# The Darker Things

blog.group-ib.com/blackmatter2

03.11.2021

BlackMatter and their victims


Andrey Zhdanov

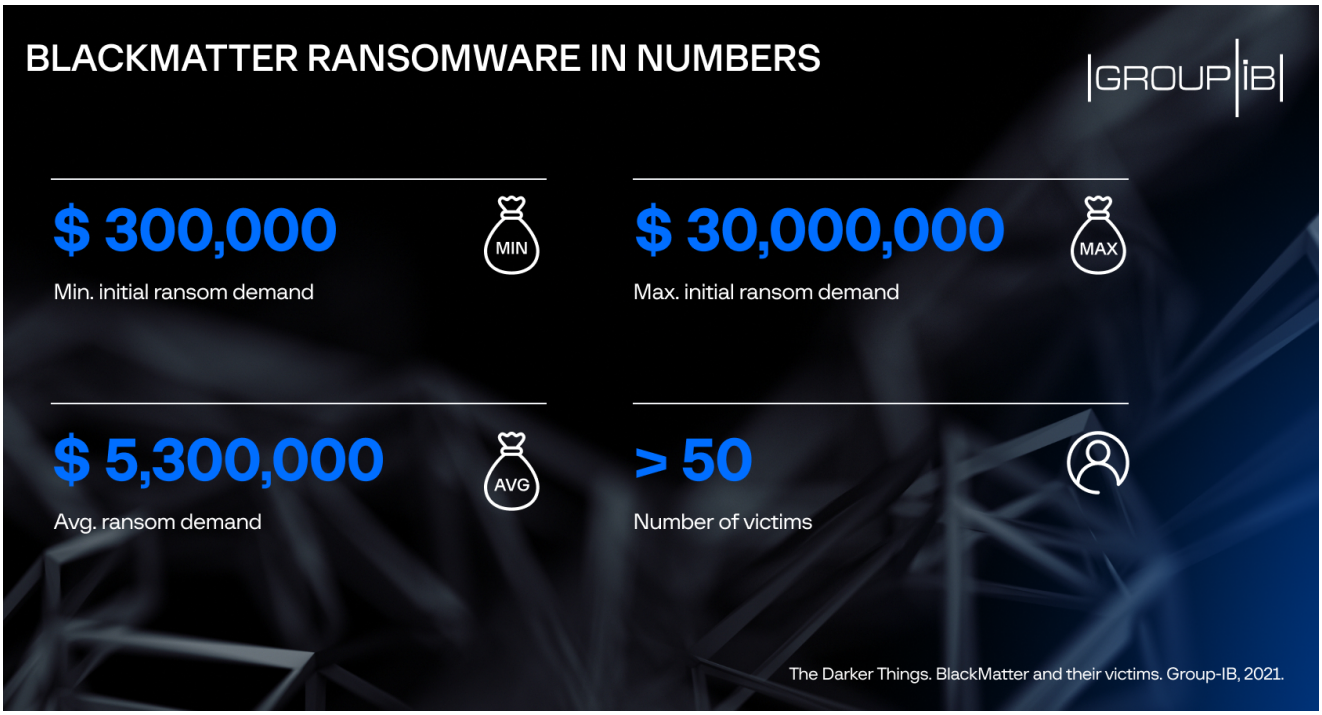
Threat Hunter at Group-IB DFIR Team

Today, on November 3, BlackMatter gang announced it was shutting its Ransomware-as-a-Service program due to the "pressure from the authorities".

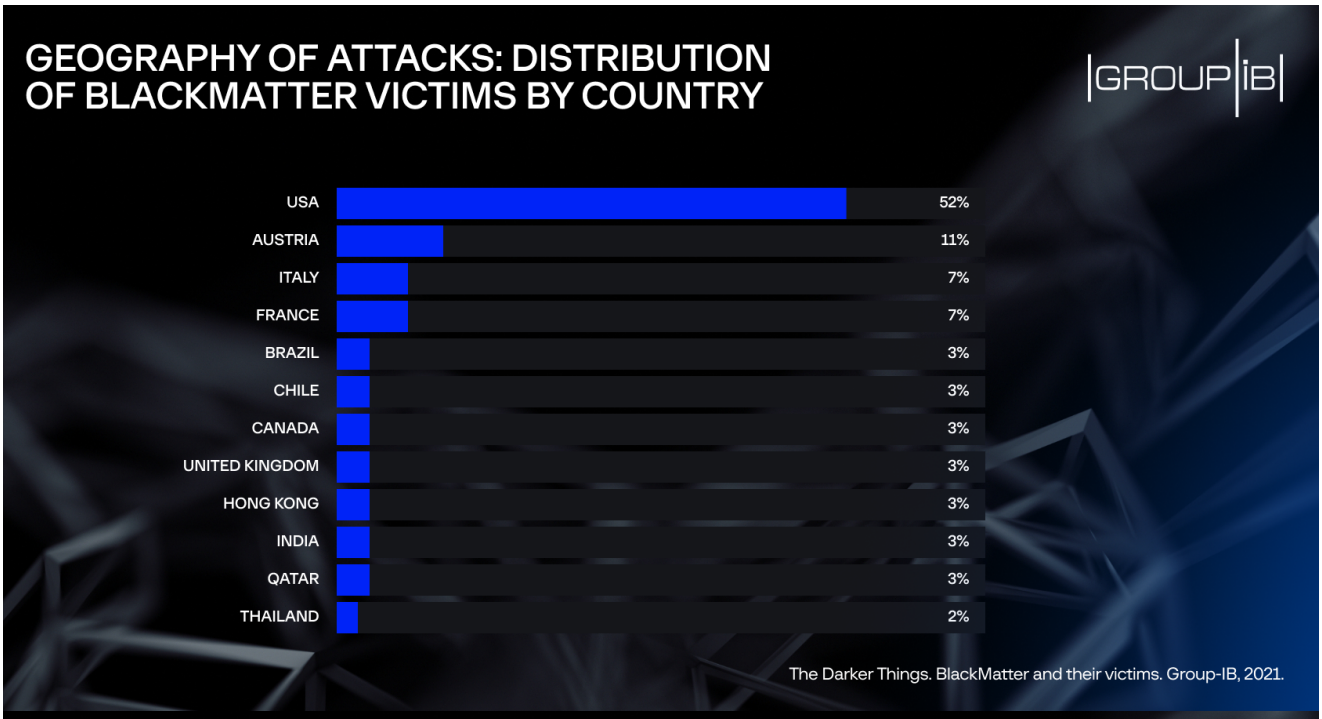
However, it doesn't mean that BlackMatter's affiliates will stop malicious activity. They will most likely join other RaaS programs. In addition, this might just be an attempt to have a fresh start under a different name. Just like BlackMatter was a rebranding of DarkSide, a new successor may appear soon. Therefore, given the similarities that we observed between DarkSide and BlackMatter ransomware back in August, it's important to be aware of the latest ransomware versions' features: malware configuration, encryption mechanisms in use etc.

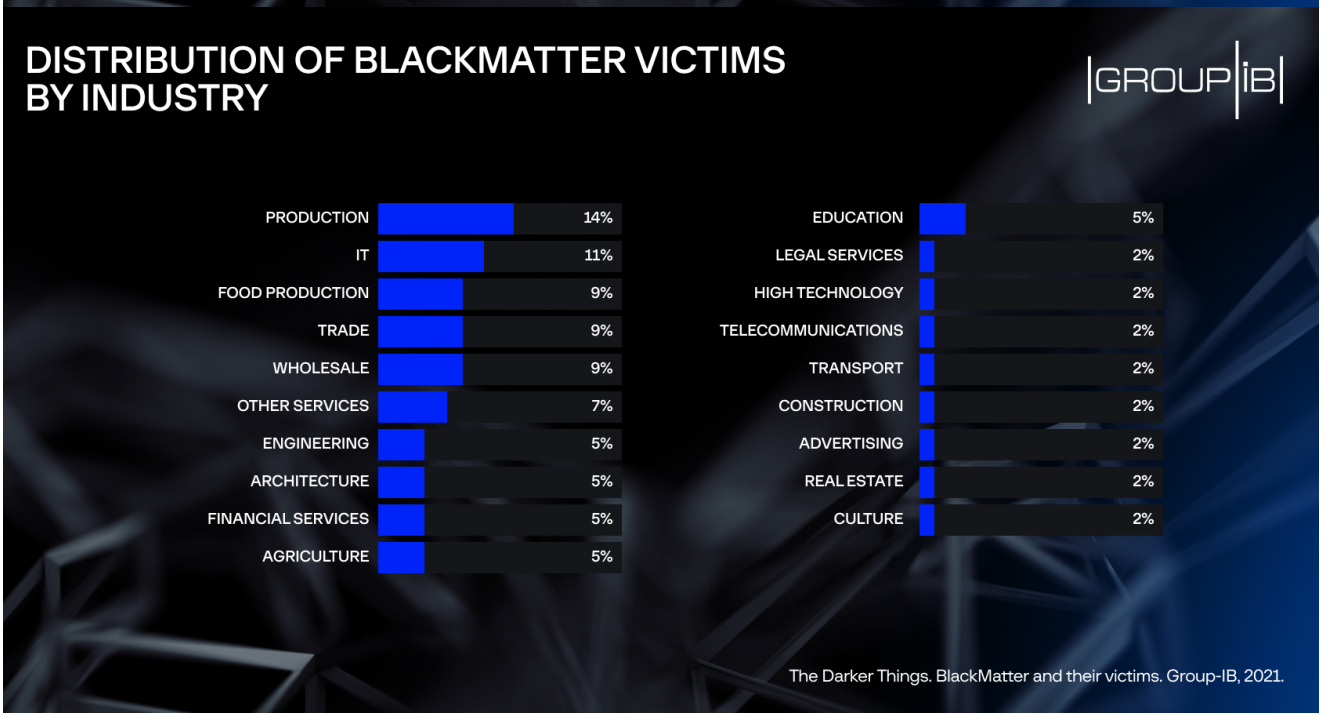
For this purpose the experts from Group-IB's Digital Forensics and Incident Response Team analyzed new BlackMatter samples for Windows and Linux, Andrey Zhdanov, Group-IB's threat hunter, will share new data on his findings.

A US architectural firm was among the first to fall victim to BlackMatter in late July 2021. Since then, the BlackMatter operators' appetites have grown considerably, the frequency of attacks has increased, and the threat actors seem to have been constantly improving their tools. The average ransom demand is $5.3 million, with the maximum, which the attackers demanded from Japan's Olympus Corporation, reaching $30 million.




BlackMatter affiliates try their best to pick their victims carefully, so as not to draw too much attention, but they are not exactly succeeding. Since the first BlackMatter attacks were reported, they have received a lot of very close attention from threat researchers. And on 18 October 2021, the CISA, FBI, and NSA issued joint recommendations, naming BlackMatter ransomware responsible for attacks on U.S. critical infrastructure that had begun in July 2021. As of November 2021, the list of BlackMatter victims consists of more than 50 companies based in the US, Austria, Italy, France, Japan, and other countries.




### BlackMatter for Windows

Depending on command line parameters, ransomware for Windows can operate in five different modes. We were able to obtain command line arguments based on analysis of their hashes.

-path [PATH] – encryption of the specified object (directory, file, network resource).

-safe – self-registration in the RunOnce key of system registry, reboot for file encryption in safe mode.

-wall – creating a BMP image with information about encryption of files and setting it as the desktop wallpaper.

[PATH] – encryption of a specified directory/file.

When other parameters are set or any parameters are absent, the system is fully encrypted according to the configuration settings. Upon completing the encryption, the ransomware creates a BMP image alerting that files have been encrypted, which it then sets as the desktop wallpaper. Starting from version 1.4, the ransomware can also print the text of the demand for ransom on the victim's default printer.

When BlackMatter launches, it checks the rights of the current user and, if necessary, tries to bypass the UAC (User Account Control) through privilege escalation using the ICMLuaUtil COM interface. Also, if the appropriate flag is set in the configuration, it attempts to authenticate using the credentials contained in the configuration data.

Before starting the encryption, BlackMatter deletes shadow copies of partitions using WQL queries (WMI Query Language).

To encrypt files, BlackMatter uses the most efficient multithreading implementation based on the use of the I/O (input/output) completion port. The malware also sets the highest priority (THREAD_PRIORITY_HIGHEST) for the file enumeration and encryption streams. By default, only the first megabyte of file contents is encrypted. In earlier versions, data was encrypted using Salsa20. Apparently, the authors of BlackMatter, just like the authors of another extortionist Petya five years ago, made mistakes in the implementation of the Salsa20 algorithm. Starting from version 1.9, the contents of the files are encrypted already using a modified version of the implementation of the ChaCha20 algorithm, presumably taken from CryptoPP library. Furthermore, the ChaCha20 encryption algorithm is implemented using SSSE3 processor instructions. ChaCha20 keys are encrypted using the RSA-1024 public key. A data block with an encrypted key is appended to the end of the file. The names of the encrypted files are as follows:

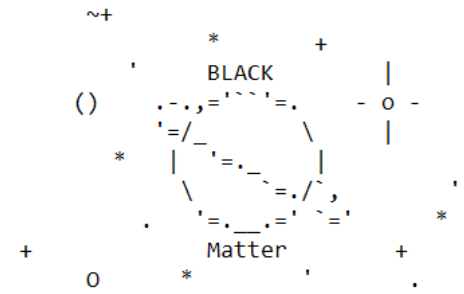
[FILENAME].[VICTIM_ID]

FILENAME – is the original name of the file.

VICTIM_ID – is the victim ID generated on the basis of the string contained in the MachineGuid value of the HKLM\SOFTWARE\Microsoft\Cryptography registry key.

The BlackMatter configuration contains the names of directories, files and extensions skipped during the encryption process as lists of checksums (hashes).

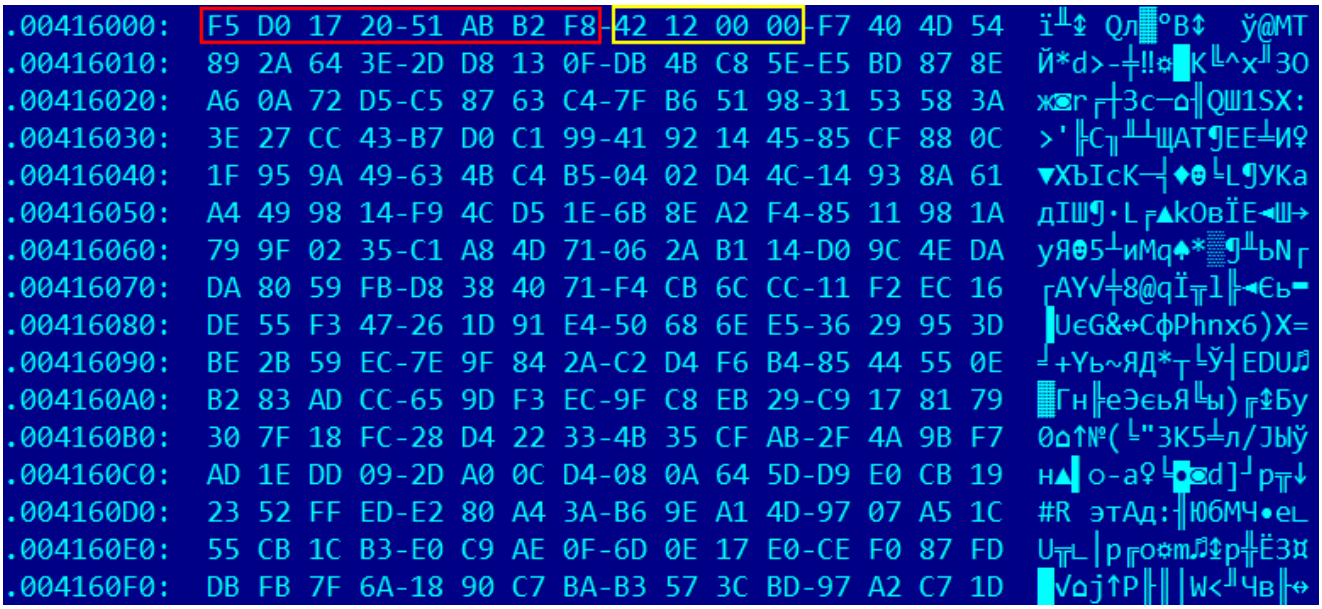
In each processed directory, the ransomware creates text files containing the demand for ransom:
[VICTIM_ID].README.txt



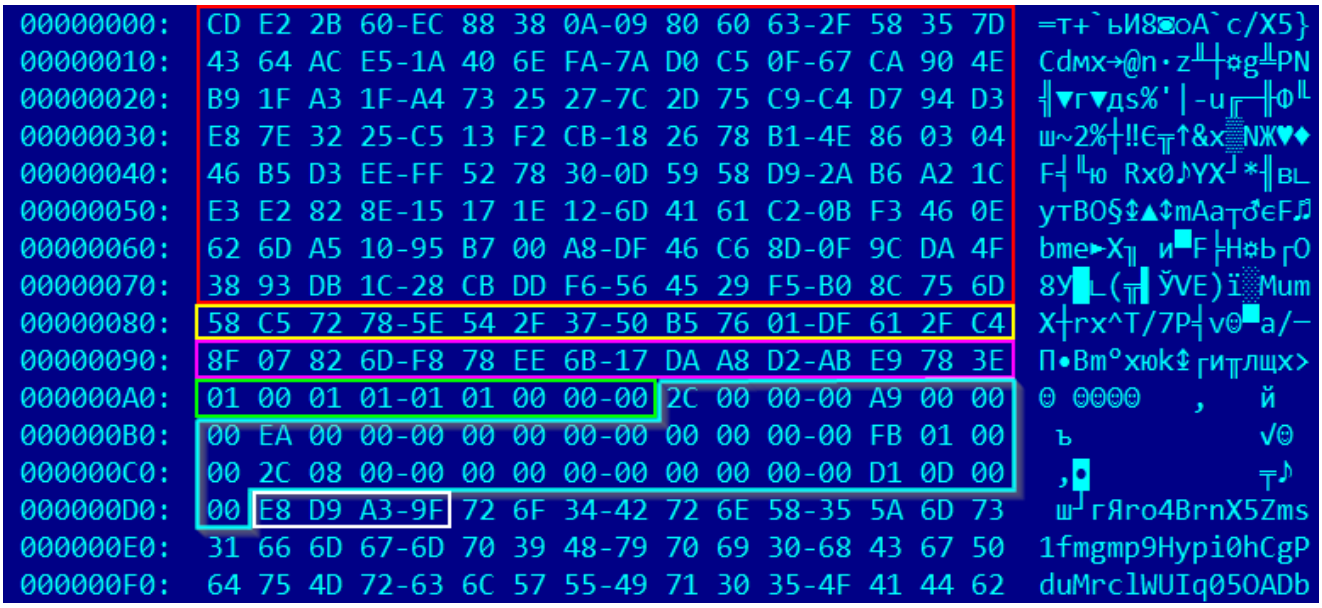

```
>>> Hello Expert System SpA
        We offer you a quick solution to this problem without too much fuss and publicity.
        You buy our decryption software and we remove all the information we were able to pull
from your network.
        Otherwise, we will make the incident public and notify your customers of the data theft
and hacking.
        The reputation will be ruined and may cause much more damage than the opportunity to
negotiate with us.
        If you value your time and money of your clients, we are waiting for the dialogue in our
chat room, the link to which you will find below.

>>> What happens?
   Your network is encrypted, and currently not operational.
   We need only money, after payment we will give you a decryptor for the entire network and you
will restore all the data.

>>> What data stolen?
        From your network was stolen of data.
        If you do not contact us we will publish all your data will send it to the biggest mass
media and your customers.

>>> What guarantees?
   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.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the
future, this does not comply with our goals.
   We always keep our promises.

>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/YX6RXMC65MRX8LLQ

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

## Configuration

The BlackMatter configuration data for Windows is contained in a section disguised as a ".rsrc" resource section, but there are no resources in it.




The first 64-bit number (0F8B2AB512017D0F5h) in the section represents the initial value for the pseudo-random sequence generator (random seed) used to encrypt the program data. The next 32-bit value represents the actual size of the configuration data. Prior to encryption, the configuration data was pre-compressed using the aPLib compression algorithm, which is popular among ransomware developers. Previously, this algorithm was found, for example, in such ransomware families as DarkSide, DoppelPaymer, Clop, and others.




Configuration data after decryption and decompression.

Logical flags that indicate the ransomware settings:

Offset table of configuration parameter values.

The table contains 32-bit numbers that represent offsets relative to the beginning of the list itself to the rest of the configuration data fields as Base64 strings, ending with a null byte. If the offset is 0, there is no field value.

## Known versions

### BlackMatter for Linux

BlackMatter ransomware for Linux targets VMware ESXi servers. According to the settings in the configuration data, the ransomware can stop virtual machines and terminate specified processes before data encryption. The ransomware also disables the firewall. To encrypt virtual machine files, the ransomware uses the esxcli utility to obtain a list of storages with "vmfs", "vffs" and "nfs" file systems.

BlackMatter for Linux implements multithreaded file encryption with the extensions specified in the configuration. Data is encrypted in blocks that are multiples of one megabyte using the HC-256 stream encryption algorithm. HC-256 keys are encrypted using the RSA-4096 public key. The CryptoPP crypto library is used to implement encryption algorithms.

Data transferring to the attacker-controlled resources on the internet is implemented in the malware using the libcurl library.

### Configuration

BlackMatter configuration data for Linux is contained in the ".cfgETD" section of the ELF file. The data is encrypted, compressed using the zlib data compression library, and encoded using Base64.

Encrypted configuration data after Base64 decoding and zlib decompression:


Configuration data is encrypted using a cyclic bytewise XOR operation using the key contained in the first 32 bytes.

After decryption, the configuration data is in JSON format.

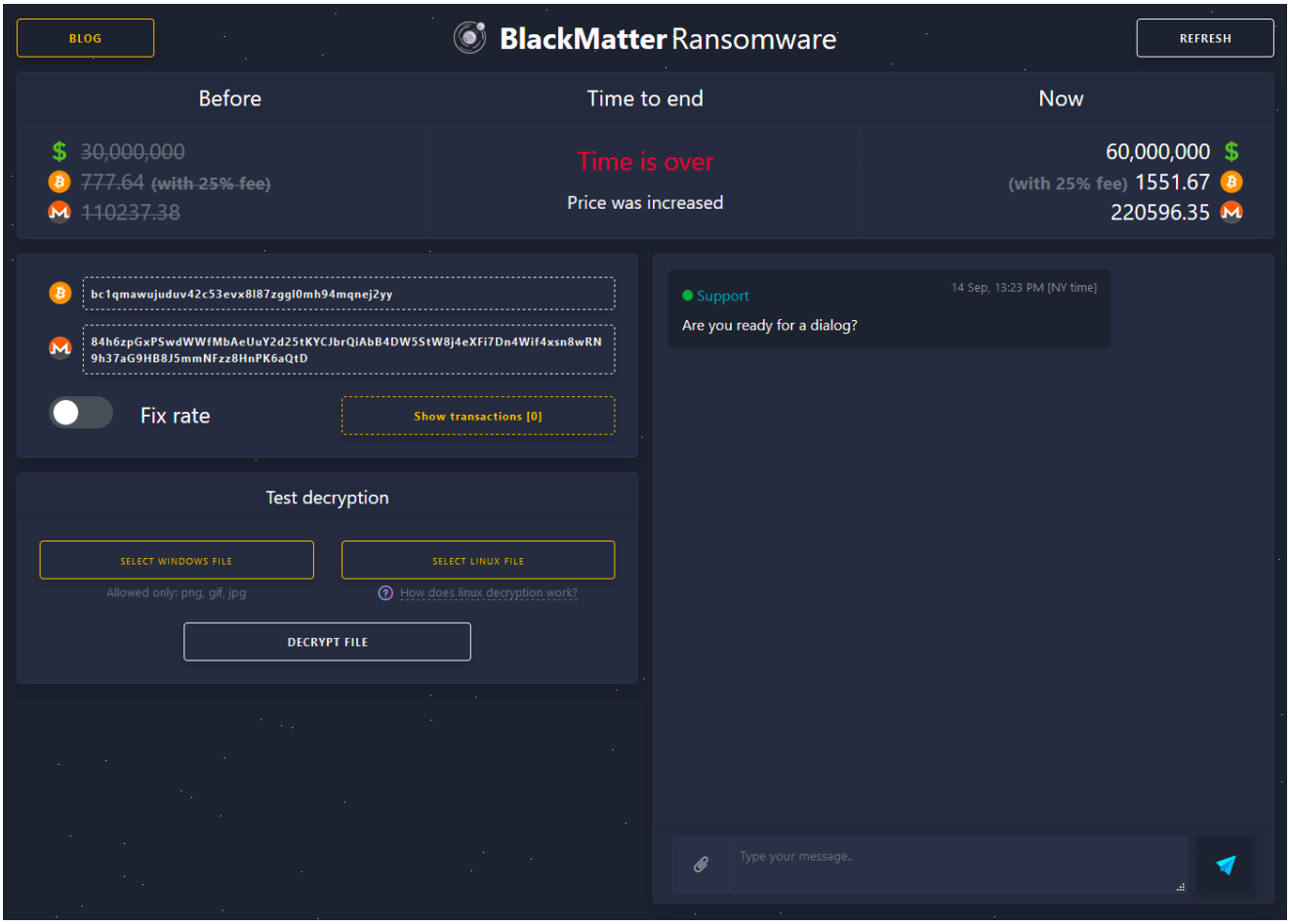
```
{
    "rsa": "MIICIDANBgkqhkiG9w0BAQEFAAOCAg0AMIICCAKCAgEA5uyveIuEmAkom7Z2ygCPkrm9tJa+4QWJxPhaRwR5c
    "remove-self": "true",
    "worker-concurrency": "0",
    "disk": {
        "enable": "true",
        "type": "single",
        "dark-size": "512",
        "white-size": "30720",
        "min-size": "0",
        "extension-list": "vmdk,vmem,vswp,log"
    },
    "log": {
        "enable": "true",
        "level": "info",
        "path": "\/tmp\/main.log"
    },
    "message": {
        "enable": "true",
        "file-name": "ReadMe.txt",
        "file-content": "      ~+                                          \n               *
    },
    "landing": {
        "enable": "true",
        "bot-id": "b0e039b42ef6c19c2189651c9f6c390e",
        "key": "e2c8e7120397b549de02a0282f6a3353",
        "urls": [
            "http:\/\/mojobiden.com",
            "http:\/\/nowautomation.com"
        ]
    },
    "kill-vm": {
        "enable": "true",
        "ignore-list": [
            "VMware vCenter",
            "VMware-VirtualSAN-Witness",
            "mfldc01.mflgroup.local",
            "mfldc02.mflgroup.local",
            "MFLDC1.MFLGROUP.local",
            "MFLDC2.MFLGROUP.local",
            "MFLDC05.MFLGROUP.local",
            "mfldc04.mflgroup.local",
            "mfldc03.mflgroup.local"
        ]
    },
    "kill-process": {
        "enable": "true",
        "list": [
            "vmsyslogd"
        ]
    }
}
```


Configuration parameters

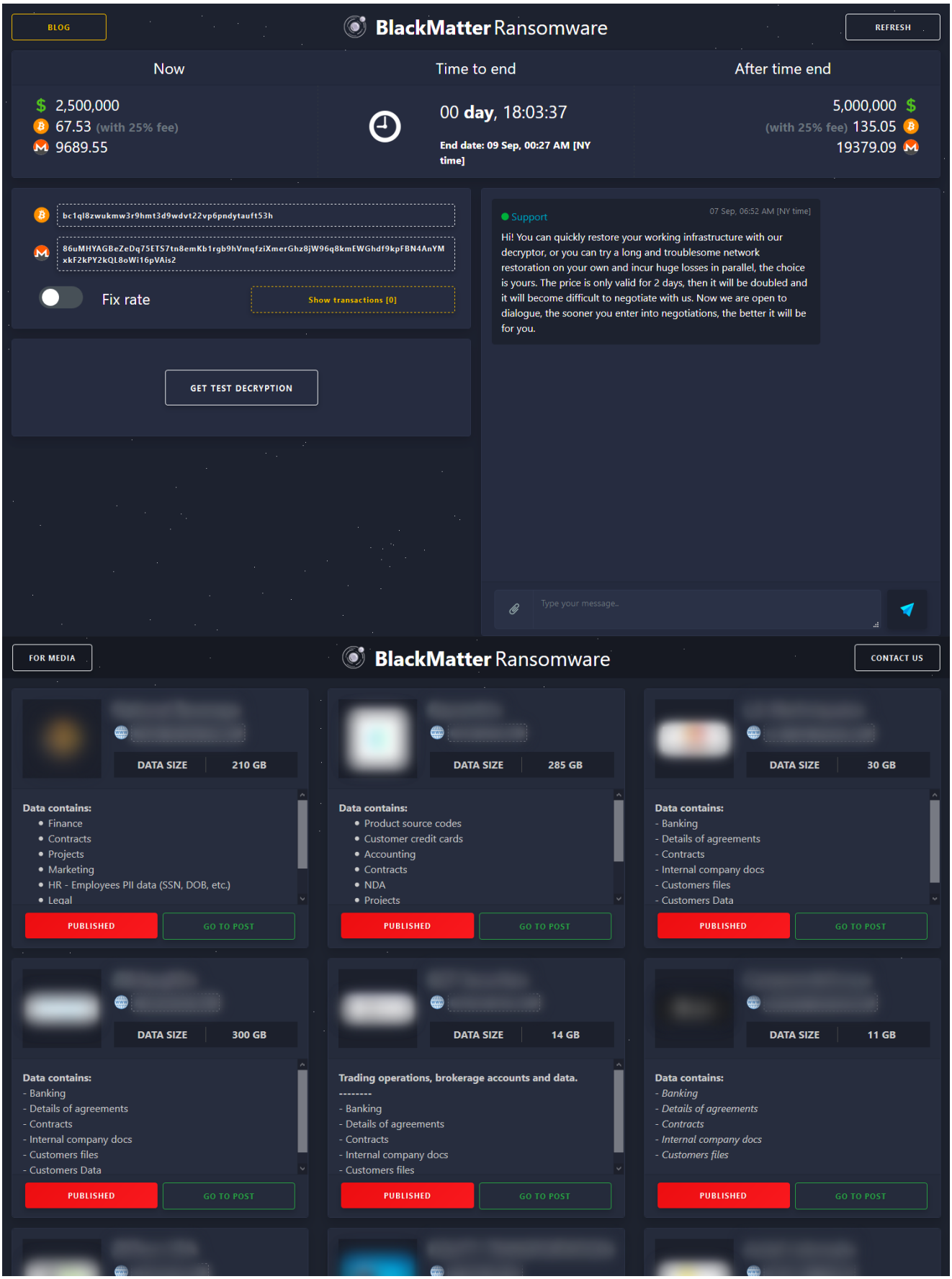
## Known versions

## Victims and threat actors

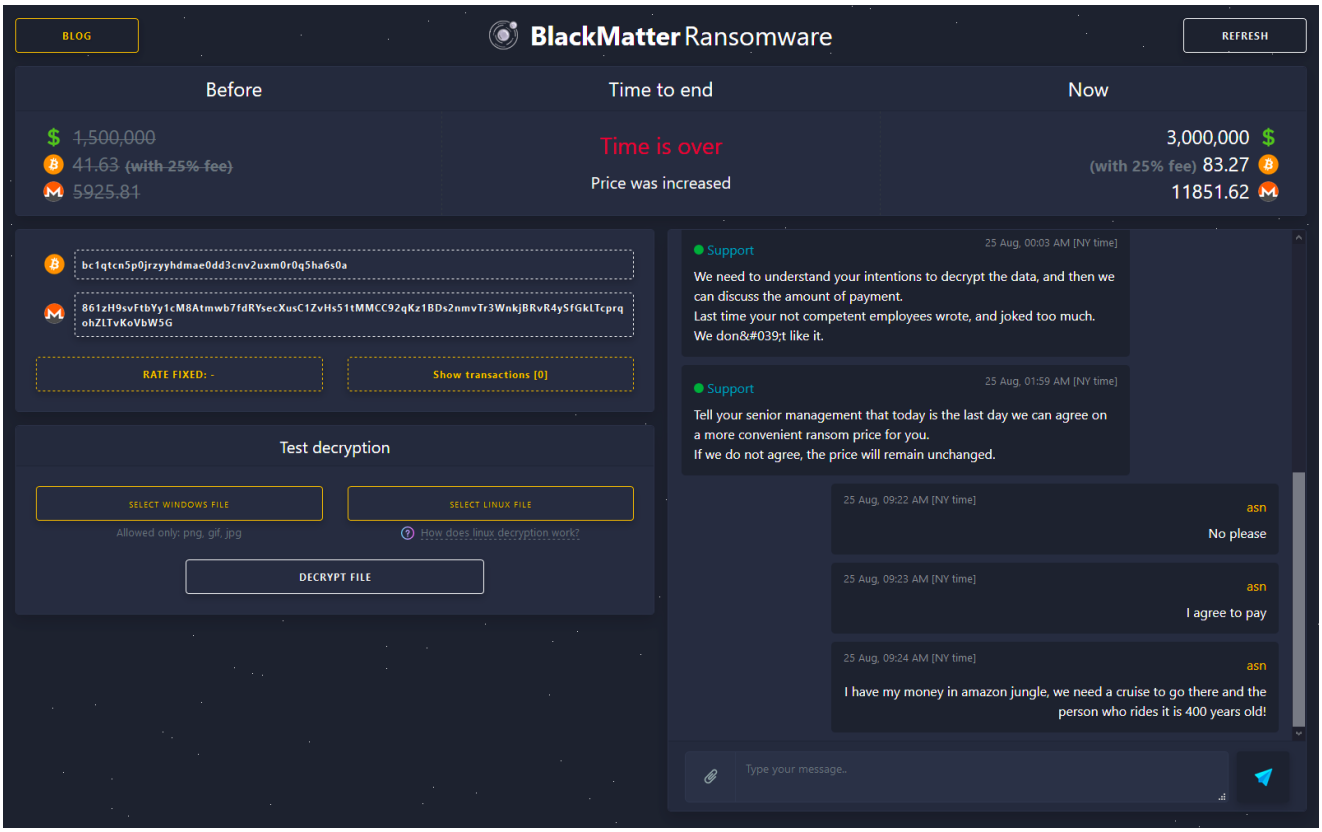
To identify its victims, BlackMatter uses a unique 16-byte identifier contained in the configuration data: company_id (Windows version) and bot-id (Linux version). For each victim, the attackers create a Tor chat room for communication. The link to this chat is specified in the text file containing the ransom demand.

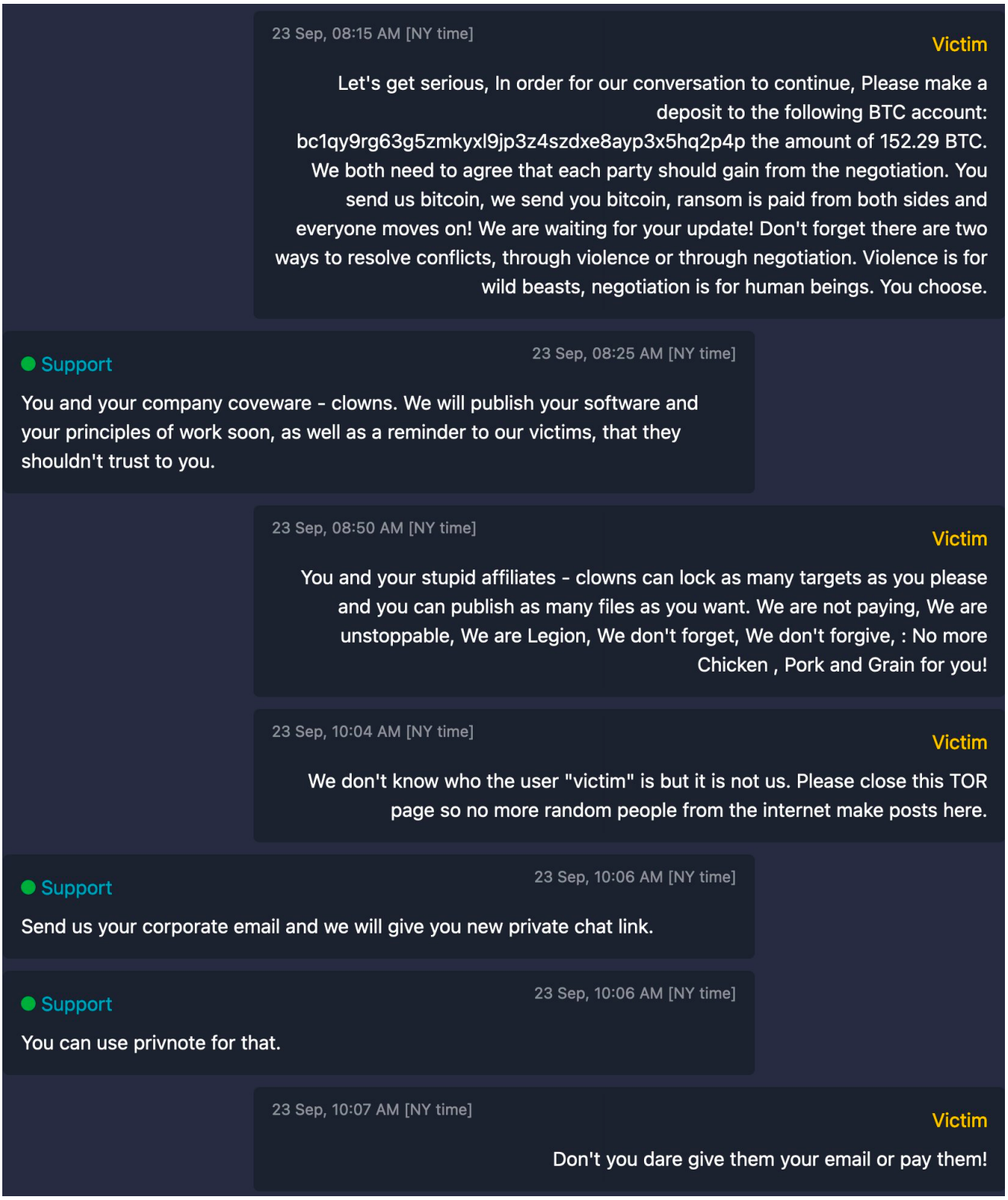



When the ultimatum expires, the threat actors double the ransom amount, and later publish the stolen documents after the victim refuses to pay.



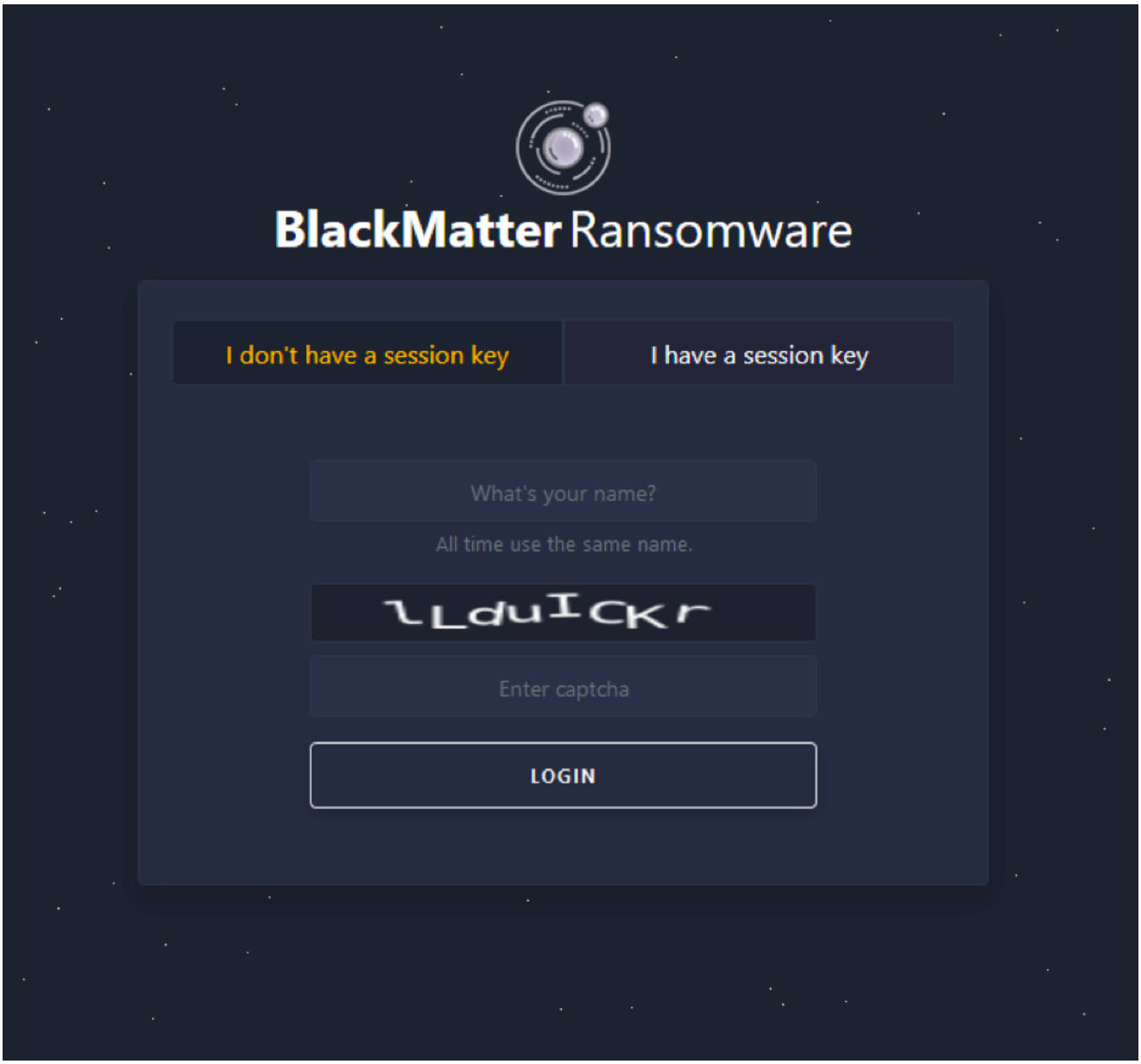

Initially, these chats were public, and many people were privy to the correspondence between BlackMatter "tech support" and their victims and even tried to outwit them.

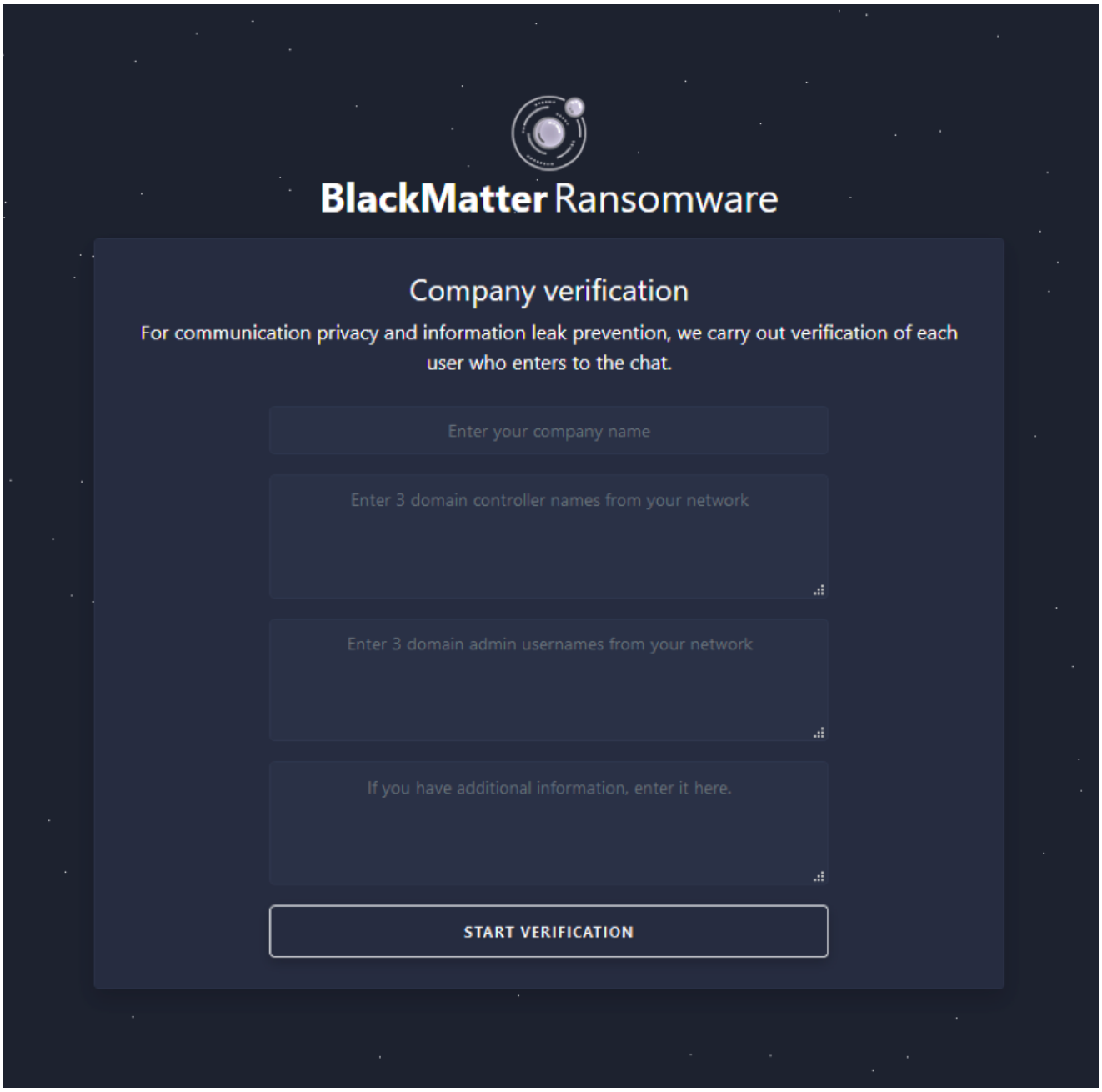

BLOG
BlackMatter Ransomware
REFRESH
Before
Time to end
Now
$ 1,500,000
41.63 (with 25% fee)
5925.81
Time is over
Price was increased
3,000,000 $
(with 25% fee) 83.27
11851.62
bc1qtcn5p0jrzyyhdmae0dd3cnv2uxm0r0q5ha6s0a
861zH9svFtbYy1cM8Atmwb7fdRYsecXusC1ZvHs51tMMCC92qKz1BDs2nmvTr3WnkjBRvR4ySfGkLTcprqohZLTvKoVbW5G
RATE FIXED: -
Show transactions [0]
Test decryption
SELECT WINDOWS FILE
SELECT LINUX FILE
Allowed only: png, gif, jpg
How does linux decryption work?
DECRYPT FILE
Support
25 Aug, 00:03 AM [NY time]
We need to understand your intentions to decrypt the data, and then we can discuss the amount of payment.
Last time your not competent employees wrote, and joked too much.
We don't like it.
Support
25 Aug, 01:59 AM [NY time]
Tell your senior management that today is the last day we can agree on a more convenient ransom price for you.
If we do not agree, the price will remain unchanged.
25 Aug, 09:22 AM [NY time]
asn
No please
25 Aug, 09:23 AM [NY time]
asn
I agree to pay
25 Aug, 09:24 AM [NY time]
asn
I have my money in amazon jungle, we need a cruise to go there and the person who rides it is 400 years old!
Type your message..



Source: https://twitter.com/ddd1ms/status/1441044423798820889

On September 23, 2021, BlackMatter partners closed public access to chat rooms, and now a session key is required to log in, which requires verification of the company and confirmation of the victim's affiliation.


BlackMatter Ransomware
I don't have a session key
I have a session key
What's your name?
All time use the same name.
lLduIckr
Enter captcha
LOGIN




### Victimology

Company_id IDs and Tor links extracted from the ransomware and text files containing the ransom demand.

As mentioned above, BlackMatter partners are trying not to draw attention to their activities, so the threat actors choose small and medium-sized businesses as the targets of their attacks. However, the attacks on Olympus and NEW cooperative caused a public outcry.

### Indicators of compromise

https://paymenthacks[.]com
http://paymenthacks[.]com
https://mojobiden[.]com

http://mojobiden[.]com
https://nowautomation[.]com
http://nowautomation[.]com
https://fluentzip[.]org
http://fluentzip[.]org

**SHA-256**

072158f5588440e6c94cb419ae06a27cf584afe3b0cb09c28eff0b4662c15486

22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6

2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009

3a03530c732ebe53cdd7c17bee0988896d36c2b632dbd6118613697c2af82117

4ad9432cc817afa905bab2f16d4f713af42ea42f5e4fcf53e6d4b631a7d6da91

6155637f8b98426258f5d4321bce4104df56c7771967813d61362c2118632a7b

668a4a2300f36c9df0f7307cc614be3297f036fa312a424765cdb2c169187fe6

72687c63258efe66b99c2287748d686b6cca2b0eb6f5398d17f31cb46294012c

7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984

c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99

c728e3a0d4a293e44314d663945354427848c220d05d5d87cdedd9995fee3dfe

f63c6d08ebfba65173763c61d3767667936851161efa51ff4146c96041a02b20

84af3f15701d259f3729d83beb15ca738028432c261353d1f9242469d791714f
a6e14988d91f09db44273c79cba51c16b444afafa37ba5968851badb2a62ef27

7c642cdeaa55f56c563d82837f4dc630583b516a5d02d5a94b57b65489d74425

cf60d0d6b05bfe2e51ca9dac01a4ae506b90d78d8d9d0fc266e3c01d8d2ba6b7

6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db

86c84c07e27cc8aba129e1cf51215b65c445f178b94f2e8c4c10e6bc110daa94

b824bbc645f15e213b4cb2628f7d383e9e37282059b03f6fe60f7c84ea1fed1f

e4fd947a781611c85ea2e5afa51b186de7f351026c28eb067ad70028acd72cda
2466fca0e29b06c78ffa8a44193fb58c30e6bec4e54bbef8e6622349b95cce4c

0751c422962dcd500d7cf2cf8bf544ddf5b2fe3465df7dd9b9998f6bba5e08a4

1c63a4fdee1528429886a0de5e89eaa540a058bf27cd378b8d139e045a2f7849

1eea3cbd729d4493c0c0a84efe6840abf1760efe221dc971d32ca5017b5c19c2

20742987e6f743814b25e214f8b2cd43111e2f60a8856a6cca87cafd85422f41

2cdb5edf3039863c30818ca34d9240cb0068ad33128895500721bcdca70c78fd

2e50eb85f6e271001e69c5733af95c34728893145766066c5ff8708dcc0e43b2

3a4bd5288b89aa26fbe39353b93c1205efa671be4f96e50beae0965f45fdcc40

4be85e2083b64838fb66b92195a250228a721cdb5ae91817ea97b37aa53f4a2b

520bd9ed608c668810971dbd51184c6a29819674280b018dc4027bc38fc42e57

5da8d2e1b36be0d661d276ea6523760dbe3fa4f3fdb7e32b144812ce50c483fa

66e6563ecef8f33b1b283a63404a2029550af9a6574b84e0fb3f2c6a8f42e89f

706f3eec328e91ff7f66c8f0a2fb9b556325c153a329a2062dc85879c540839d

8323fdfda08300c691d330badec2607ea050cc10ee39934faeebedf3877df3ac

8f1b0affffb2f2f58b477515d1ce54f4daa40a761d828041603d5536c2d53539

9cf9441554ac727f9d191ad9de1dc101867ffe5264699cafcf2734a4b89d5d6a

b0e929e35c47a60f65e4420389cad46190c26e8cfaabe922efd73747b682776a

b4b9fdf30c017af1a8a3375218e43073117690a71c3f00ac5f6361993471e5e7

cb5a89a31a97f8d815776ff43f22f4fec00b32aae4f580080c7300875d991163

e4a2260bcba8059207fdcc2d59841a8c4ddbe39b6b835feef671bceb95cd232d

e9b24041847844a5d57b033bf0b41dc637eba7664acfb43da5db635ae920a1b4

eaac447d6ae733210a07b1f79e97eda017a442e721d8fafe618e2c789b18234b

eafce6e79a087b26475260afe43f337e7168056616b3e073832891bf18c299c1

f7b3da61cb6a37569270554776dbbd1406d7203718c0419c922aa393c07e9884

496cd9b6b6b96d6e781ab011d1d02ac3fc3532c8bdd07cae5d43286da6e4838d

2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c

4524784688e60313b8fefdebde441ca447c1330d90b86885fb55d099071c6ec9

5236a8753ab103634867289db0ba1f075f0140355925c7bd014de829454a14a0

69e5f8287029bcc65354abefabb6854b4f7183735bd50b2da0624eb3ae252ea8

730f2d6243055c786d737bae0665267b962c64f57132e9ab401d6e7625c3d0a4

8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952

ccee26ea662c87a6c3171b091044282849cc8d46d4b9b9da6cf429b8114c4239

ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f526c1fe3b8bf2d6e7404

fe2b2beeff98cae90f58a5b2f01dab31eaa98d274757a7dd9f70f4dc8432a6e2

26a7146fbed74a17e9f2f18145063de07cc103ce53c75c8d79bbc5560235c345

7a223a0aa0f88e84a68da6cde7f7f5c3bb2890049b0bf3269230d87d2b027296

9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58

2f20732aaa3d5ce8d2efeb37fe6fed7e73a29104d8227a1160e8538a3ee27dad

9a8cd3a30e54a2ebb6d73fd7792ba60a6278a7301232321f226bb29fb8d0b3d6

1247a68b960aa81b7517c614c12c8b5d1921d1d2fdf17be636079ad94caf970f

6a7b7147fea63d77368c73cef205eb75d16ef209a246b05698358a28fd16e502

1247a68b960aa81b7517c614c12c8b5d1921d1d2fdf17be636079ad94caf970f

6a7b7147fea63d77368c73cef205eb75d16ef209a246b05698358a28fd16e502
d4645d2c29505cf10d1b201826c777b62cbf9d752cb1008bef1192e0dd545a82

**YARA rules**

```
/*
BlackMatter ransomware
*/

import "elf"

rule DarkSide_BM
{
    meta:
        author = "Andrey Zhdanov"
        company = "Group-IB"
        family = "ransomware.darkside_blackmatter"
        description = "DarkSide/BlackMatter ransomware Windows payload"
        severity = 10
        score = 100

    strings:
        $h1 = { 64 A1 30 00 00 00 8B B0 A4 00 00 00 8B B8 A8 00
                00 00 83 FE 05 75 05 83 FF 01 }

    condition:
        ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
        (
            (1 of ($h*))
        )
}

rule BlackMatter
{
    meta:
        author = "Andrey Zhdanov"
        company = "Group-IB"
        family = "ransomware.blackmatter.windows"
        description = "BlackMatter ransomware Windows payload"
        severity = 10
        score = 100

    strings:
        $h0 = { 80 C6 61 80 EE 61 C1 CA 0D 03 D0 }
        $h1 = { 02 F1 2A F1 B9 0D 00 00 00 D3 CA 03 D0 }
        $h2 = { 3C 2B 75 04 B0 78 EB 0E 3C 2F 75 04 B0 69 EB 06
                3C 3D 75 02 B0 7A }
        $h3 = { 33 C0 40 40 8D 0C C5 01 00 00 00 83 7D 0? 00 75
                04 F7 D8 EB 0? }

    condition:
        ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
        (
            (1 of ($h*))
        )
}

rule BlackMatter_Linux
{
    meta:
```

```
        author = "Andrey Zhdanov"
        company = "Group-IB"
        family = "ransomware.blackmatter.linux"
        description = "BlackMatter ransomware Linux payload"
        severity = 10
        score = 100

    strings:
        $h0 = { 0F B6 10 84 D2 74 19 0F B6 34 0F 40 38 F2 74 10
                48 83 C1 01 31 F2 48 83 F9 20 88 10 49 0F 44 C9
                48 83 C0 01 4C 39 C0 75 D7 }
        $h1 = { 44 42 46 44 C7 4? [1-2] 30 35 35 43 C7 4? [1-2]
                2D 39 43 46 C7 4? [1-2] 32 2D 34 42 C7 4? [1-2]
                42 38 2D 39 C7 4? [1-2] 30 38 45 2D C7 4? [1-2]
                36 44 41 32 C7 4? [1-2] 32 33 32 31 C7 4? [1-2]
                42 46 31 37 }

    condition:
        (uint32(0) == 0x464C457F) and
        (
            (1 of ($h*)) or
            for any i in (0..elf.number_of_sections-2):
            (
                (elf.sections[i].name == ".app.version") and
                (elf.sections[i+1].name == ".cfgETD")
            )
        )
}
```

**How to protect your network against ransomware:**

Make your remote access tools secure. Use multifactor authentication or at least set complex passwords and change them regularly.

Eliminate vulnerabilities in publicly accessible apps as soon as possible, especially those that could allow attackers to bypass the external perimeter.

Implement comprehensive email protection to detect and stem the most sophisticated threats. More
Monitor what your contractors do in your network. Providing them with remote access should be strictly regulated.

Instantly patch vulnerabilities on hosts on the internal network that attackers could leverage to escalate privileges or propagate across the network.

Monitor the use of dual-use tools that could help attackers conduct network reconnaissance, obtain authentication data, and much more.

Restrict access to cloud storage. This will help keep attackers from exfiltrating data from the corporate network.

Make sure all accounts have the least possible privileges on the systems. In case of an attack, this will make it difficult for threat actors to move laterally across the network.

Use separate accounts with multifactor authentication to access servers containing backups. Moreover, make sure that you have offline copies.

Implement a modern threat monitoring and blocking tool that will help contain and repel attacks at any stage of the kill chain. More
For more information about attacks using manually controlled ransomware, see the Group-IB report " Ransomware 2020/2021":