from law enforcement, XSS banned all ransomware topics from their forum in early 2021.

With this avenue shut down, LockBit's owners pivoted to using their own infrastructure for advertising. At the end of June 2021, those behind LockBit posted a page on their leak site (bigblog[.]at) announcing recruitment for their LockBit 2.0 affiliate program.



[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

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

Unparalleled benefits are encryption speed and self-spread function.

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

Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

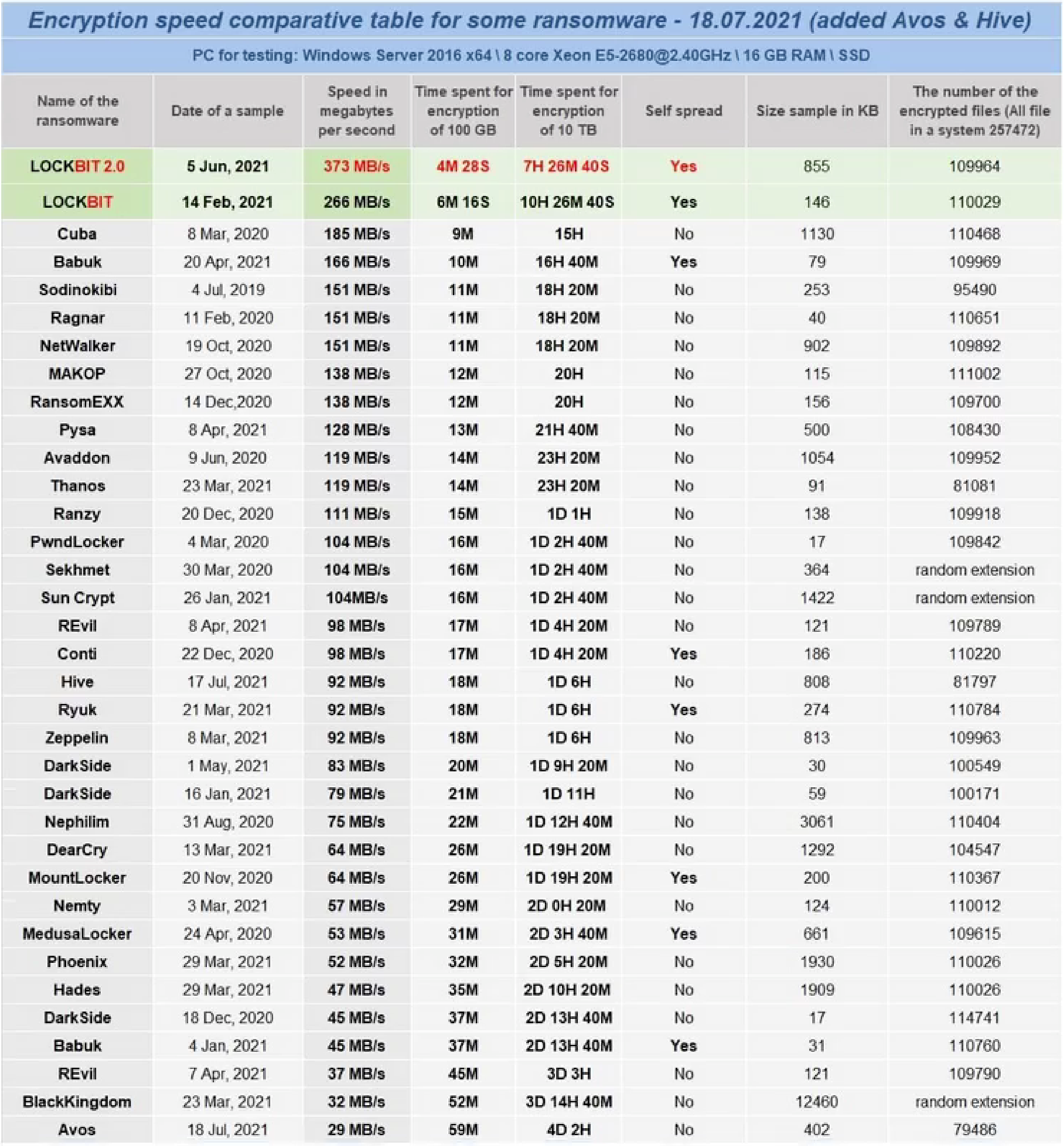
LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

Figure 1: LockBit's June 2021 advertisement with new features, seeking new affiliates (source: bigblog[.]at)

According to their post, the affiliate is responsible for gaining access to "the core server", likely referring to a domain controller, and then the rest will be carried out by the LockBit payload.

The group mentions their payload does not operate in Russian-language speaking countries and specifies that they will only work with experienced penetration testers. Additionally, the group claims their ransomware is faster than any other ransomware families and includes a table for comparing supposed encryption speeds against other prolific ransomware codes.

The affiliate also gets to decide the ransom amount and will receive the payment directly, sending the LockBit gang's cut of the profit after the ransom is paid.



Encryption speed comparative table for some ransomware - 18.07.2021 (added Avos & Hive)

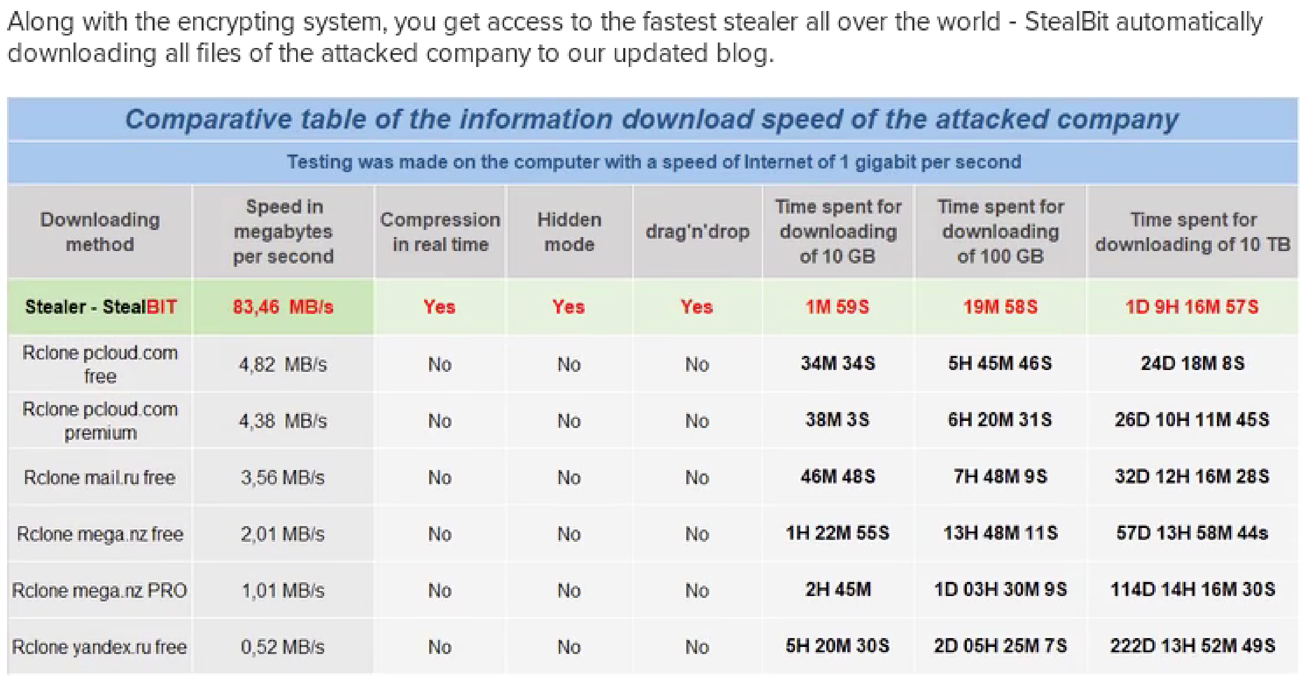
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

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
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808	81797
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
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402	79486

Figure 2: LockBit operators' encryption speed comparison vs. top competitors (source: bigblog[.]at)

To facilitate extortion if a victim refuses to pay for a decryption key, LockBit also includes access to an information stealer they call StealBit, which allegedly exfiltrates files from victim networks to the LockBit blog. This malware is also touted as a high-speed uploader, which is supposed to reassure affiliates that their operation will be swift.

X-Force researchers were able to identify files submitted to VirusTotal in August 2021 that may be samples of the StealBit malware, but analysis is still ongoing at the time of this publication.



Along with the encrypting system, you get access to the fastest stealer all over the world - StealBit automatically downloading all files of the attacked company to our updated blog.

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
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
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

Figure 3: LockBit operators boast StealBit's upload speeds (source: bigblog[.]at)

A Spike in Victims' Data Exposure

Prior to the announcement of LockBit 2.0's affiliate program, the last dark web leak from the gang appears to have been published on December 30, 2020. Posting activity resumed approximately seven months later on July 21, 2021, shortly after new recruitment attempts began, with about 76 new posts published within a six-day period.

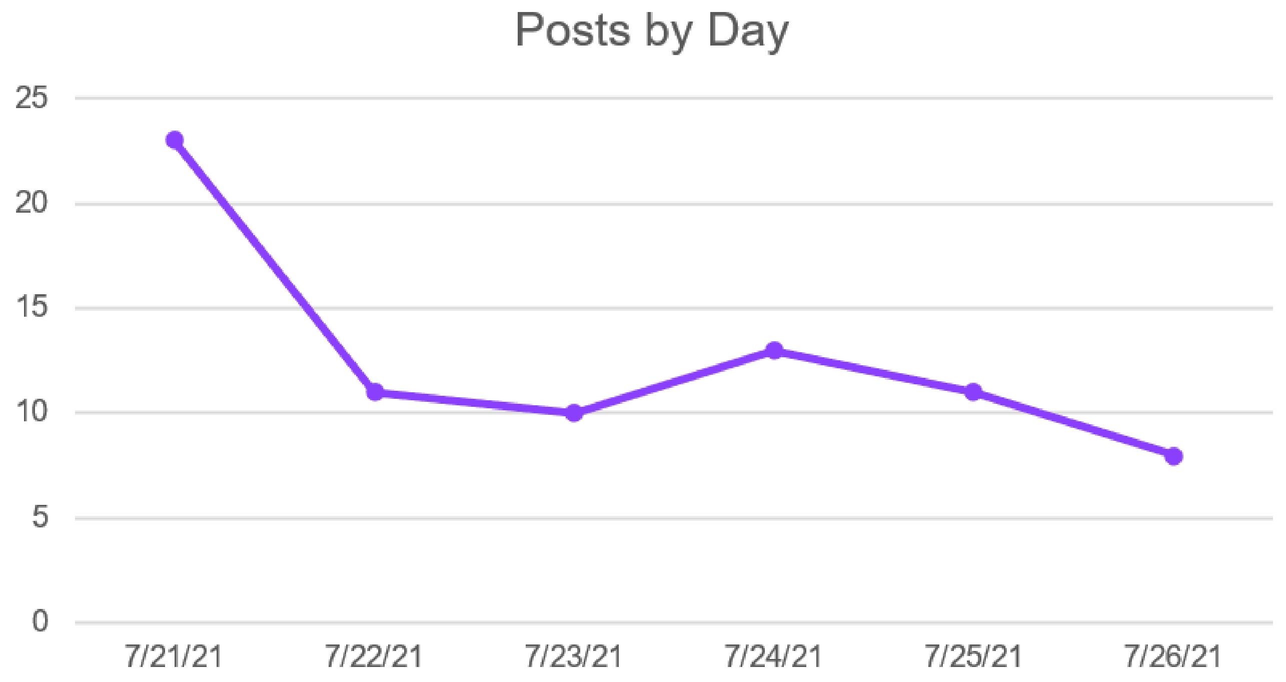


Figure 4: Stolen data posts created per day on bigblog[.]at

Looking at other ransomware families' leak sites in the three-week period since LockBit's return (7/21/2021-8/11/2021), LockBit appears to be currently operating one of the most active ransomware leak sites.

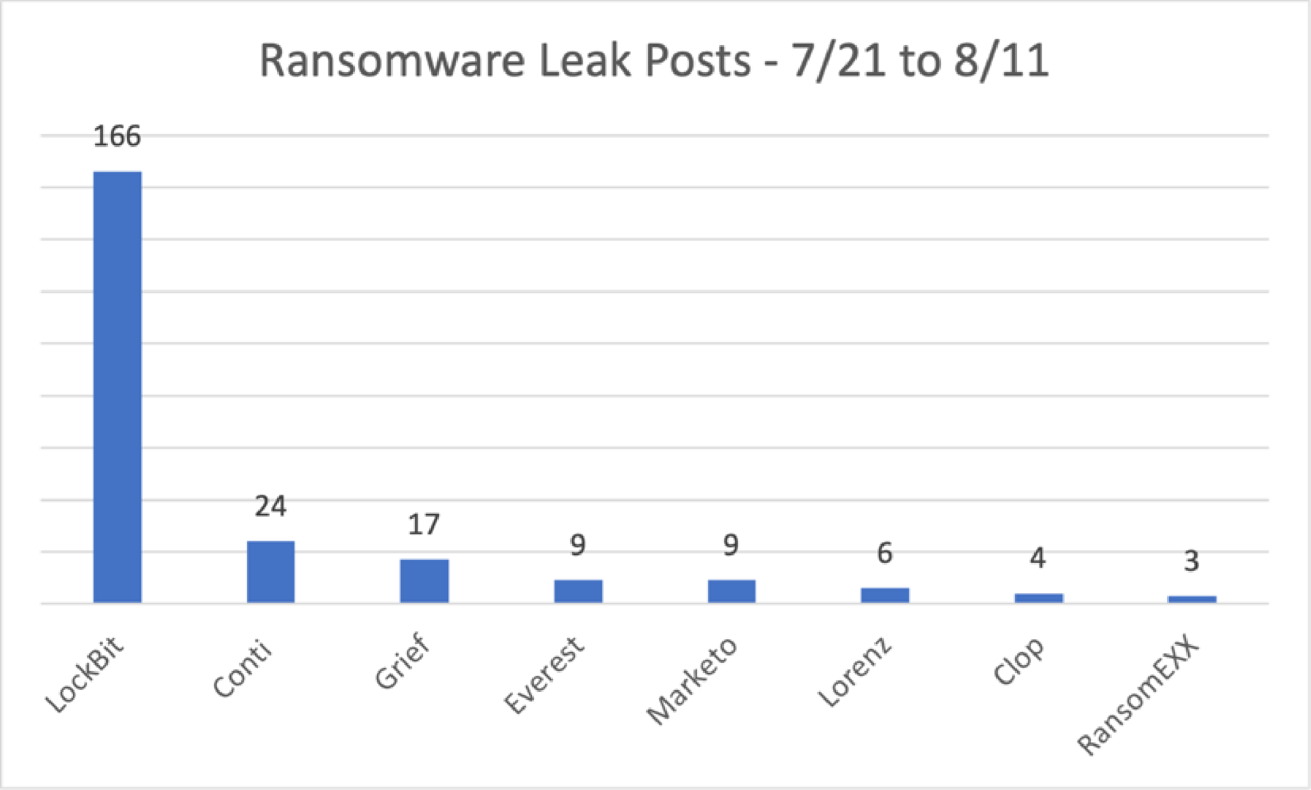


Figure 5: Leak site activity by the number of posts within the monitored period

Victims by Industry, Geography

With regards to victims, IBM X-Force identified the below industries and geographies being impacted by LockBit and its affiliates:

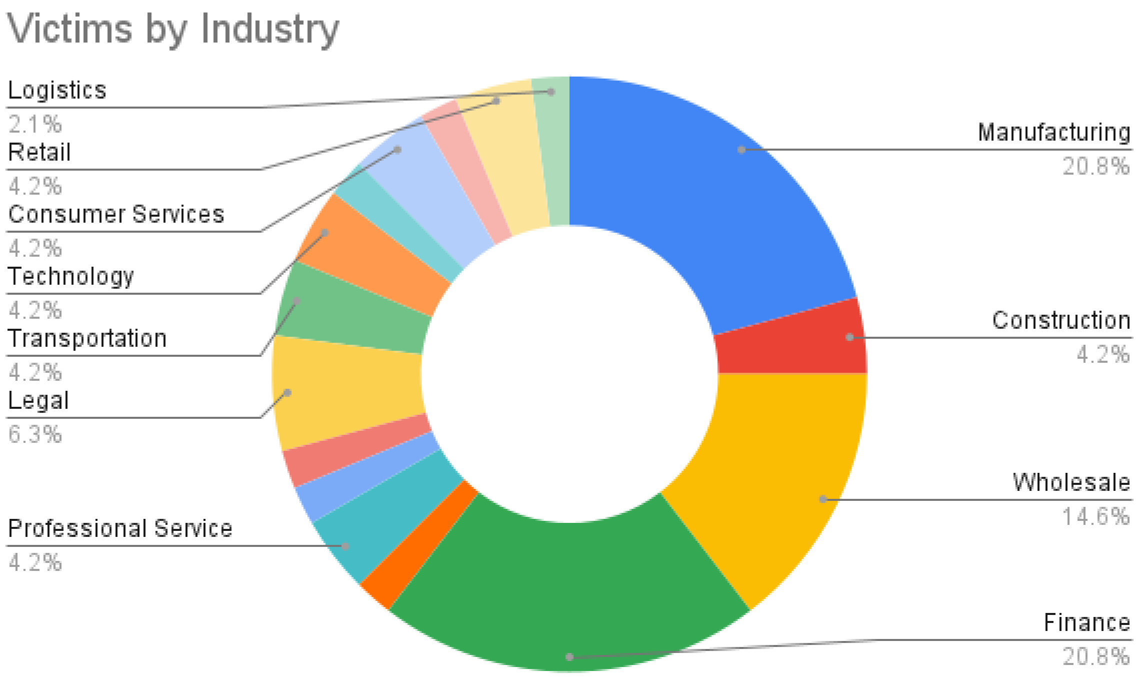


Figure 6: Top LockBit victims by industry (source: IBM X-Force)

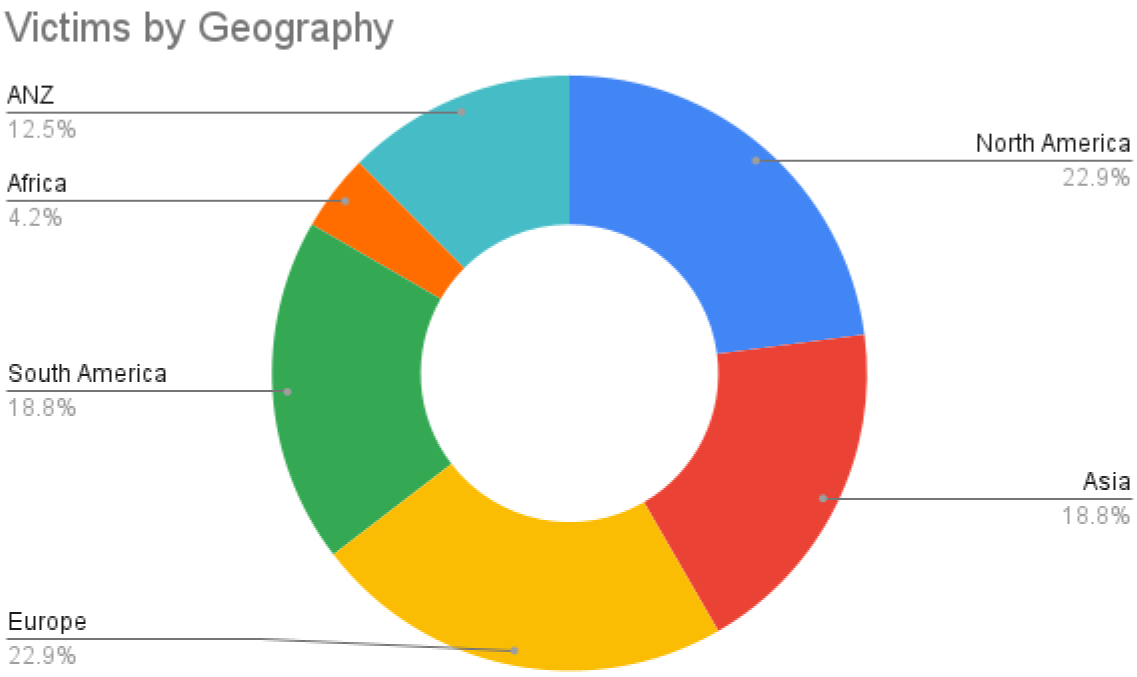


Figure 7: Top LockBit victims by region (source: IBM X-Force)

While a few regions and industries have multiple victims involved, IBM was unable to identify any clear targeting patterns. Each LockBit affiliate likely has its own choices of targeting, which may be targeted or opportunistic.

Given the timing of the new affiliate program being advertised and the spike in activity, IBM X-Force suspects that LockBit was able to recruit affiliates who had already begun compromising networks.

New Infrastructure

LockBit's use of a data leak site first appeared in September 2020. Their leak sites and support sites (where victims can purchase a decryptor) are offered at both surface and dark web addresses. Along with the observed uptick in activity, IBM researchers discovered the use of newly registered infrastructure for these sites.

LockBit's primary blog that publishes victim data and advertises its affiliate program is currently being hosted on the clear web at bigblog[.]at. Whois information for this domain indicates that LockBit registered the domain on July 6, 2021. Pivoting off the unique registrant email reveals that their new clear web decryptor site, decoding[.]at, was also registered on the same date.

IBM X-Force was able to uncover the domain locksupp[.]at, which was leveraging the same name servers as decoding[.]at. Whois and nameserver history indicates that this domain was in use around June 6, 2021, but it appears it was suspended by June 29, 2021. It is not currently reachable and its purpose is unknown at this time.

New Samples

X-Force identified over a dozen new submissions of LockBit samples to VirusTotal occurring since the launch of the LockBit 2.0 affiliate program. Analysis was performed on several of these samples to determine any changes in these new variants.

Much of LockBit's functionality remains the same in version 2.0, with a similar encryption routine. A hybrid AES/RSA encryption approach is still used. The two minor updates are the renaming of the registry key in which the RSA public session key is stored and the creation of a file used as a mutex while files are being encrypted. Additionally, the registry run key used for persistence is now a GUID-type string instead of an alpha-numeric string.

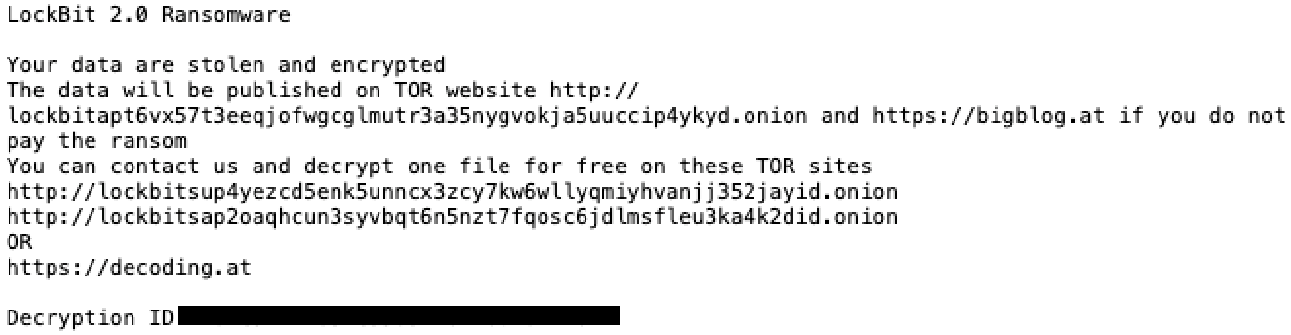
On top of these minor changes, two major additions were discovered: the addition of a new deployment technique and the physical printing of ransom notes.

Active Directory Deployment

One of the most significant changes identified during the analysis was the implementation of a novel technique for deployment. The payload has the capability to automatically deploy itself to Microsoft Active Directory clients via Group Policy Objects (GPO). When executed on an Active Directory Domain Controller, LockBit 2.0 creates several GPOs to carry out the infection process. The Windows Defender configuration is altered to avoid detection. It refreshes network shares, stops certain services and kills processes. The LockBit executable is then copied into the client desktop directories and executed. PowerShell is used to apply the new GPOs to all domain-joined hosts in a specified organization unit (OU).

Ransom Note

The following is an example of the ransom note left behind after files are encrypted:



```
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 [redacted]
```

Figure 8: LockBit's post-encryption ransom note (source: IBM X-Force)

Another interesting addition to the extortion techniques is a new LockBit functionality to repeatedly print the ransom note to any printers connected to the victim host.

A Growing Threat to Watch For

LockBit does not appear to be slowing down, with regular leaks being published daily since the launch of their 2.0 affiliate program. It is likely that the ransomware payload will also continue to evolve and expand its capabilities. This ransomware group and the many others currently operating in the threat landscape present a major threat to organizations in all industries and geographies, except those in the Commonwealth of Independent States (CIS) countries where most malware operators avoid attacking local organizations.

Organizations should prioritize protecting their networks and data from this threat or risk joining the growing list of victims of RaaS affiliates. The following are a few actions companies can take that can help mitigate risks and minimize damage:

- Establish and drill an incident response team. Whether in-house or as a retained service, the formation of an incident response team and drilling the most relevant attack scenarios can make a big difference in attack outcomes and costs.

- Establish and maintain offline backups. Ensure you have files safely stored from attacker accessibility with read-only access. Also, consider the use of offsite/cold storage solutions. The availability of backup files is a significant differentiator for organizations that can help them recover from a ransomware attack.
- Implement a strategy to prevent unauthorized data theft, especially as it applies to uploading large amounts of data to legitimate cloud storage platforms that attackers can abuse. Consider blocking outbound traffic to unapproved cloud hosting services.
- Employ user and entity behavior analytics to identify potential security incidents. When triggered, assume a breach has taken place. Audit, monitor and quickly act on suspected abuse related to privileged accounts and groups.
- Deploy multifactor authentication on all remote access points into an enterprise network — with particular care given to secure or disable remote desktop protocol (RDP) access. Multiple ransomware attacks have been known to exploit weak RDP access to gain initial entry into a targeted network.
- Use penetration testing to identify weak points in enterprise networks and vulnerabilities that should be prioritized for patching. In particular, we recommend implementing mitigations for CVE-2019-19781, which multiple threat actors have used to gain initial entry into enterprises in 2020 and 2021 — including for ransomware attacks.
- Consider prioritizing the immediate remediation, as applicable, of the following frequently exploited software vulnerabilities:

    - CVE-2019-2725
    - CVE-2020-2021
    - CVE-2020-5902
    - CVE-2018-8453

VPN-related CVEs

- CVE-2019-11510
- CVE-2019-11539
- CVE-2018-13379
- CVE-2019-18935
- CVE-2021-22893

RDP

-
    - Restrict port access on TCP port 3389
    - Apply multifactor authentication to remote access logins
    - Remediate RDP vulnerabilities such as Windows RDP CVE-2019-0708 (BlueKeep)
    - CVE-2020-3427
    - CVE-2020-0610
    - CVE-2020-0609
- Segment networks according to the data they host.
- Encrypt the data most likely to be stolen in an attack.
- Consider adopting a zero trust approach and framework to better control what users can access and potentially halt an attack in its tracks.

If you are experiencing cybersecurity issues or an incident, contact X-Force for assistance: U.S. Hotline: 1-888-241-9812 | Global Hotline: +(001) 312-212-8034. Learn more about X-Force's threat intelligence and incident response services.

Indicators of Compromise

SHA256 Hashes
00260c390ffab5734208a7199df0e4229a76261c3f5b7264c4515acb8eb9c2f8
0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049
2ba9fab56458fe832afecf56aae37ff89a8b9a494f3c2570d067d271d3b97045
4de287e0b05e138ab942d71d1d4d2ad5fb7d46a336a446f619091bdace4f2d0a
743ecc953dcd83a48140c82d8a7dcac1af28e0839aed16628ddfc9454bec8dfa
8155c6bea7c1112f022e9c70279df6759679295bd4d733f35b6eea6a97d3598f
856d5253f68bebcba161bc8f8393f34c806717faa6297c669c75fb13b17f8d03
9bca4fe6069de655467e59929325421b93617bccfdf23e9fba02615d36d60881
a98ffa66c07f634d19dc014bb2d63fa808d7af5dc9fb9b33aa19a8b944608816
acad2d9b291b5a9662aa1469f96995dc547a45e391af9c7fa24f5921b0128b2c
b3faf5d8cbc3c75d4c3897851fdaf8d7a4bd774966b4c25e0e4617546109aed5
dd8fe3966ab4d2d6215c63b3ac7abf4673d9c19f2d9f35a6bf247922c642ec2d
ea028ec3efaab9a3ce49379fef714bef0b120661dcbb55fcfab5c4f720598477
f32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202

f3e891a2a39dd948cd85e1c8335a83e640d0987dbd48c16001a02f6b7c1733ae

Megan Roddie
Cyber Threat Researcher - IBM X-Force IRIS

Megan Roddie is a Cyber Threat Researcher with IBM's X-Force IRIS. She has a M.S. in Digital Forensics along with several industry Digital Forensics and Inci...