Unknown Title

⋮ 9/23/2025

NOTE: This is a lengthy investigation that eventually took four months. Any future updates of this group would be reflected in this same blog post.

TABLE OF CONTENTS

- NEGOTIATION ANALYSIS
- RANSOM NOTE ANALYSIS
- NEW SAMPLE ANALYSIS
- LEAK ANALYSIS: FOUND MALWARE AMONG VICTIM BREACH
- DETECTION NAME ANALYSIS
- WHY THE UNITED STATES NOT ON THE VICTIM LIST  ?
- MITRE ATT&CK TTPs
- IOC

EXECUTIVE SUMMARY

Gunra Ransomware is a Double Extortion Ransomware group that primarily targets global victims, excluding the **US**, unlike other Ransomware Groups. The group had targeted only a single English-speaking country—**Canada** so far. They target Windows primarily, and rolled out their Linux counterpart recently, which marks the continuous development.

The group uses Phishing as a main attack vector to deliver malicious pieces to their targets and carry out negotiations on a WhatsApp-themed chat Panel. The group is capable to encrypt huge files (9TB) in a limited timeframe by using advanced stream cipher encryption such as **Salsa20 or ChaCha20**.

They undergo several changes on their DLS (Data Leak Site) in a short time, hence adopting a hit-and-trial for a wider audience reach. This Research includes the modus operandi of the group and the handy tools used by the group during their operations.

INTRODUCTION

Gunra Ransomware appeared initially on **23rd April 2025**. Like other Ransomware Groups, this group lists its victims on their DLS (Data Leak Site).

Artistic Representation | Credit: Self-AI

They specifically targets Windows Environment (EXE) and also targets ELF (Linux) machines recently.

VICTIMOLOGY

Surprisingly, **not a single US victim has been found** (till now). This is a rare situation in the Ransomware Scenario, as the US tops the list in every Ransomware Ecosystem.

At the time of writing, the group has added 18 victims between April and September 2025.

Here, the list is topped by **South Korea, Brazil, Japan, Canada, UAE, Egypt,** and **Panama**. From the victim list, we can see that only 1 single English-Speaking Nation is targeted i.e. **CANADA**.

Apart from the above nations: **Columbia, Nicaragua, Croatia, Italy** are also part of Gunra Victim List.

> **NOTE**: Either the group does not target US entities due to strong extradition policies (if found), or their national interest lies in the US

Sectors targeted by the group are:-

- MANUFACTURING
- HEALTHCARE
- TECHNOLOGY
- SERVICE
- FINANCE

GUNRA RANSOMWARE GROUP INTEL

Here are some of the juicy info uncovered during the Investigation:-

- 💡 Negotiation Portal is stylized with a WhatsApp Theme
- 💡 The negotiation portal is possibly hosted with Slack
- 💡 DLS hosted with Apache/2.4.63 (Win64) PHP/8.4.5
- 💡 Used Lumma Stealer in their operations
- 💡 Demanded $10M, then reduced to $7M
- 💡 Demanded $1M from another victim
- 💡 Access to Internal Files and Office 365 Cloud claimed
- 💡 9TB data encrypted in 2 days, i.e 52 MB/s gets encrypted using **Salsa20** or **ChaCha20**, high-speed stream ciphers capable of throughput

They have used a Microsoft Phishing email to lure the victims, which was obtained directly from the Threat Actor:

email.7z

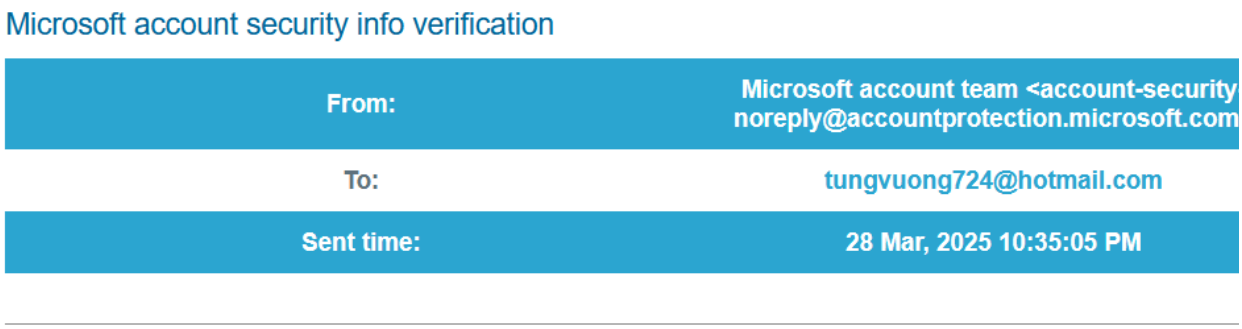
Download from command line:

```
wget https://bashupload.com/FOIGR/email.7z
```

Direct download (9.4 KB)

Phishing Email from Gunra shared

Here is the preview of the email:-



Microsoft account security info verification

From:	Microsoft account team <account-security-noreply@accountprotection.microsoft.com
To:	tungvuong724@hotmail.com
Sent time:	28 Mar, 2025 10:35:05 PM

Microsoft account

Thanks for verifying your security info

Recently, you verified the security info on the Microsoft account tu**4@hotmail.com. This was a periodic security check which only happens if you haven't used a security code recently. You won't need to provide a code every time you sign in.

It's important to keep the security info associated with your account correct and up-to-date. We'll never use this info to spam you or for any marketing purposes — it's only to verify your identity if there's ever a problem with your account.

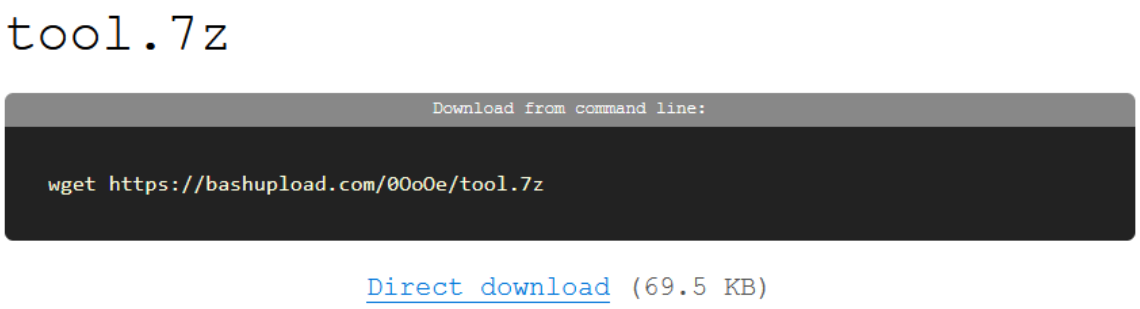
To learn more or contact support, click here.

Phishing Mail from GUNRA Ransomware Group

Title used: Microsoft account security info verification
Email ID: account-security-noreply@accountprotection.microsoft.com

The email is legit and headers are genuine, and does not poses any risk. However, it can be assumed that the threat actor might have shared a genuine mail instead of a malicious one.

Upon inquiring about the tool, they have shared a tool titled "**GUNRA**"



Gunra Group Shared Tool

Upon receiving it, I analyzed it and uploaded it to VT, which you can find here. This sample also have the same functionality spotted with the same file-size.

Gunra Operators are using **Bash Upload Service** as temporary storage to share their leaks or tools.

DIVING INTO DATA LEAK SITE (DLS)

Gunra hosted their Data Leak Site on Version 3 TOR Domain, powered by **Apache/2.4.63 (Win64) PHP/8.4.5**.

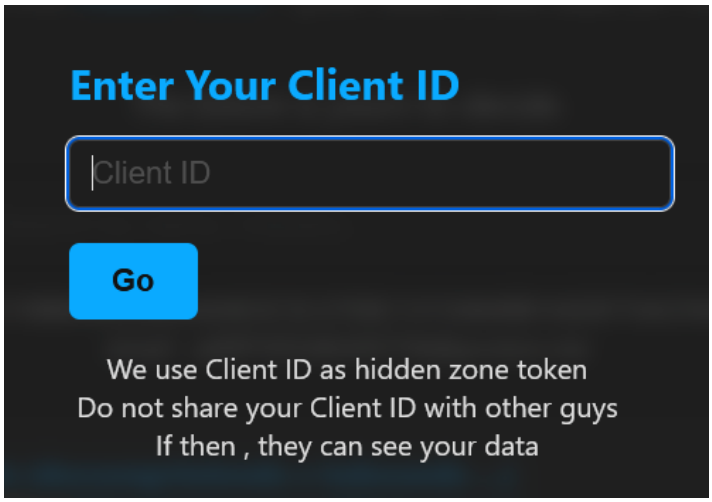
Unlike other Ransomware DLS, this group had facilitated a **Search** option by industry to narrow down the Research. This helps to quickly identify the victim by querying the Industry.

- gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad.onion

Gunra Data Leak Site on Dark Web

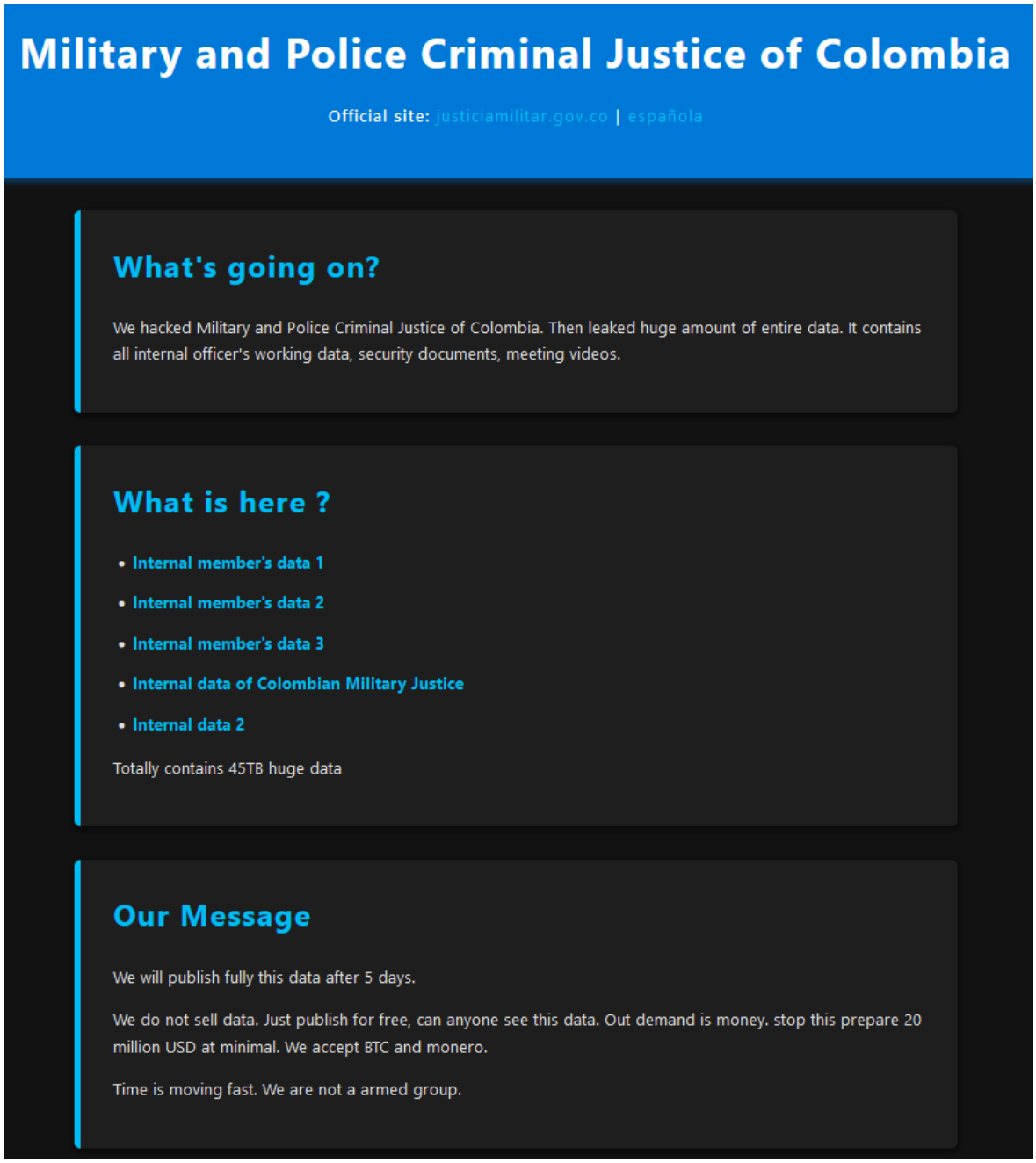
The latest victims are listed/advertised with the "**NEW**" tag. Old victims are listed below.

The "**hidden area**" highlighted on the DLS is the Client Login Panel, which is guarded by a **ClientID** that is found in the Ransom Note.



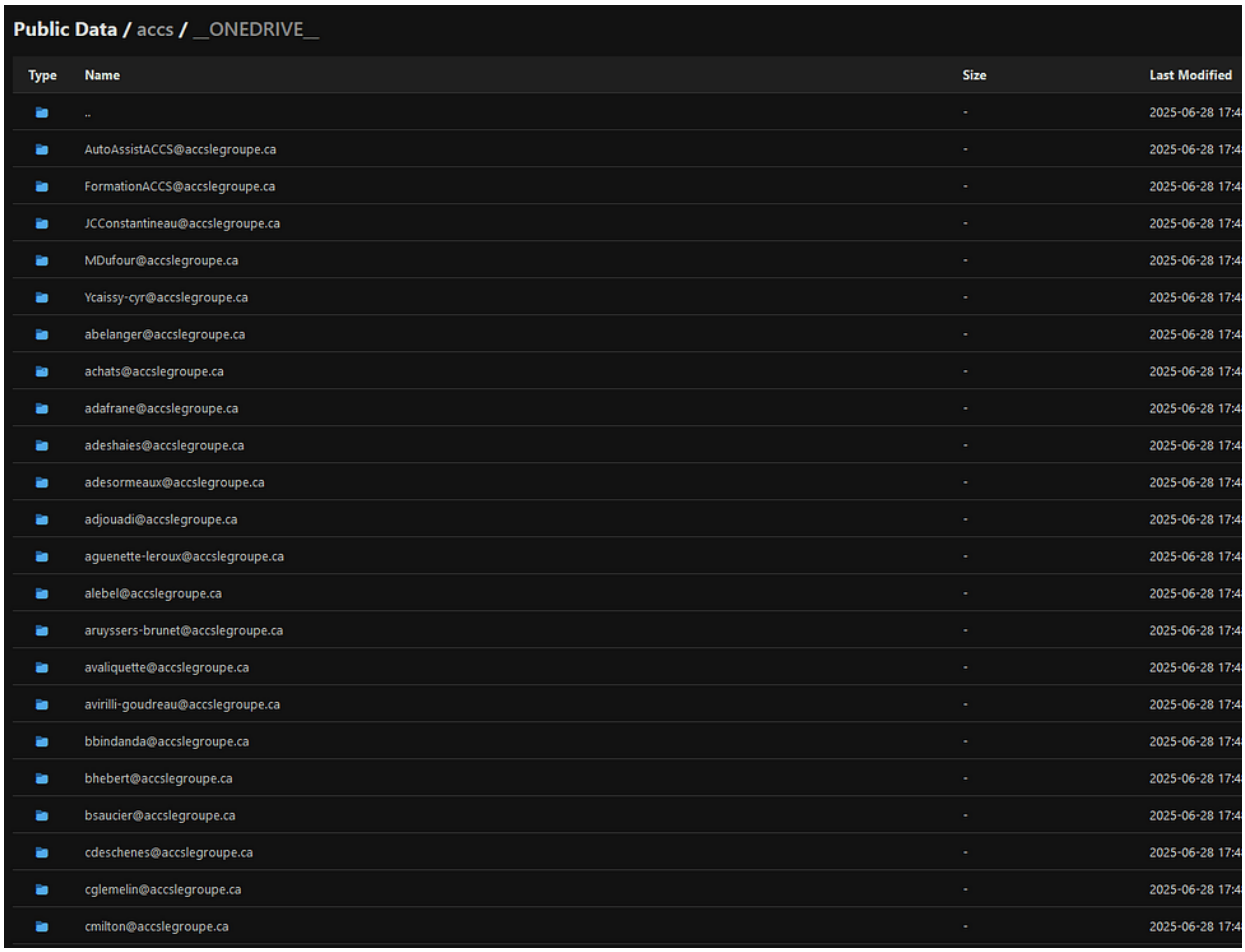
Victim Login Prompt

The victim's data is being guarded with Client ID before releasing it publicly.



Inside Client Login Panel

The data is arranged in a structured way:



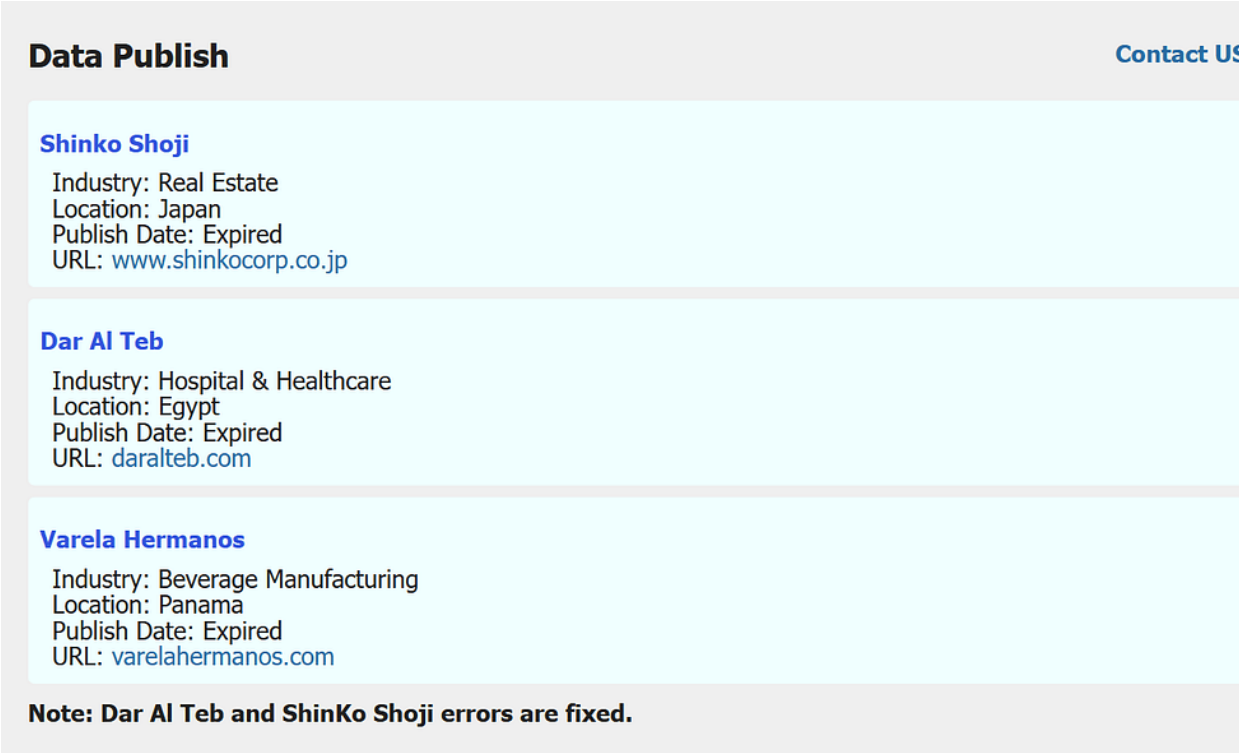
Client Data

As this was a revamped site, the DLS of Gunra didn't look like this earlier. The group had launched its clear web version, which we will look at in the next section.

Let's trace back the old DLS of Gunra Group…

DATA LEAK SITE TIMELINE

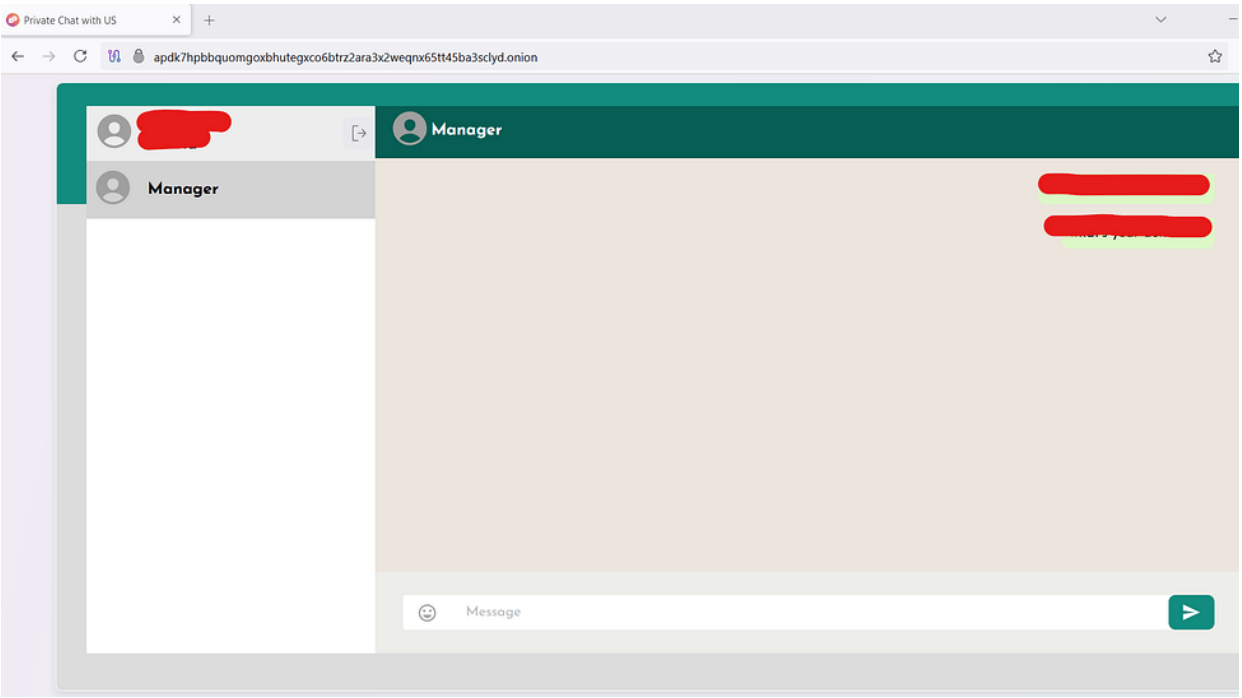
The group initially appeared in **April 2025** with the same TOR Domain. The Gunra Ransomware DLS initially appeared like this:-



Old Data Leak Site of Gunra Ransomware

The group maintains a WhatsApp-themed Negotiation Portal for the victims to communicate, which can be reached at:-

apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion



Negotiation Portal of Gunra

While inspecting the messages, it is found that the Backend of this Negotiation Chat is connected to another TOR Domain:-

2bw7r32r5eshwk2h7uekj3lwzorxds2jyhyzqyilphid3r27x5hsf4yd.onion

This domain is not reachable directly; however, the messages in the Negotiation Portal were being serviced via this domain.

In short:-

`Negotiation Panel`: `apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion`
`Negotiation Panel Backend`:
`2bw7r32r5eshwk2h7uekj3lwzorxds2jyhyzqyilphid3r27x5hsf4yd.onion`

It is found that the group is using Slack in the back-end of Victim Conversation:-

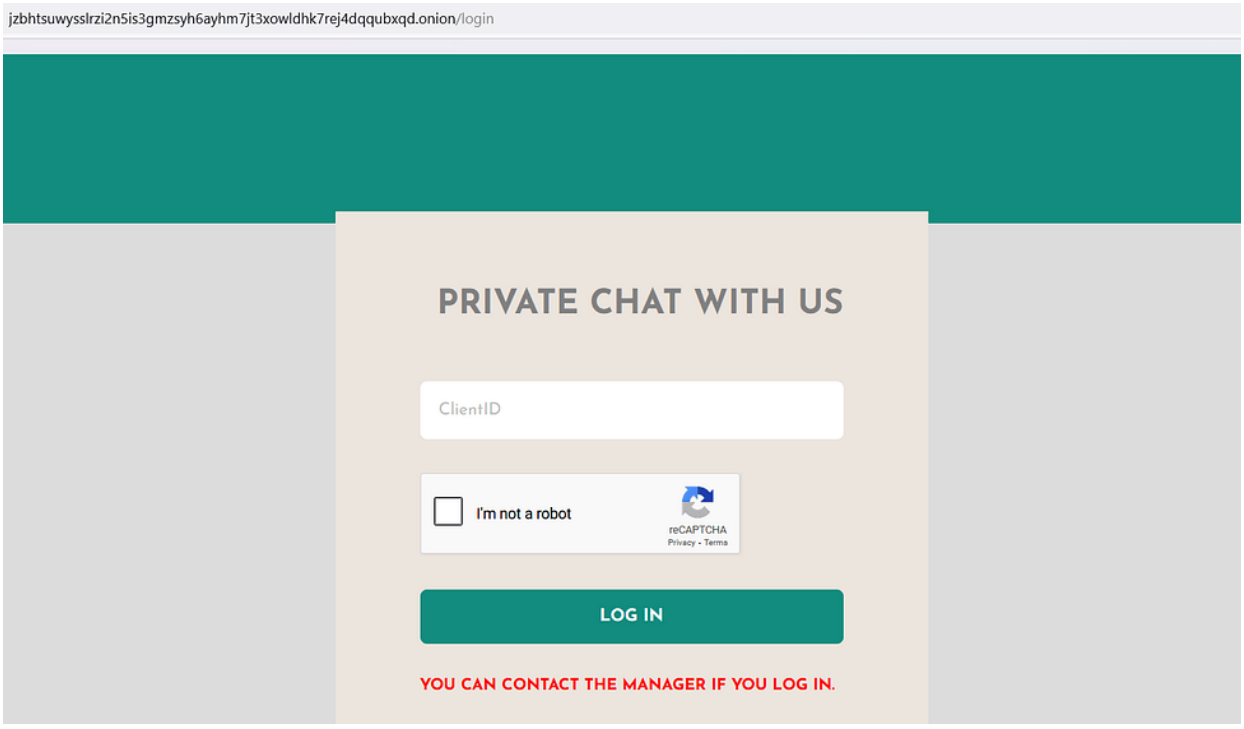
Chat Powered by Slack

UPDATE—1

In early **May 2025**, the group had introduced a new Onion Domain, which is dedicated to Clients with a new Client ID, unlike in former times.

On clicking "**Contact with ID**" it will navigate to the newer domain

jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd.onion



Client Login Panel of GUNRA Ransomware

Like the previously decommissioned domain, this domain's messaging queue was connected to another TOR Domain at the backend.

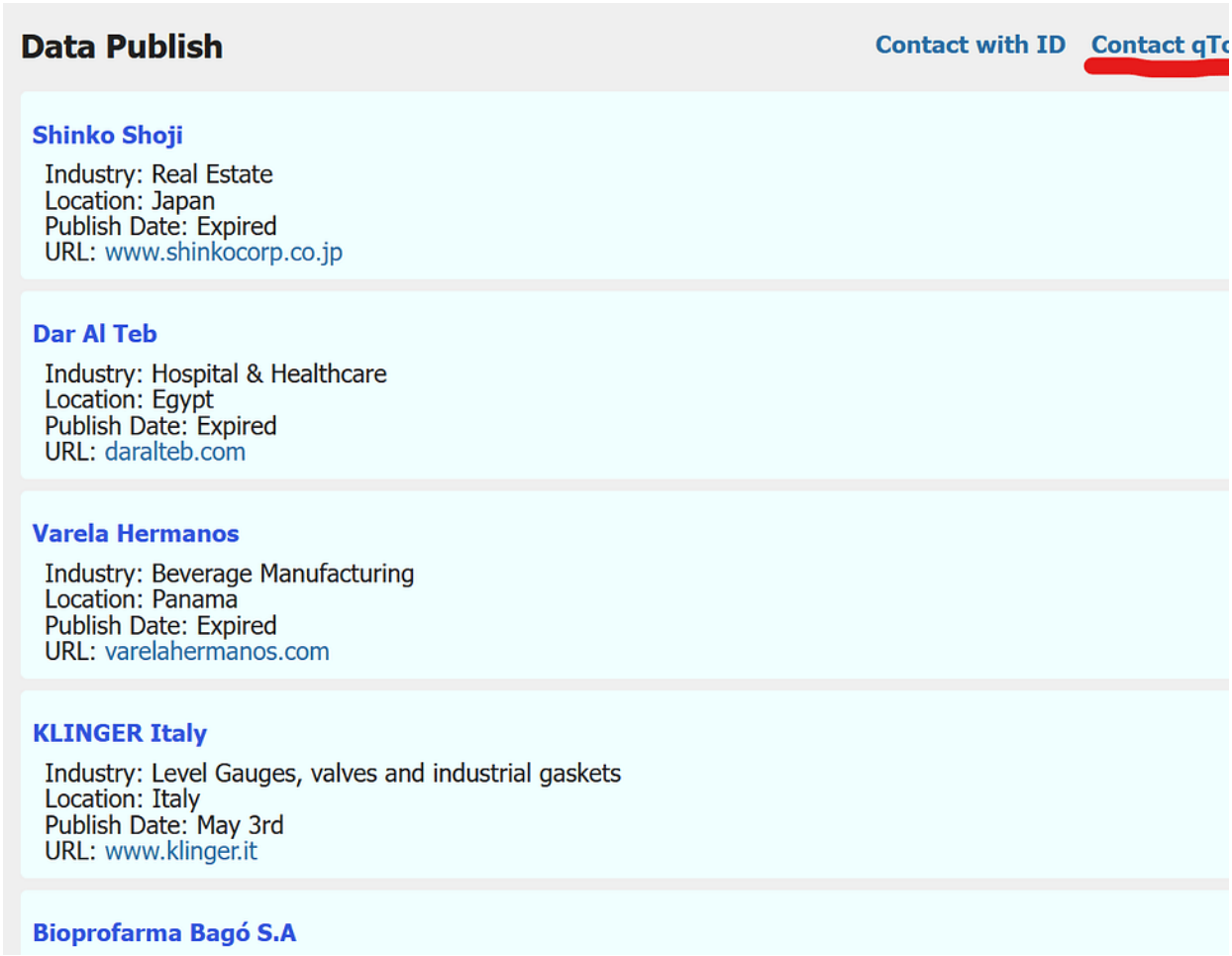
r3tkfu3h7sx4k6n7mr7ranuk5godwz7vlgvv2dk2fs2cbma5nailigad.onion

```
Negotiation Panel: jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd.onion
Negotiation Panel Backend:
r3tkfu3h7sx4k6n7mr7ranuk5godwz7vlgvv2dk2fs2cbma5nailigad.onion
```

The client negotiation panel was guarded using **ReCaptcha**, which takes a longer time to resolve the captchas to proceed with the Negotiation Access (esp. in TOR).

UPDATE—2

In mid May 2025, the group had decommissioned old Onion Domain **apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion** and added support of TOX.



DLS Updated with minor changes

UPDATE—3

In June 2025, the group launched their Data Leak Site on Clear Web with the following address:-

- **datapub.news**

This website is titled "**Public Data Share**" by Gunra Group and was registered on **7th June 2025**, hosted with **BlackHost**, resolving to **86.54.28.216** running on Ubuntu Server with nginx as Web Server using **PHP/8.4.5**. It is registered under **AS174 Cogent Communications**.

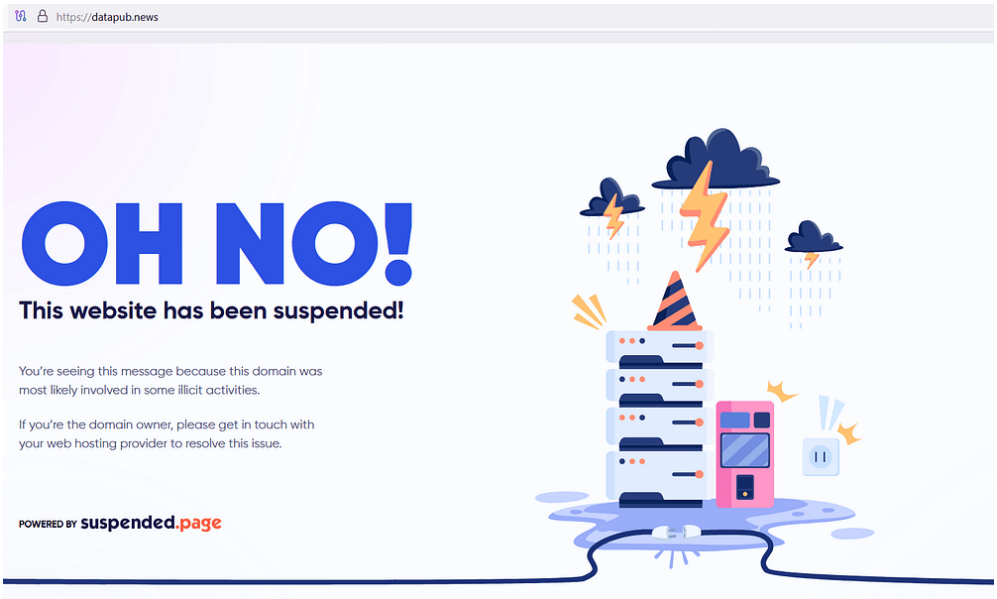
By visiting the website, we can deduce the following email address: **a00f105546345756@proton.me**

NOTE: The same host was facilitated various Phishing Incidents like **AppleJeus** from the **Lazarus Group** previously.

Now, we understand from the above data that GUNRA had undergone various revisions on their Data Leak Site to finally settle on the Dark-Themed DLS.

UPDATE—4

In August, the website was taken down and made offline, though the TOR website remains operational.

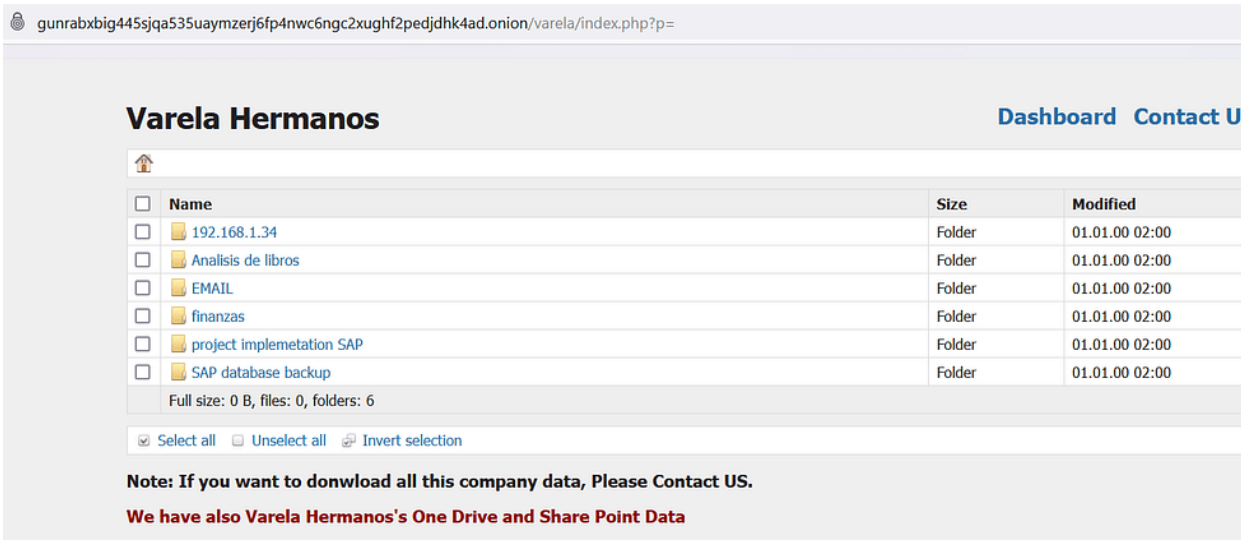


This underlines the fact that upon receiving a formal complaint, Black Host suspends the website, as they are not Bulletproof Service Providers.

UPDATE—5

On 27th April 2025, the leaks are published on the same server as the DLS is hosted.

Now, the negotiation portal had been removed, and the leaks are directly available, which indicates the group does not want any more negotiation for the listed victims.



Victim Leak listed

The entire leak is not available as they are selling it for the interested parties, which can be evident from the following line:-

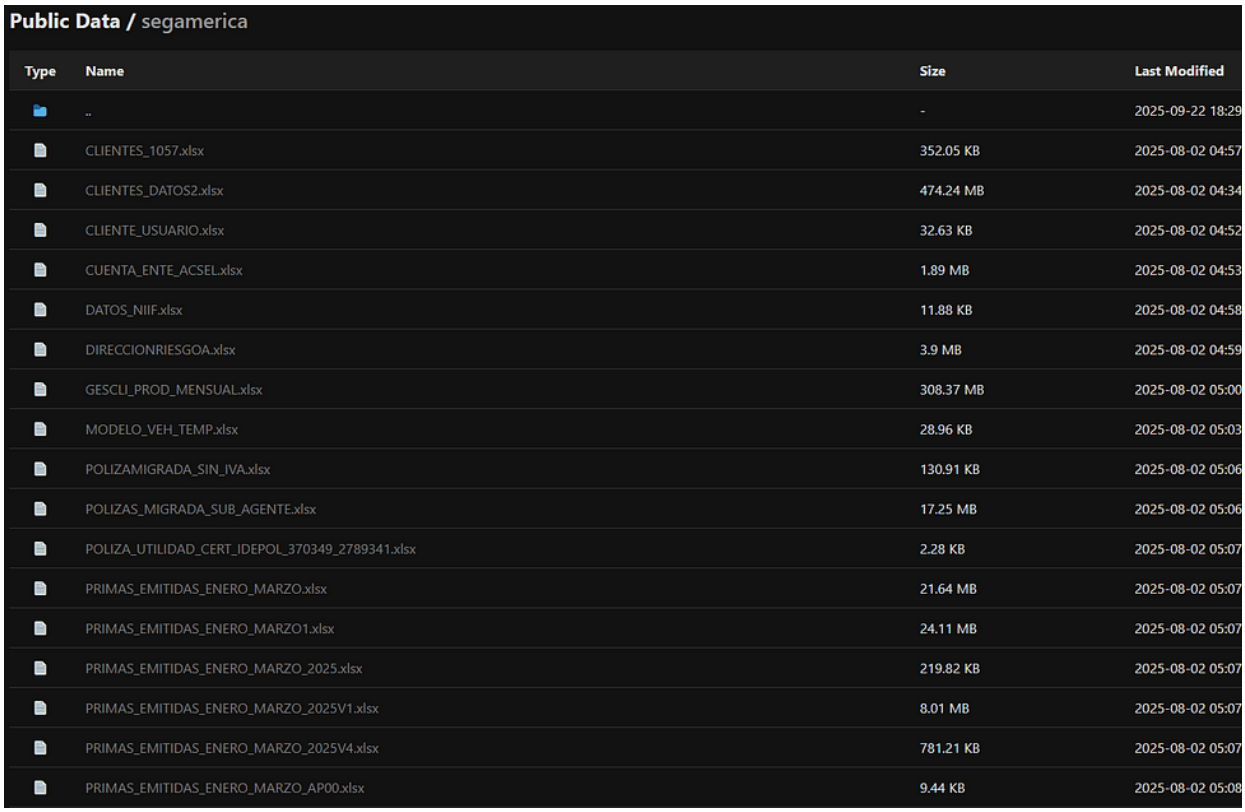
Note: If you want to donwload all this company data, Please Contact US.

There is a typo in the NOTE section, which indicates that the threat actor is a fast typist and ignores to check for typos before publishing the data.

The DLS was titled as "**Data Publish**" and later "**Public Data Share**".

Now, the negotiation portal is being linked to the "**Contact US**" page in the DLS.

Though the surface web went offline, the TOR Domain remains operational, and all the leaks are hosted within the same DLS.



Leaks are hosted within the same DLS

SAMPLE ANALYSIS INTEL

I have identified 6 Samples of Gunra Ransomware (in total as of now). It is found that the earliest sample is coded on **10th April 2025**. The latest sample is found to be compiled on **28th May 2025** (EXE) and 16th July 2025 (ELF).

Out of 6 samples, 2 are sized at 1.79 MB and rest are 195 KB, 121 KB, 421 KB.

All the samples are included at the end of this article under the IOC section.

A few artifacts found on the Sample Analysis are:-

- 📌 Gunra is a spin-off from Conti Ransomware, as the code-base is identical
- 📌 Read Me file titled: **R3ADM3.txt** which was previously used by Conti Group previously
- 📌 Upon infection, all the files are appending the extension ".ENCRT" after data encryption.
- 💡 Initial Access: Spear Phishing Document
- 💡 Traces of Akira Ransomware were also spotted
- 📌 Instructs to erase about (60+) Volume Shadow Copies
- 📌 Data Encryption: Salsa20, ChaCha
- 📌 Data Encoding: XOR, Base64
- 📌 Data Hashing: murmur2
- 📌 Mutex: kjsidugiaadf99439

💡Used this query for Shadow Deletion: (Process #59) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy WHERE ID='{8FD052FE-440B-4B35-B239-BD9DD042C664}'

💡The same above query used by LockBit 4.0, VanHelsing, Conti, Monti for Shadow Copy Deletion

💡Used Path: **D:\wrk\tool\encrypter\x64\Debug\encrypter.pdb**

📌All samples use Microsoft Visual C/C++ with Microsoft Linker

💡Linux Sample uses GCC (Debian 14.2.0–17), a recent compiler for Unix-based systems, specifically targeting 64-bit Linux environments, given the GCC 14.2.0 release date

💡ELF64 format for Unix/Linux, specifically AMD64–64 architecture, targeting modern Linux distributions (e.g., Debian, Ubuntu, or similar server OS)

💡2 Executables use LTCG (Link-Time Code Generation), suggesting optimization for performance

💡Console payload: Stripped for evasion (no embedded debug); higher MSVC++ probability suggests core encryption component

💡2 Executables are console-based and stripped to external PDB, suggesting optimized release builds for Windows (likely Windows 10/11 or Server editions)

💡Visual Studio (2019 or 2022) and MSVC++, with versions indicating C++ usage are used

Though the initial samples have a code-overlap with Akira and Conti, the newer versions of Gunra Ransomware is fresh and is not copied from any other known variants.

This is one such example:

MD5: 7dd26568049fac1b87f676ecfaac9ba0

DoNoT LOADER USAGE IN GUNRA RANSOMWARE

While analyzing the code, it is found that Gunra had used various loaders such as **Donot** Loader's routine embedded within the ransomware binary.

🔍 Key Indicators of Loader Behavior

Feature	Evidence	Description
Control Transfer	`jmp 0x127000`	Execution jumps to a new memory region, indicating unpacked or relocated code.
Stack Setup & Sanitization	`sub rsp, 0x218`, `rep stosd`	Prepares a clean stack frame and clears memory.
Obfuscation Reversal	`xor rax, rbp`	Likely reconstructs a pointer or function address.
Modular Calls	`call 0xafb03`, `call 0xb07ce`, etc.	Suggests API resolution, memory allocation, and payload staging.
Payload Metadata Setup	`mov qword ptr [rax + 0x18], rcx`	Prepares memory structures for payload execution.
Execution Transition	`jmp 0x127225`	Likely hands off control to the final payload.

Behavioral Flow

1. Execution jumps to a new memory region (`0x127000`).
2. Stack is initialized and memory is cleared.
3. Obfuscated values are decoded using XOR.
4. Internal functions are called to:

—Resolve APIs

—Allocate memory

—Possibly decrypt or decompress payload
—Inject or execute the final stage
5. Payload metadata is written to memory.
6. Execution transitions to the next stage via another jump.

Here you can use this YARA Rule to detect the same in the future:-

```
rule Embedded_Donot_Loader_Stub_Ransomware
{
    meta:
        author = "THERAVENFILE"
        description = "Detects embedded DONOT loader stub used in GUNRA ransomware"
        version = "1.0"
        date = "2025-07-07"
strings:
        $jmp_transfer = { FF 25 ?? ?? ?? ?? } // jmp to new region (e.g., jmp
0x127000)
        $stack_setup = { 48 81 EC 18 02 00 00 } // sub rsp, 0x218
        $stosd_loop  = { B9 4E 00 00 00 B8 CC CC CC CC F3 AB } // mov ecx + mov eax
+ rep stosd
        $xor_decode  = { 48 33 C5 } // xor rax, rbp
        $jmp_final   = { E9 ?? ?? ?? ?? } // jmp to final payload
    condition:
        all of them
}
```

NOTE: The above YARA Rule is created with Co-Pilot as per the fed Instruction Set. Hence, it may contain FPs. Use it by tweaking it as per your Malware Sample Analysis.

If you want to dig a deep-down into Linux Sample, you can find an analysis here by Trend Micro.

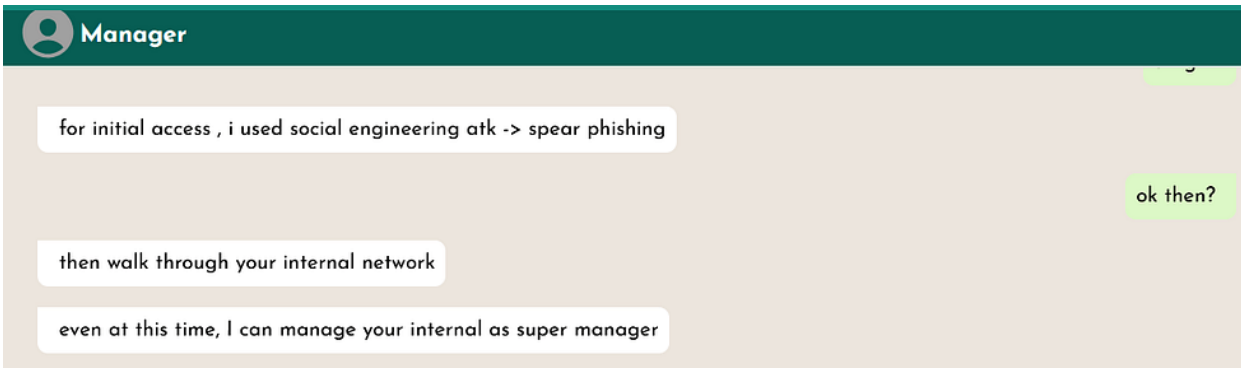
During analysis of GUNRA Samples, it is found that some of the samples are mis-tagged as Gunra. Remember the fact that the files with .ENCRT only belongs to Gunra or DLS. No other parameters stand as of now.

NEGOTIATION ANALYSIS

During Negotiation, the group demanded **13 BTC**, **$10M and $2M** from the victims. From a Colombian Victim, the group initially demanded **$20M** as ransom, which is unrealistic, but agreed to **$70K**.

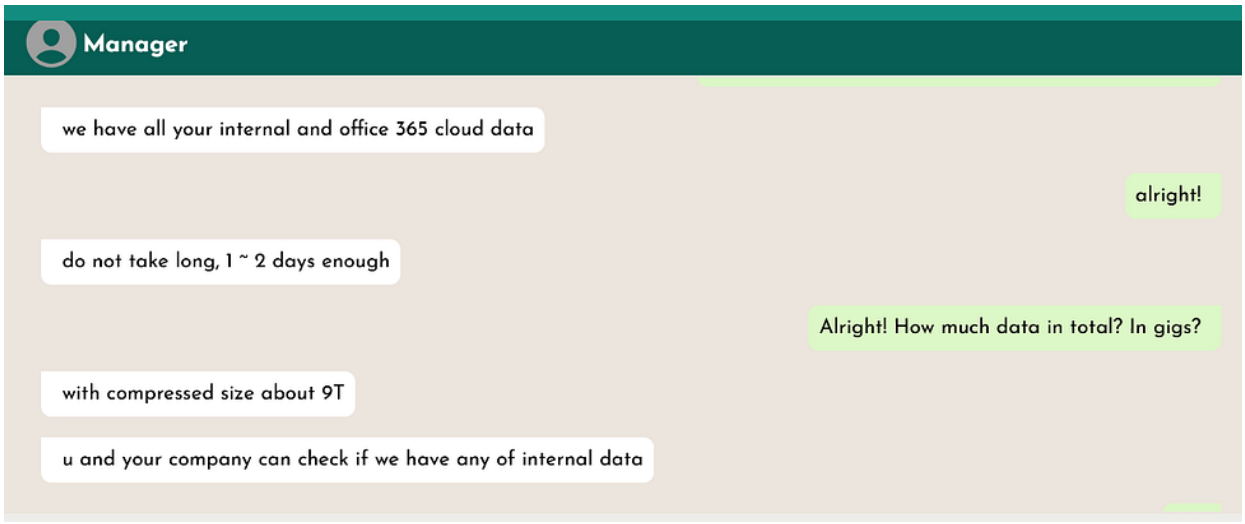
Unrealistic ransom demands mark it as immature operators. This points out the fact that the Threat Actors are over-ambitious.

Here are some of the screenshots with Gunra Group:-



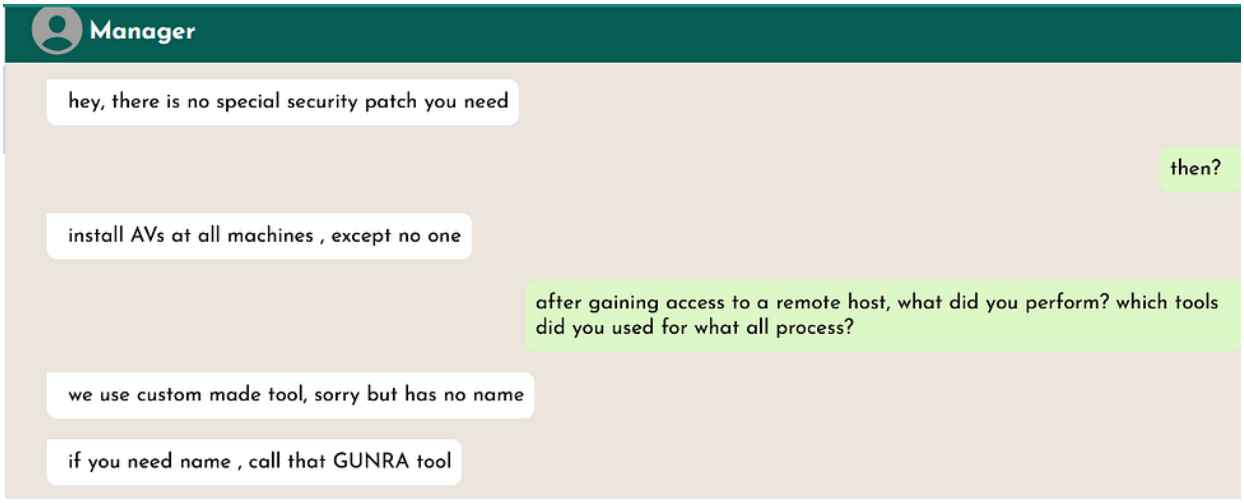
Gunra Ransomware Conversation: 1

After gaining access, the threat actor conducted Lateral Movement via a custom tool, which they call “GUNRA”.



Gunra Ransomware Conversation: 2

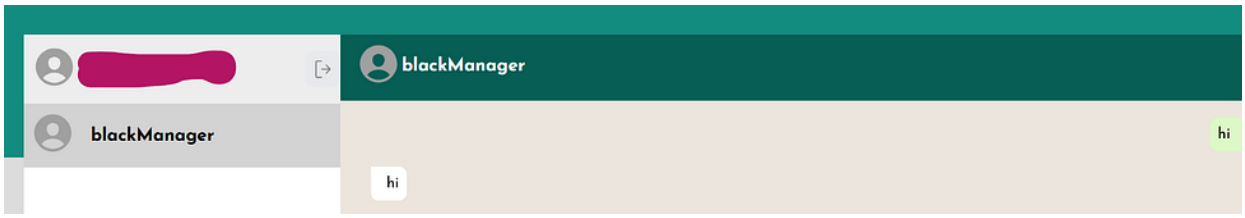
When asked about the patch…



Gunra Ransomware Conversation: 3

While investigating other victims, I came across other Chat Rooms in a new URL:-

jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd.onion



Gunra Ransomware Conversation: Victim 2

In this, the Post of "**Manager**" became "**Black Manager"** as we can see in the above screenshot.

For another client, the following is found:-

Gunra Ransomware Conversation: Victim 3

Here, the admin has been changed to "**redManager"**.

NOTE: This indicates there could be multiple parties assigned for each victim with different color codes.

This dedicated negotiation portal is guarded with Captcha, which is frustrating for the client to log in to their account, after atleast 10 tries of Captcha.

RANSOM NOTE ANALYSIS

Gunra Group drops its Ransom Note on Victim's machine with a filename titled as: **R3ADM3.txt** which was previously used by Conti Ransomware Group.

Here is the Ransom Note:-

YOUR ALL DATA HAVE BEEN ENCRYPTED
We have dumped your sensitive business data and then encrypted your side entire data.
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program, you must contact us.
We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free when you contact us.
You Only Have 5 Days To Contact Us
How to contact us
. Download "Tor Browser" and install it.
. In the "Tor Browser" open this site here :
http://apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion
. After signup and login to this site and contact Manger
You need to contact "Manager" to recover all your data successfully.
DANGER
O NOT MODIFY or try to RECOVER any files yourself.We WILL NOT be able to RESTORE them.
nd also we will publish your data on the dark web if there is no reply from you within 5 days.
Publish URL: http://gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad.onion/

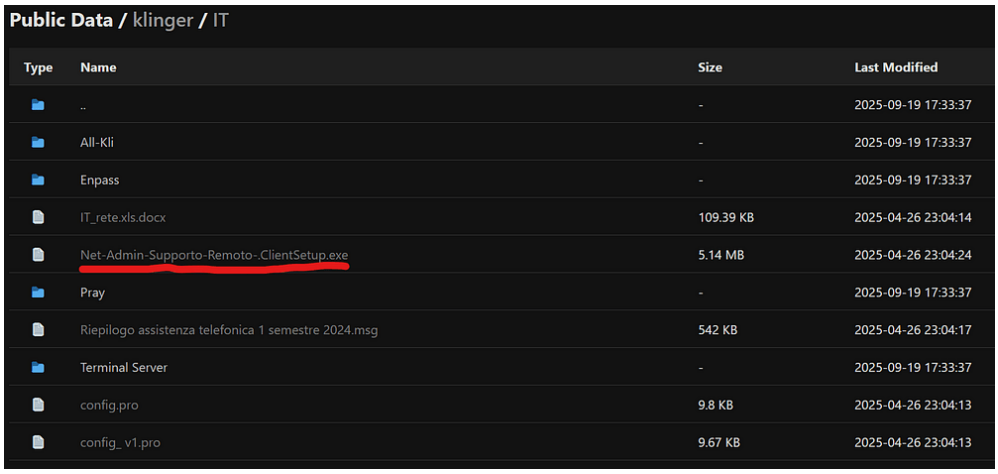
The Ransom note to a victim is also spotted in Spanish:-

```
TODOS SUS DATOS HAN SIDO ELIMINADOS PERMANENTEMENTE
Hemos eliminado todos los datos de su organizaci
n y realizado copias de seguridad.
nica forma de recuperar sus archivos es que nos los env
Para recibir los datos, debe contactarnos.
Le garantizamos que puede recuperar todos sus archivos de forma segura y sencilla. Pero no tiene tiempo suficiente.
Puede obtener algunos de sus archivos gratis si nos contacta.
Si no nos contacta, publicaremos sus datos gratuitamente.
mo contactarnos
1. Descargue e instale el navegador Tor.
2. En el navegador Tor, abra este sitio:
http://jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd.onion
3. Tras iniciar sesi
n con el ID de cliente que aparece a continuaci
n, contacte con el administrador.
ID de cliente: [redacted]
Debe contactar con el administrador para recuperar todos sus datos correctamente.
PELIGRO
No comparta su ID de cliente con terceros.
Usamos su ID de cliente como token de zona oculta para explorar sus datos y as
poder acceder a sus archivos.
Si comparte su ID de cliente con otros, ellos podr
n ver sus archivos.
Tambi
n puede obtener informaci
n sobre nosotros en esta URL.
Enlace de Onion: http://gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad.onion
Red despejada: https://www.datapub.news
```

From the ransom note, we can see the group had added a new Clearnet website called: **datapub.news**, which was registered on **7th June 2025**.

LEAK ANALYSIS: FOUND MALWARE AMONG VICTIM BREACH

While analyzing a leak, a remote connect tool caught my attention with the file name as: **Net-Admin-Supporto-Remoto-.ClientSetup.exe** (MD5: c07b712a984a506042ea2cf6e193f20c)



Public Data / klinger / IT

Type	Name	Size	Last Modified
	..	-	2025-09-19 17:33:37
	All-Kli	-	2025-09-19 17:33:37
	Enpass	-	2025-09-19 17:33:37
	IT_rete.xls.docx	109.39 KB	2025-04-26 23:04:14
	Net-Admin-Supporto-Remoto-.ClientSetup.exe	5.14 MB	2025-04-26 23:04:24
	Pray	-	2025-09-19 17:33:37
	Riepilogo assistenza telefonica 1 semestre 2024.msg	542 KB	2025-04-26 23:04:17
	Terminal Server	-	2025-09-19 17:33:37
	config.pro	9.8 KB	2025-04-26 23:04:13
	config_ v1.pro	9.67 KB	2025-04-26 23:04:13

Upon submitting the sample to VT, it gave 42 detections which is unusually high for a legitimate Remote Tool.

These are the detections spotted for this tool:-

```
W32.AIDetectMalware
Win/grayware_confidence_60% (D)
Trojan.Siggen21.26087
A Variant Of Win32/RemoteAdmin.ConnectWiseControl.E Potentially Unsafe
Trojan.Win32.MultiInjector.dd!s1
HackTool/ConnectWiseControl.e
PUA.ScreenConnect
Trojan.Agent.edgo
Unwanted-Program ( 005c6d501 )
Not-a-virus:HEUR:RemoteAdmin.Win32.ConnectWise.gen
Trojan.Malware.300983.susgen
Ti!64049E058F34
Static AI - Suspicious PE
BehavesLike.Win32.ConnectWise.tc
Pua:HackTool.Win32.Connectwise.16001881
PUP-IPR
W32/ConnectWise.B.gen!Eldorado
BScope.Riskware.ConnectWise
Riskware.RemoteAdmin!O4vT/8AeK2A
Tool.Convagent.Win32.869
```

> **NOTE**: *KLINGER Italy* is a leading manufacturer and marketer of Level Gauges, valves and industrial gaskets
>
> It is found that the sample is ConnectWise. Following, we will see how this piece is malicious

DETECTION NAME ANALYSIS: CONNECTWISE

```
Malware-Specific Detections
===========================
W32.AIDetectMalware
Trojan.Siggen21.26087
Trojan.Win32.MultiInjector.dd!s1
Trojan.Agent.edgo
Trojan.Malware.300983.susgen
Ti!64049E058F34
```

These labels from multiple vendors (e.g., BitDefender, DrWeb, Fortinet) point to trojan-like behavior, including payload injection and generic malware signatures. These are not typical of legitimate software.

```
HackTool and RemoteAdmin Flags
==============================
Static AI - Suspicious PE
BehavesLike.Win32.ConnectWise.tc
```

These suggest the file exhibits suspicious characteristics in its executable structure or runtime behavior, often associated with malicious modifications.

```
Potentially Unwanted Program (PUP/PUA)
======================================
PUA.ScreenConnect
Unwanted-Program (005c6d501)
PUP-IPR
```

These are less severe and could apply to legitimate remote access tools due to their potential for misuse. However, in the context of a leak and alongside Trojan detections, they add to the suspicion.

```
Grayware and Generic Detections
===============================
Win/grayware_confidence_60% (D)
W32/ConnectWise.B.gen!Eldorado
```

These indicate the file is flagged as potentially harmful software with moderate confidence, possibly due to obfuscation or behaviors not explicitly tied to a known malware family.

WHY IS THE UNITED STATES NOT ON THE VICTIM LIST 🇺🇸 ?

The group is either from the US or excludes the US from their Victim List. This is evident as most of their targets are from Asia and Europe.

There could be multiple reasons behind this decision. The group might be well-aware that infecting a US entity would face serious extradition issues in the long run, as long-forgotten Hack Groups/Cyber Crimes got busted from multiple locations in coordinated operations such as **EndGame, Talent, Phobos Aetor** etc. The group could be geo-located to the US currently, which creates a high alert to get noticed on their Radar.

By avoiding the US targets, the group might evade a quicker tailing by the FBI or CISA, as the home country is always quicker in action than a foreign law division, as tons of clearance have to be issued before making an extradition policy with the US before pressing the charges.

> **NOTE**: If they target a US entity in the near future, please excuse my above section as it will be nullified 🙂

MITRE ATT&CK TTPs

After analyzing GUNRA samples, the following techniques are found:-

```
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0008: Lateral Movement
TA0009: Collection
TA0010: Exfiltration
TA0011: Command and Control
TA0028: Persistence Mobile
TA0029: Privilege Escalation Mobile
TA0030: Defense Evasion Mobile
```

```
TA0031: Credential Access Mobile
TA0033: Lateral Movement
TA0034: Impact
TA0035: Collection
TA0036: Exfiltration
TA0037: Command and Control Mobile
TA0038: Network Effects
TA0039: Remote Service Effects
TA0040: Impact
TA0041: Execution
TA0042: Resource Development
TA0043: Reconnaissance
T1003: OS Credential Dumping
T1005: Data from Local System
T1014: Rootkit
T1055: Process Injection
T1090: Proxy
T1027: Obfuscated Files or Information
 T1027.002: Software Packing
 T1027.005: Indicator Removal from Tools
T1036: Masquerading
T1047: Windows Management Instrumentation
T1057: Process Discovery
T1063: Security Software Discovery
T1071: Applications Layer Protocol
T1081: Credentials in Files
T1082: System Information Discovery
T1083: File and Directory Discovery
T1119: Automated Collection
T1129: Shared Modules
T1143: Hidden Window
T1176: Software Extensions
T1185: Browsers Session Hijacking
T1486: Data Encrypted from Impact
T1490: Inhibit System Recovery
T1496: Resource Hijacking
T1518: Software Discovery
T1539: Steal Web Session Cookie
T1542: Pre-OS Boot
 T1542.003: Bootkit
T1552: Unsecured Credentials
 T1552.001: Credentials in Files
T1555: Credentials from Password Stores
 T1555.003: Credentials from Web Browsers
T1574: Hijack Execution Flow
 T1574.002: DLL Side-Loading
T1548: Abuse Elevation Control Mechanism
T1564: Hide Artifacts
 T1564.001: Hidden Files and Directories
```

IOC

```
TOR DOMAINS
===========
gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad.onion
apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion
jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd.onion
vrlgjxbl6yroq26xkcjpafgmmxrlpawvr4agppna6apfxjxav2mq66ad.onion
```

```
2bw7r32r5eshwk2h7uekj3lwzorxds2jyhyzqyilphid3r27x5hsf4yd.onion
r3tkfu3h7sx4k6n7mr7ranuk5godwz7vlgvv2dk2fs2cbma5nailigad.onion

MD5
===
9a7c0adedc4c68760e49274700218507
7dd26568049fac1b87f676ecfaac9ba0
ae6f61c0fc092233abf666643d88d0f3
f6664f4e77b7bcc59772cd359fdf271c
8d47d8a5d6e25c96c5e7c7505d430684
3178501218c7edaef82b73ae83cb4d91
94b68826818ffe8ceb88884d644ad4fc
4c0e74e9f94dff611226cd1619cb1e1d

URLs
=====
https://bashupload.com/0OoOe/tool.7z
https://bashupload.com/FOIGR/email.7z
https://datapub.news

Mail
====
ilovemycubscout@gmail.com
a00f105546345756@proton.me

IP: 86.54.28.216

TOX ID
2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22
```

Follow me on Twitter for interesting DarkWeb/InfoSec Short findings!

NOTE: The article is purely Individual Research and is only associated with THE RAVEN FILE and is not subjected to be used/published anywhere without the Author's consent.