Cyber empire of crypto ransomware

Part 2

ROOT LEVEL RESOURCES

Trend analysis

In 2021, the number of new public affiliate programs [1] decreased sharply. Although this had no effect on the emergence of new DLSs [2], implying that a lot of ransomware programs keep running without affiliate programs. Data of new victim companies on DLS ransomware operators' websites grows.

Conti, Lockbit, and Avvadon were the most active groups in 2021. They released the biggest number of companies on DLS, while the percentage from the total number of victims dropped because of the increase in the number of small ransomware operator groups (in 2020, Maze, Egregor, and Conti topped this list).

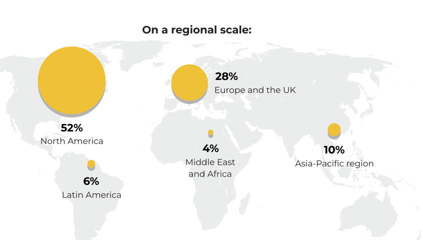
In 2022, the top 3 active groups are:

LockBit — Conti — Pysa

As for the **geographic distribution of victims**, it is as follows:

Country	Victims	Share
USA	968	49,4%
Canada	110	5,6%
France	103	5,2%
United Kingdom	92	4,7%
Italy	76	3,9%
Germany	72	3,6%
Spain	42	2,1%
Australia	41	2,1%
Brasil	39	2,0%
India	24	1,2%
Netherlands	22	1,1%
Others	295	6%

On a regional scale:



The main **attacked industries** in 2022 were **manufacturing**, **real estate**, and **transport**. They were also in the top 3 in 2021, suggesting that attackers tend to target the same company types they find most profitable.

The companies that they find the most attractive

210	Manufacturing
207	Real estate
178	Transport
169	Professional services
140	Financial services
128	Trade and Shopping
125	Healthcare
97	IT
82	Government and Armed Forces
79	Food and Beverage
75	Science and Engineering
70	Education
50	Energy
45	Administrative services
43	Final Goods
40	Hardware
31	Communications and Media Relations
30	Media and Entertainment
29	Security
27	Travel and Tourism
27	Software
24	Clothing and Accessories
23	Engineering
23	Natural resources
21	Sales and Marketing
18	Data and Analytics
16	Agriculture and Farming
56	Other

1 A public affiliate program (RaaS) is an offer to join a group that runs crypto ransomware in order to distribute malware in exchange for a ransom payment.

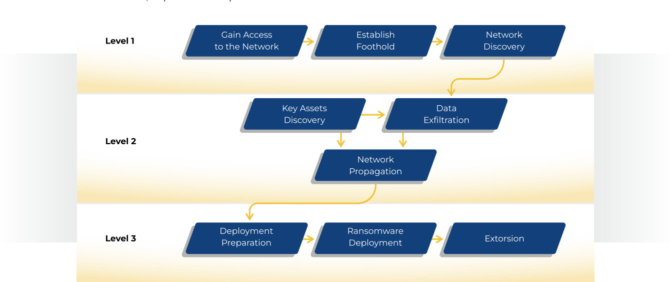
2 DLS are used by ransomware operators as a double extortion technique. That is, they are used to create more pressure on victims to force them pay. After paying the ransom, the encryption operators promise to delete the compromised data from the DLS or not to share it in the public domain.

An overview of tactics, techniques and procedures involved in attacks

ROOT LEVEL RESOURCES

The active development of the RaaS market, as well as shifting the focus of many financially motivated groups to organizing ransomware attacks, has had a major impact on the number of investigated incidents of this type.

Thus, experts developed a **unified structure of ransomware attacks:**



A set of typical ransomware attack techniques and tools remains stable, since this toolkit proved to achieve its goal, as well as to create tutorials even for less-experienced users.

The evolution of the initial access broker market allowed attackers to easily gain access to their victims' networks and greatly influenced the effectiveness and number of ransomware attacks.

The most common **techniques for gaining initial access** are compromising remote access services (21%), phishing (26%), and exploiting publicly available applications (47%).

Attacking publicly available terminal servers with remote desktop protocol (RDP) connections is still a popular method of compromising remote access services. Most often, attackers gain access by brute forcing passwords, for example, using **NLBrute**.

In some cases, attackers used the **BlueKeep** vulnerability exploit.

The lack of multi-factor authentication allowed attackers to actively compromise accounts for VPN connection. Moreover, several vulnerabilities, including some rather old ones, for example in **Pulse Secure** and **Fortinet** products, made it possible to actively use VPN to access corporate networks.

Recent vulnerabilities allowing initial access to networks were exploited in ransomware attacks shortly after being released.

For example, Conti and AvosLocker partners actively used **ProxyShell**, which allowed them to attack vulnerable Microsoft Exchange servers along with state-sponsored groups.

Another example is when partners of **HelloKitty**, the ransomware that became well-known after the attack on **CD Projekt RED**, exploited vulnerable **SonicWall** devices.

In some cases, attackers managed to gain access to so-called **zero-day vulnerabilities**. A telling example is the **REvil** partners' attack on **Kaseya**.

Popular botnets, such as **IcedID**, **Qakbot**, **Hancitor**, **Trickbot**, and others, are still actively used by ransomware operators to gain initial access.

Often the email content is quite trivial, and the malicious document contains instructions for running a macro that will download the bot to the compromised computer.

In some cases, attackers also exploited vulnerabilities to download and launch malicious code. For example, **BazarLoader** operators actively used a vulnerability in **MSHTML** to infect emailed documents that were distributed by the **Ryuk** ransomware.

Along with traditional phishing, BazarLoader operators also used **vishing**. They sent emails with information about a paid subscription and a phone number to cancel it. The caller was convinced to go to the site and download an unsubscription form, which, obviously, was a malicious document.

Popular attack techniques:

100%	Command and scripting interpreter
100%	Remote Services
95%	Remote System Discovery
93%	Impair Defenses
91%	OS Credential Dumping
89%	Encrypted data for impact
89%	Inhibit system recovery
72%	Exfiltration over Web service
69%	Segned binary proxy execution
66%	System services

Traditionally, attackers widely use various **command and script interpreters**. Popular interpreters are **Windows command line; PowerShell; Visual Basic; JavaScript**.

The first two are used at different stages of the attack cycle. Visual Basic is actively exploited by malicious macros, while JavaScript is less common, thus increasing the chance of a successful compromise.

IcedID operators used JavaScript files packed in ZIP archives to deliver payloads. At the same time, links to the archives were posted on Google sites, which reduced the victims' vigilance. Moreover, the victim was prompted to sign in to their Google account, following which the archive was downloaded automatically.

In most cases, the first stage of an attack is just access to the corporate network. Attackers use all means to start advancing through the network and to elevate privileges. This is proven by the fact that in 100% of cases **remote access services** are used.

The most common method is still Remote Desktop Protocol (RDP). Some groups even have scripts to enable such access.

Speaking of network propagation, we should mention ***methods for gathering information about remote systems***. Attackers actively use a variety of network scanners, as well as tools for gathering information about **Active Directory**.

The **Server Message Block** (SMB) protocol is no less popular, both for network propagation and ransomware deployment.

Successful ransomware deployment is almost impossible without ***neutralizing defenses***, involving prepackaged scripts that run on target hosts through a group policy modification or **PsExec**. Moreover, many ransomware instances contain lists of processes and services related to protections that will be stopped during malware deployment. For example, one of the strings used by **BlackMatter** to identify processes and services for subsequent shutdown was the sophos string pointing to a popular anti-virus protection tool.

Credential dumping is still popular. Besides well-known tools, such as **Mimikatz**, which are easily detected by security software, attackers started to use less eye-catching methods, including those based on the exploitation of built-in Windows tools.

Attackers encrypted data for ransom in only 89% of incidents. This is due to the fact that attackers limited their efforts to offloading data, or users detected suspicious activity before the ransomware was deployed.

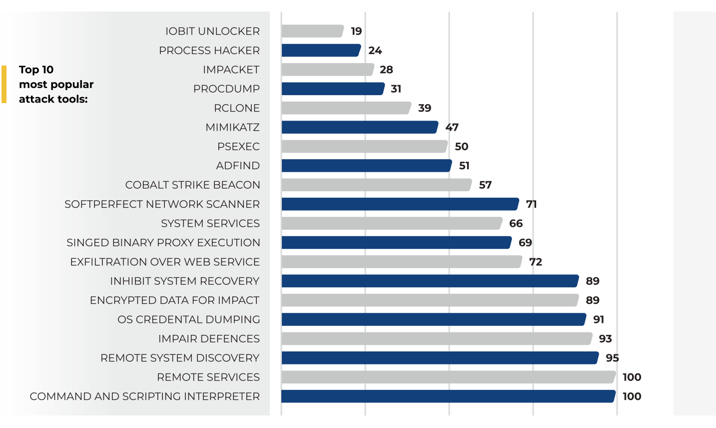
The same percentage of incidents involved attackers breaching system recovery tools, namely Windows shadow copies. Such functionality was incorporated both directly into ransomware and in scripts.

Many groups are still actively offloading data from compromised networks. They often ***use web services*** for this purpose. Various cloud storage services are especially popular, such as **MEGA**, **DropMeFiles**, **SendSpace**.

Referring to popular post-exploitation techniques, we should mention the code ***running through a signed application***. The clear examples of this technique are the exploitation of **rundll32.exe** and **regsvr32.exe**.

The latest technique listed among the top ten is the ***exploitation of system services***. The reason is that attackers use **PsExec** and its implementations, which are part of post-exploitation frameworks such as **Cobalt Strike**.

Top 10 most popular attack tools:



The identification of remote systems aimed at further propagating or deploying ransomware is one of the main goals of cybercriminals. A popular commercial network scanner, **SoftPerfect Network Scanner**, has been used for this purpose.

Cobalt Strike is another popular tool. In some cases, attackers used Beacon instead of bots as part of phishing emails. For example, phishing emails containing malicious documents were sent to deliver the **Squirrelwaffle** downloader, which in turn downloaded the **Cobalt Strike Beacon**.

ADFind, a tool for gathering information about Active Directory, was used by attackers almost on a par with Cobalt Strike. Attackers downloaded it at an early stage to examine compromised infrastructure.

Furthermore, one of the attackers' goals is to execute commands and malicious code on remote hosts. For this reason, half of the incidents had traces of **PsExec** exploits, both for launching commands and for directly distributing the ransomware.

The **Mimikatz** credential and memory extraction tool is still popular. Moreover, attackers use its versions, such as the PowerShell version of Invoke-Mimikatz and the Python version of Pypykatz.

Some ransomware operators decided to simplify the life of their partners by enriching their toolkit with automatic data collection and uploading tools. StealBit by LockBit is a good example. Nevertheless, many still offload data with their own tools. The most popular tool used for this purpose is **Rclone**.

Since popular credential extraction tools are easy to detect, some attackers use legitimate tools to dump lsass.exe (using **ProcDump**).

In addition to PsExec, the SMBExec script from the **Impacket** package was used extensively to execute commands on remote hosts.

Process Hacker, a popular tool for monitoring system resources, was also actively used to gather information about existing protections and their subsequent neutralization.

Iobit Unlocker, a tool used by cybercriminals for similar tasks, was employed to terminate processes that interact with databases and prevent their encryption.

However, we should note that the presented techniques and tools are not exhaustive.

Behind the scenes of the cyber ransomware world

ROOT LEVEL RESOURCES

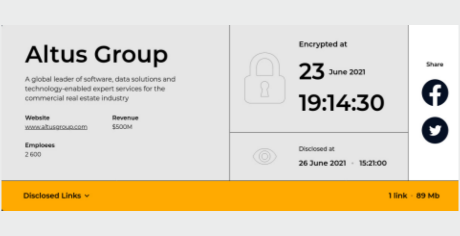
1 HIVE

In summer 2021, **Hive** group activity was detected using DLS.

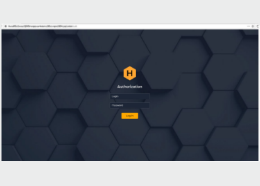
They use a combination of AES and RSA to encrypt the data, whereupon the software uploads it to a remote server. Encrypted files can be identified by the .hive extension.

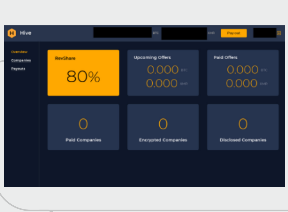
The distinctive feature of DLS is that it worked with APIs. Besides Hive, there are only 2 groups that also used API - **Grief** and **DoppelPaymer**.

Hive posted the stolen files on file-sharing sites (sendspace, anonfiles, send.exploit, and others).



As early as fall 2021, an affiliate program advertisement appeared on the RAMP forum. As a result of communication with the intruder, access to a closed affiliate program was obtained (the address of the administrative panel and authentication data for logging in were provided), which made it possible to determine that it was Hive.





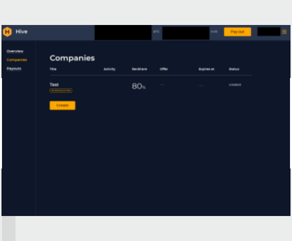
The home page opens after entering your login and password, which shows:

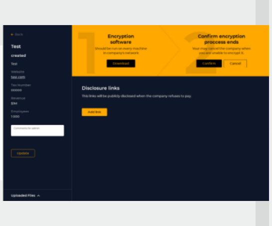
- What percentage of the ransom the perpetrator receives
- How much the attacker is supposed to get in the future, how much he has already received, the number of victims who have already paid
- Encrypted and disclosed companies
- As well as the overall balance and login

The Companies section contains the most interesting data. Here you can find the name of the victim's company, its website, a brief description, as well as the revenue and number of employees.

The Payouts tab controls the withdrawal of funds from the affiliate program to the intruder's personal wallet.

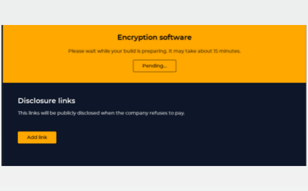
Once this information is filled in, the following window opens:



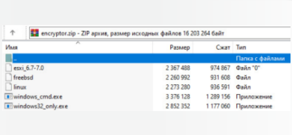


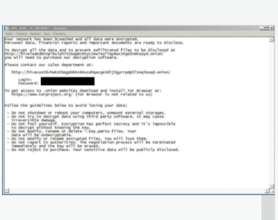
Once you open the company card, you can download the ransomware for the victim company and check whether its data was encrypted or not.

The ransomware generation takes up to 15 minutes. If the company refuses to pay the ransom, it is possible to add a link that will be shared on the Hive blog.



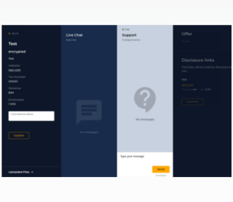
After creating the ransomware, an .rar archive will be generated with the following files:

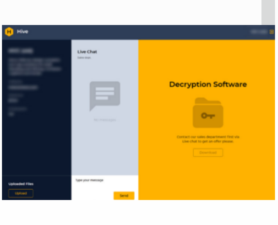




Once infected, a ransom note will be automatically created with a link to the site as well as a login and password to access:

Once the attacker confirms that the company has been encrypted, a chat with the victim will be opened. However, the victim and the attacker don't communicate directly – all communication goes through the administrator.

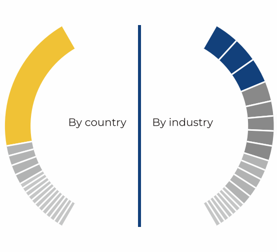




Once victims pay the ransom, they will receive a decriptor with instructions on how to use it.

Distribution of Hive victim companies

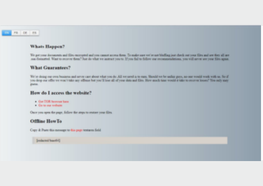
By country	
USA	28
UK	2
Australia	2
Netherlands	2
China	2
Canada	1
Peru	1
Switzerland	1
Portugal	1
Thailand	1
India	1
Norway	1
Spain	1
Germany	1
Taiwan	1
France	1
Italy	1

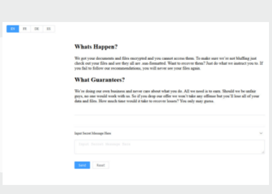


By industry	
5	Real estate
5	IT
5	Manufacturing
4	Other
3	Trade and Shopping
3	Transport
3	Media and Entertainment
3	Financial services
2	Professional services
2	Administrative services
2	Food and Beverage
2	Hardware
2	Healthcare
1	Crediting and investing
1	Clothing and Accessories
1	Education
1	Privacy and Security
1	Final goods
1	Games
1	Software

2 Suncrypt

Suncrypt was detected in the fall of 2019. The ransom note was then translated into English, French, German, and Spanish and looked as follows:

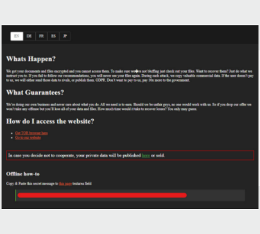




It contained a message that the company files were encrypted, as well as a unique victim code and a link to the attackers' resource, where you had to enter the received code.

The first samples of this ransomware specifying their current DLS site were found in ransom notes in late summer 2020.

The note looks almost exactly the same, except that it appears in Japanese and new links. The first leads to the DLS groups and the second to the personal chat.



When the DLS first appeared in the public domain, it already contained compromised data on five victims. Three of them were in the U.S. (industries: government and armed forces, privacy and security, real estate: construction), the other two in Canada (software) and Norway (manufacturing). At the same time, each compromised company on the DLS has its own unique ID in the database of attackers.

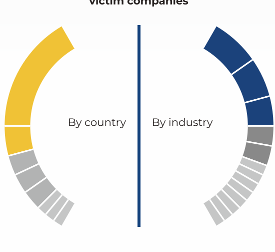
The peculiarity of this DLS is that some records return a Forbidden message in response to a query. For example, some of the current **Forbidden** Ids matched companies previously attacked, but now their data has been removed from the DLS, presumably as a result of the companies paying a ransom.

Suncrypt openly states that they are ready to sell full data about the company to any interested person.

The resource itself has two main subsections - New clients and Full dumps. According to the attackers, they initially publish 10% of the company's data and only then put it up for sale. If the data is not redeemed within a week, the rascals post the full dump of the company.

Distribution of SunCrypt victim companies

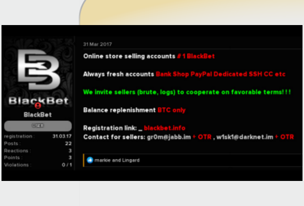
By country	
USA	12
Norway	3
Canada	2
Belgium	2
Germany	2
Italy	1
UK	1
Australia	1

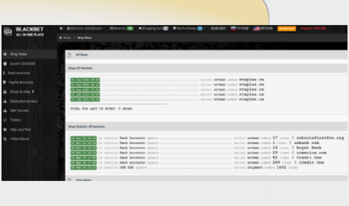


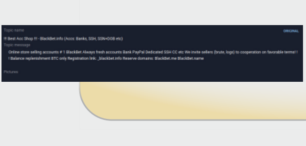
By industry	
5	Manufacturing
4	Energy
3	Trade and Shopping
2	Real estate
2	Professional services
1	Government and Armed Forces
1	Education
1	IT
1	Transport
1	Security
1	Healthcare
1	Financial services
1	Science and Engineering

3 RTM: how new affiliate programs, or silent lockers, originate

Over the past two years, ransomware has become a major threat to businesses. More and more cybercriminals are changing focus to ransomware, due to its clear monetization and considerable financial potential. Some are trying to repeat the success of Lockbit and organize their own Ransomware-as-a-Service. This trend is evident especially in the case of the person called **RTM Team (aka BlackBet)**. The transformation process of RTM is quite illustrative:

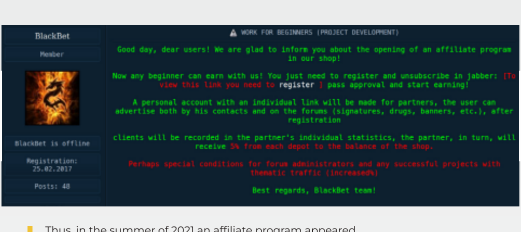






BlackBet first appeared on the forum in the winter of 2017, where he advertised his own marketplace for the sale of various data

He also bought U.S. logs, mined, sold and bought malware, sold network accesses, and conducted other malicious activities. His main trait was that he was always trying to follow the most profitable trends. When the attacker realized that ransomware was just such a trend, he decided to try it out.



Thus, in the summer of 2021 an affiliate program appeared.

An analysis of the RTMTeam (aka BlackBet) sample found that malware performs selective file encryption using Chacha20 and Curve25519 asymmetric encryption algorithms, as well as AES via x86 extensions. While infecting, malware lists the lines of embedded disks and checks for a valid root drive and mounted disks. It skips OS paths and some application folders and proceeds to encrypt all user files, rendering them useless for recovery without a backup or decryption key. The malware also checks for processes and services with lines embedded in the last section of the binary file for the appropriate termination of the process and service.

Moreover, the dumpster, system event, application and security logs of the infected system are cleaned and then the shadow copies are checked, containing code to access and request the shadow copies using WMI as the interface.

Once the files are encrypted - the wallpaper is changed to a jpeg file with a ransom demand, and a text file with the ransom demand is placed in each directory where the files were encrypted.

Following infection, the malware removes itself from the startup path.

The samples presented in the archive and the sample obtained through the PS dropper are equal in functionality and differ in appearance by static attributes, including encryption keys and ID numbers. This indicates that these may be generated samples with different IDs for each infected system.

4 Groove and first Fake DLS

The first mention of them appeared in the summer of 2021, when the main administrator of the RAMP forum required help in creating a website for Groove. The Groove site remained empty for a long time, and then several leaks appeared there. The site looked like a typical DLS.

Groove attracted a lot of attention from both RAMP users and the media after the publication of 10,000 access points to Fortinet.

Yet in the fall of 2021, Groove's owner (boriselcin) posted on the xss.is forum that the whole DLS was fake and was created solely to manipulate the media, as ransomware is now gaining attention.

Thus, due to the increased popularity of ransomware and affiliate programs, we can assume that Fake DLSs and Fake-Ransomware-as-a-Service are going to emerge from now on. To join such "affiliate programs", the accomplice will have to pay, whereupon the administrator disappears.

ROOT LEVEL RESOURCES

Recommendations for proactive threat hunting

1. Track the events involving the creation of suspicious folders or files or the running of processes such as rundll32.exe or regsvr32.exe with winword.exe/excel.exe.
2. Detect suspicious cscript.exe / wscript.exe launches, especially those related to network activity.
3. Detect powershell.exe processes with suspicious or obfuscated command lines.
4. Analyze executable files and scripts placed in the autorun folder, added to the Run keys or started with the task scheduler.
5. Track the execution of sdbinst.exe for suspicious command line arguments.
6. Check creation of new keys in HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options.
7. Make sure that your protection systems know how to detect command lines specific to credential dumping tools such as Mimikatz.
8. Look for artifacts specific to network reconnaissance tools, such as AdFind command line arguments.
9. Detect artifacts associated with executing files from unusual locations, such as C:\ProgramData, %TEMP% or %AppData%.
10. Detect registry and Windows firewall modifications related to RDP connections.
11. Track and analyze RDP connections to detect network promotion attempts.
12. Detect wmic.exe launches using suspicious command lines.
13. Track abnormal behavior of bitsadmin.exe, especially related to downloading potentially malicious files.
14. Make sure that your systems are able to detect Cobalt Strike Beacon payloads and similar tools specific to post-exploitation frameworks (at least those that run with typical command line arguments and from typical locations).
15. Monitor network connections from common system processes. Use Cobalt Strike's known server lists, which you can obtain from your Cyber Threat Intelligence vendor.
16. Keep track of new service creation events associated with PsExec, SMBExec, and other dual-purpose or pentesting tools.
17. Monitor executable files disguised as common system files (such as svchost.exe) but with anomalous parent files or locations.
18. Track signs of unauthorized use of remote access tools on your network.
19. Track cloud storage client installation events and cloud storage access events and verify if they are legitimate.
20. Track common FTP programs on end hosts to detect file installation events with malicious configurations.