Cyble - Deep Dive Into Ragnar_locker Ransomware Gang

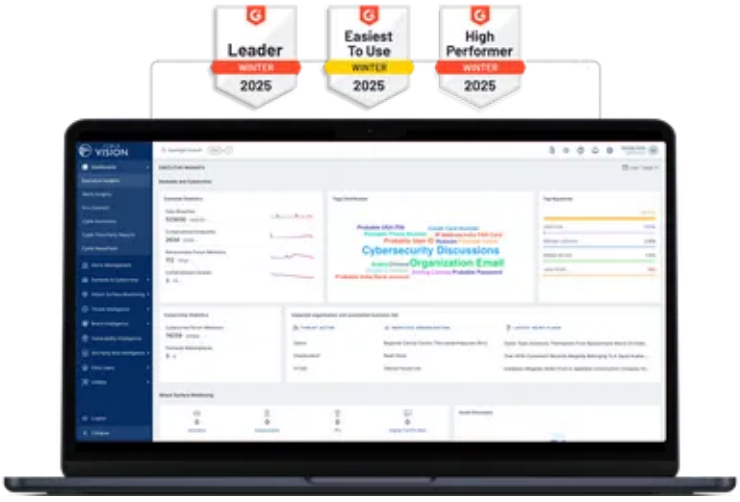
Published: 2022-01-20 · Archived: 2026-04-05 12:45:05 UTC

Ragnar_locker ransomware targets multiple high-profile Windows platforms using the double extortion technique.

Organizations worldwide face a multi-pronged threat from Ransomware groups at a greater frequency than recorded before. As the organizations' primary danger remains losing access to their systems and data, the threat of Ransomware groups leaking the data if their ransom requests are not met or the victim reaches out to law enforcement authorities has been raising more concern.

Cyble Research Labs has analyzed and published information about the most prominent and active ransomware groups in the past and provided recommendations to prevent such incidents. This blog is a deep dive into one of the most active Ransomware groups, Ragnar_Locker, how they operate, their capabilities, and how to secure yourself/your organization from them.

Ragnar_locker ransomware was first observed in late 2019, targeting multiple high-profile targets on Windows platforms. Ragnar_locker also uses the double extortion technique for financial gain like most notorious ransomware gangs.



This group targets several countries worldwide, as shown in the figure below.

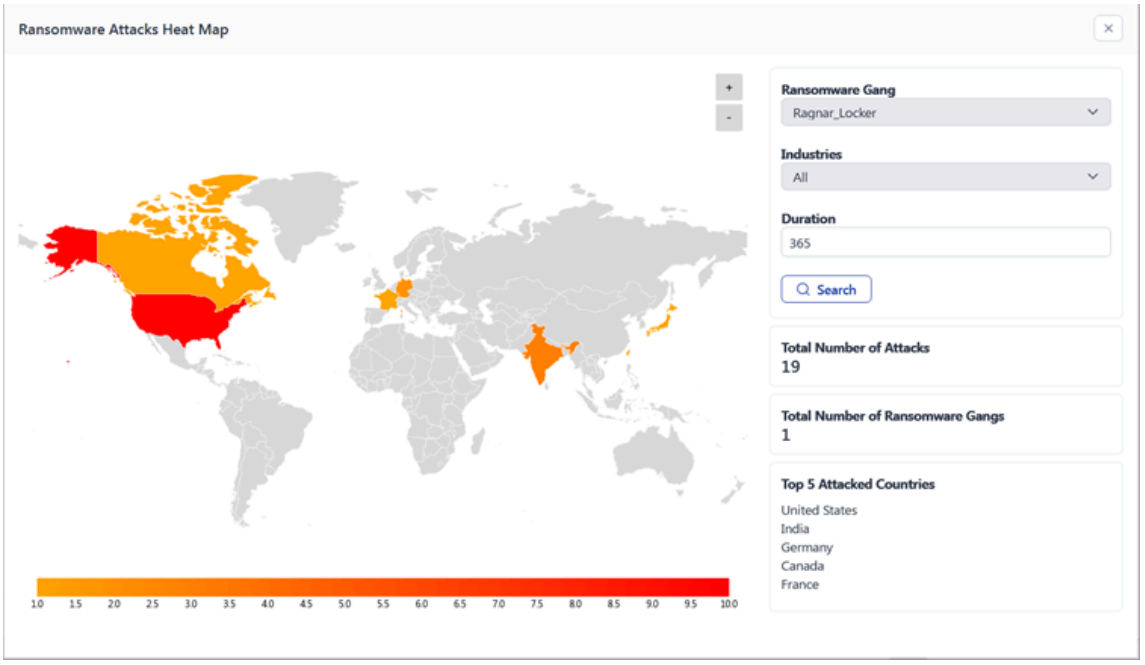


Figure 1 Ragnar_locker Ransomware Victim Details

Technical Analysis

Based on static analysis, we found that the malicious file is a 32-bit Graphical User Interface (GUI) based binary, as shown in Figure 2.

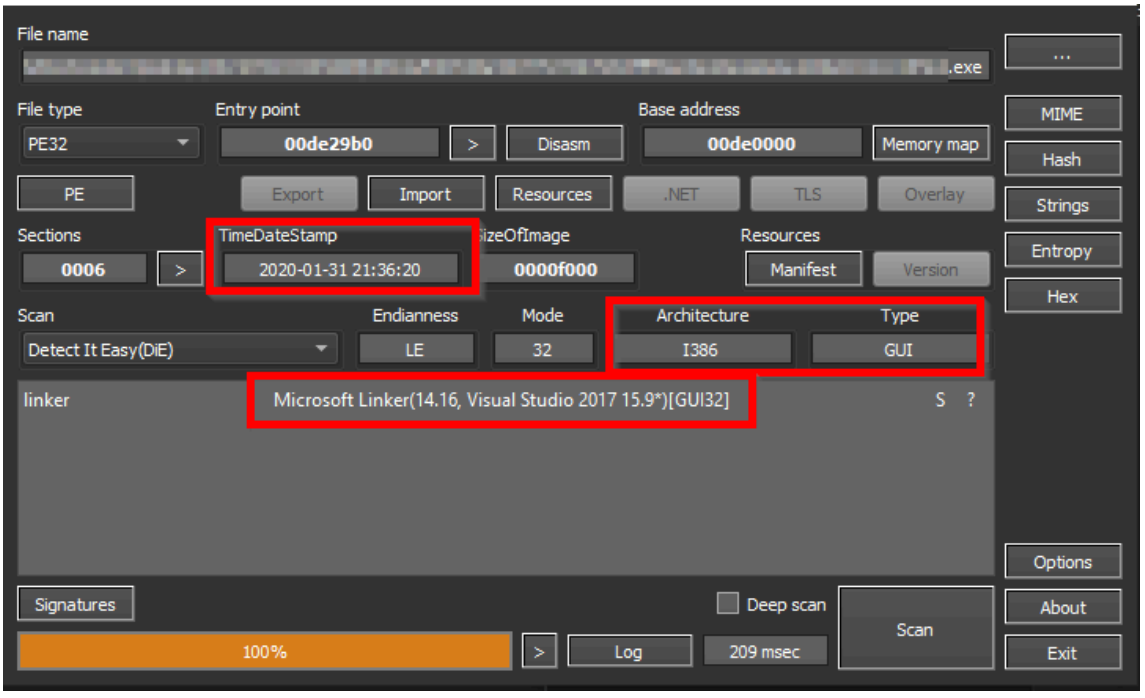


Figure 2 Static File Details of Ragnar_locker Ransomware

After execution, Ragnar Ransomware initially searches for system details using *GetLocalInfoW() API*, which extracts the system's default language. After identifying the system language, it compares this with a hardcoded list of languages present in the Ransomware binary, as shown in the figure below.

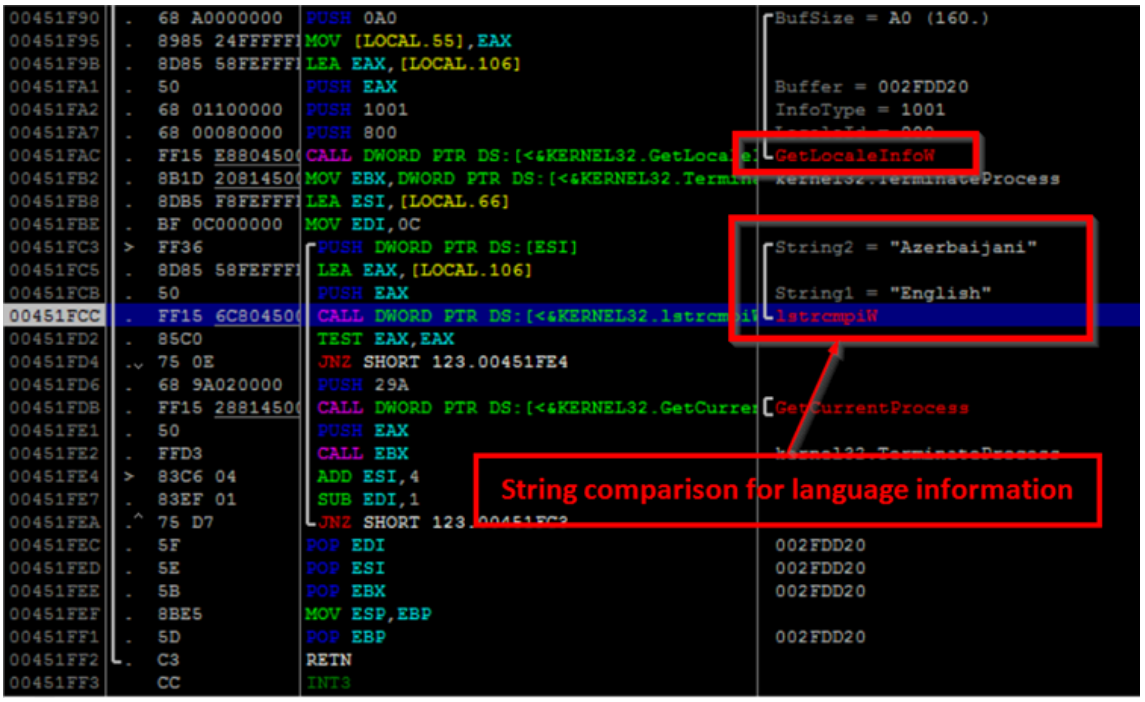


Figure 3 Ragnar_locker Ransomware Language Check

If the identified system language is present in the hardcoded list, the Ransomware terminates its execution using the*TerminateProcess()* API.

The languages hardcoded into the Ransomware are Belorussian, Azerbaijani, Ukrainian, and other languages commonly spoken in the former Soviet Union (USSR).

Ragar Ransomware then looks for other system information using APIs to retrieve the victim's system name, username, GUID, and product name.

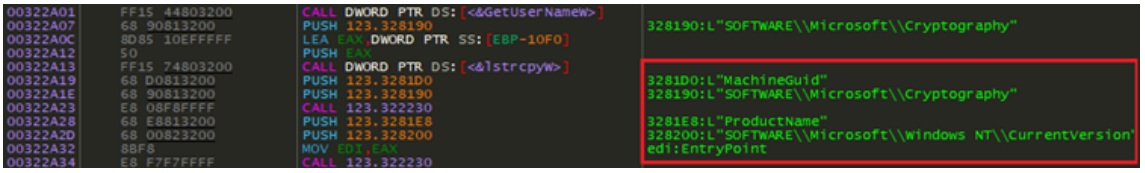


Figure 4 Ragnar_locker Ransomware Enumerating System Information

The Ransomware collects the above system information and calculates its size. This information and size are then fed to a custom logic to generate a unique hash to create an event in the system using *CreateEventW()* API, as shown in Figure 5.

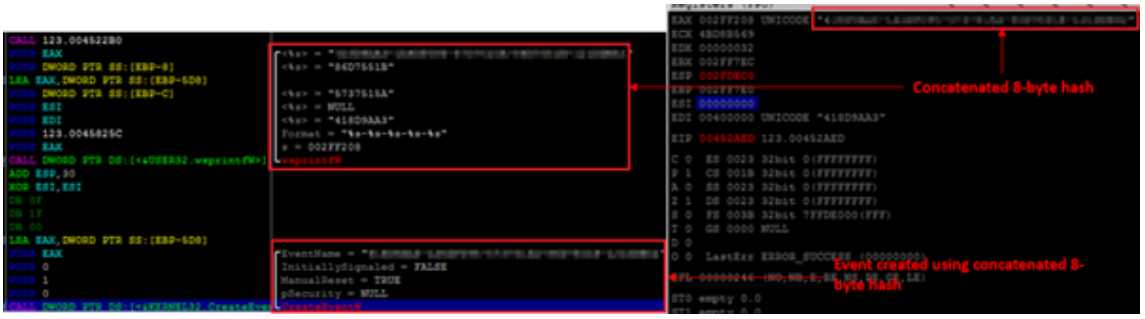


Figure 5 Ragnar_locker Ransomware Creating Event

This malware then enumerates all the physical drives in the system. Ragnar Ransomware uses *CreateFileW()* API function to check which physical drives are accessible by the system. The malware then executes a loop that runs sixteen times to get all the accessible physical drives.

Figure 6 shows the enumeration of \\\\.*PHYSICALDRIVE*.

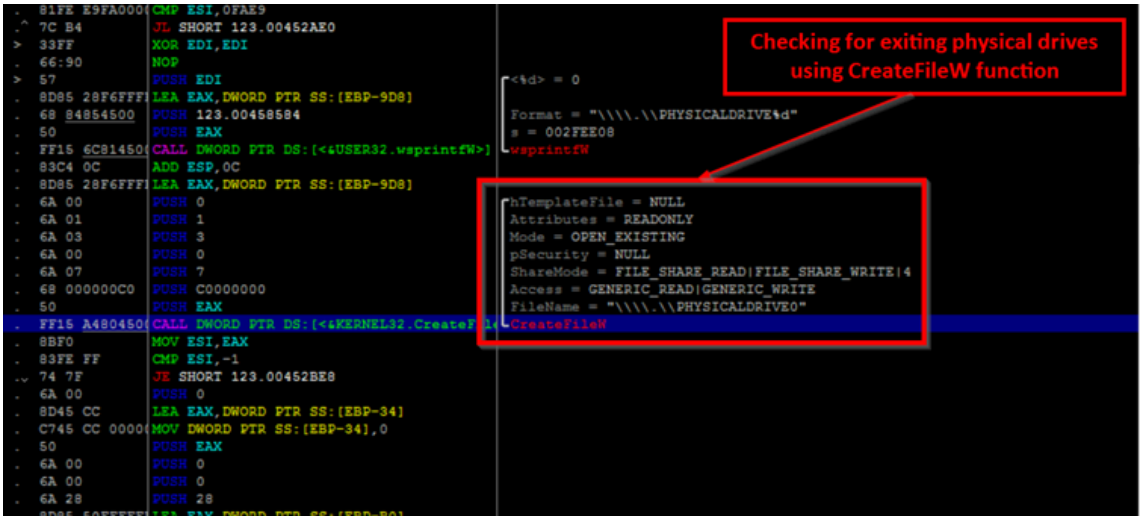


Figure 6 Ragnar_locker Ransomware Checking for Physical Drives

After checking the physical drives, the Ransomware extracts all the system volume names using *GetLogicalDrives()* API, as shown in the figure below.

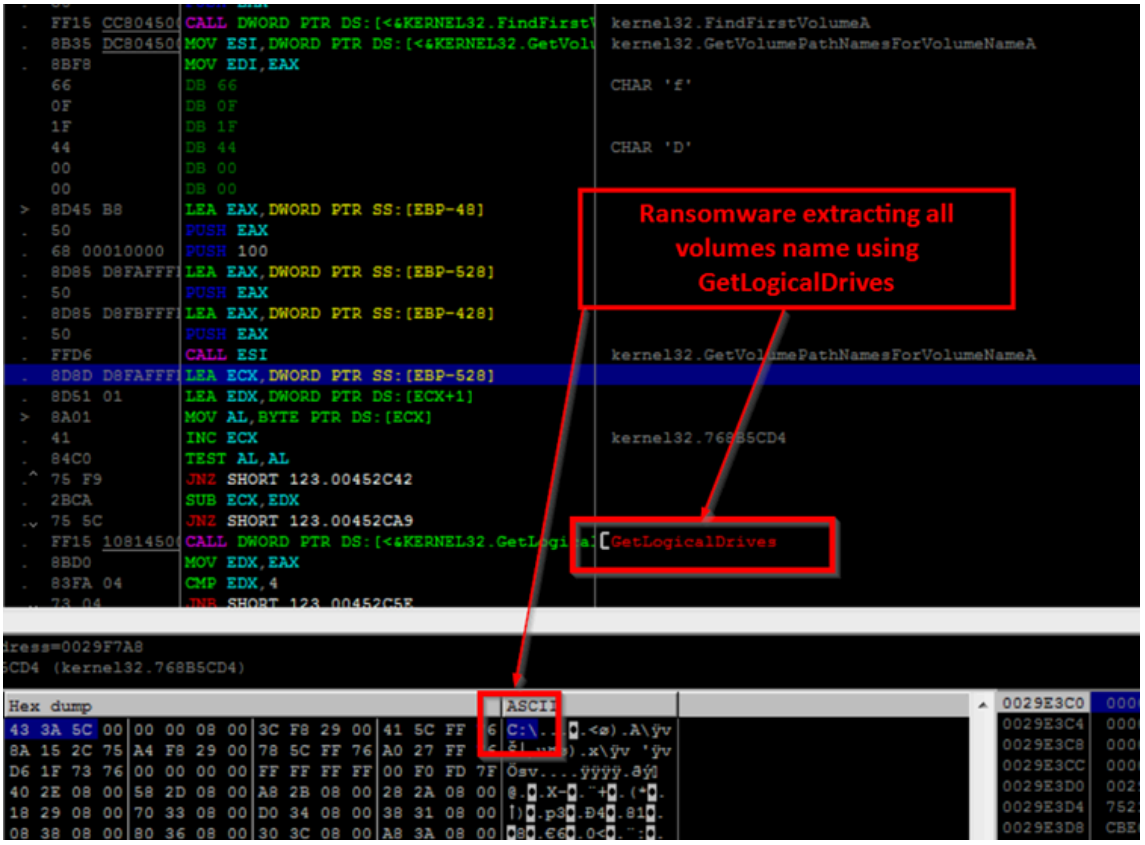


Figure 7 Ragnar_locker Ransomware Enumerating Hard Drive Volumes

After retrieving the volume names, the Ransomware then calls *GetVolumeInformationA()* API to get the details of the volume.

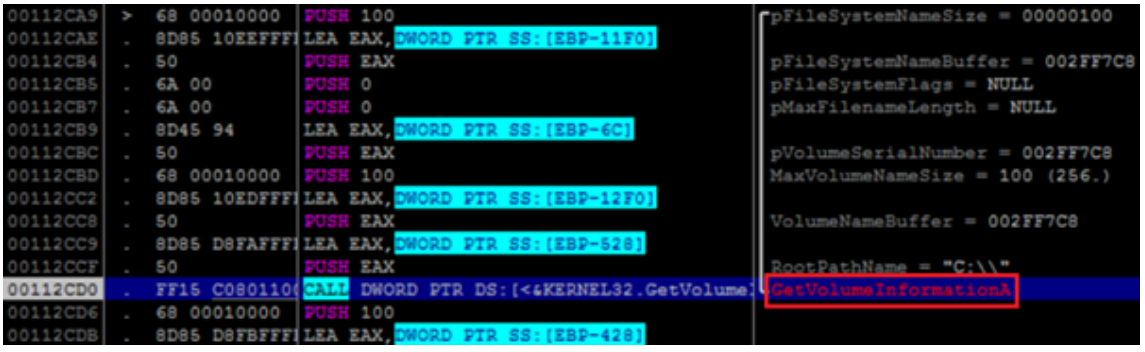


Figure 8 Retrieves Volume Details

The malware now prepares the key required to encrypt the files in the latter part of its execution. The malware uses cryptographic APIs such as *CryptAcquireContextW()* , *CryptGenRandom()* and *CryptReleaseContext()* to generate random keys.

Then, the malware uses a custom decryption logic which decrypts the strings that have information about the name of the services. After identifying the names of the services, the Ransomware checks for their presence and terminates them if the services are actively running on the victim's machine. Some of these services include VSS, SQL, Memtas, etc.

To identify the services running in the machine, the Ransomware first calls *OpenSCManagerA()* API, which establishes a connection to the service control manager that gives the TA access to the service control manager database.

Upon gaining access to this database, the following APIs() will be called:

- *OpenServiceA()* – Opens the specified service.
- *QueryServiceStatusEx()* – Gets the status of the service.
- *EnumDependentServiceA()* – Retrieves the dependent services.
- *ControlService()* – takes control of the service for stopping.

If *OpenSCManagerA()* API fails to get the handle to Service Control Manager (SCM), then the Ransomware skips calling the above service-related APIs.

The Ransomware then proceeds to execute *CreateProcessW()* API to call wmi/vssadmin to delete any shadow copies in the system. After this, the Ransomware decrypts the RSA public key, encrypting the randomly generated key, as shown in Figure 9.

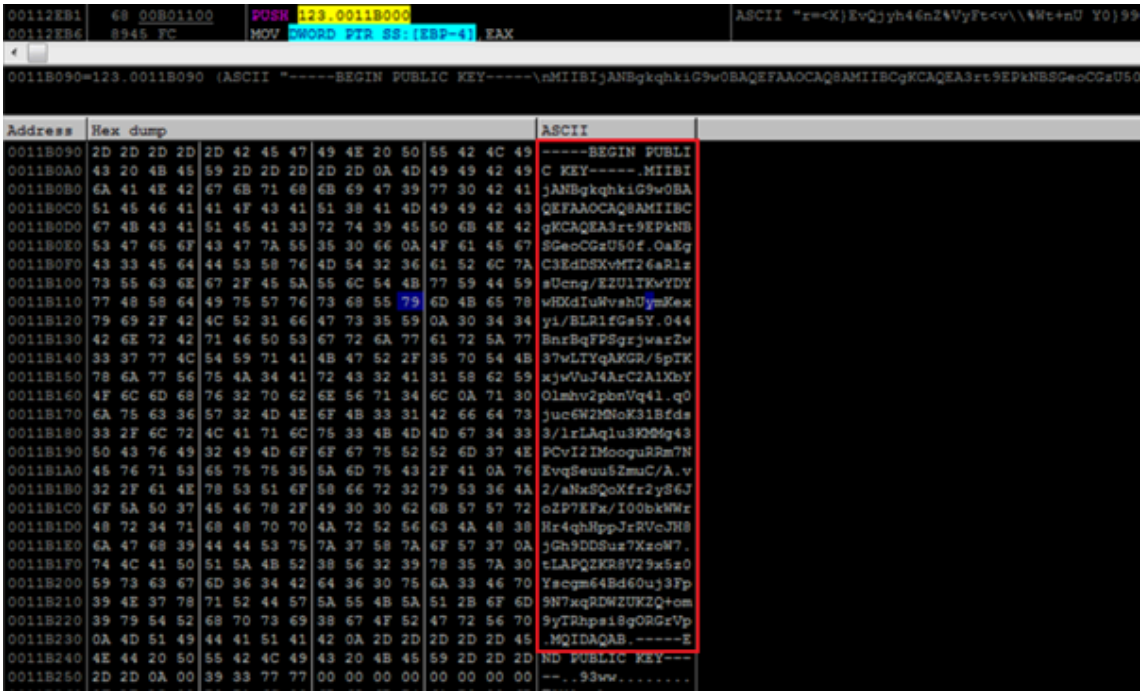


Figure 9 RSA Public Key

The Ransomware decrypts the ransom notes in the memory, shown to the victims after file encryption on their system. Then, it gets the device name and creates a unique hash used to generate the ransom note name in the below format.

- RGNR_[Unique-hash].txt

It calls *SHGetSpecialFolderPathW ()* API, gets the path of the Public folder (c:\user\public\Documents), and creates ransom notes in it. The ransom note content is then written using *WriteFile() API*.

The Ransomware then searches for files in the Windows directory for encryption using the *FindFirstFileW()* and *FindNextFileW()* APIs.

Before initiating encryption, the ransomware checks and excludes specific folders from encryption – such as Windows, Tor Browser, Google, Opera.

The Ransomware also excludes certain files from encryption such as RGNR_[unique_hash].txt, autorun.inf, boot.ini, amongst others.

Specific extensions are also exempted from encryption – such as .db, .sys, .dll.

The Ransomware specifically excludes these files, folders, and extensions to ensure that TAs are not damaging any system-critical files. Victims will thus have access to the affected device to pay the ransom after successful encryption.

Finally, the Ransomware encrypts the file using the salsa20 algorithm and displays a ransom note on the victims' machine. As shown in the figure below, the encrypted files will have appended extension ragnar_[unique_hash] in the victims' device.

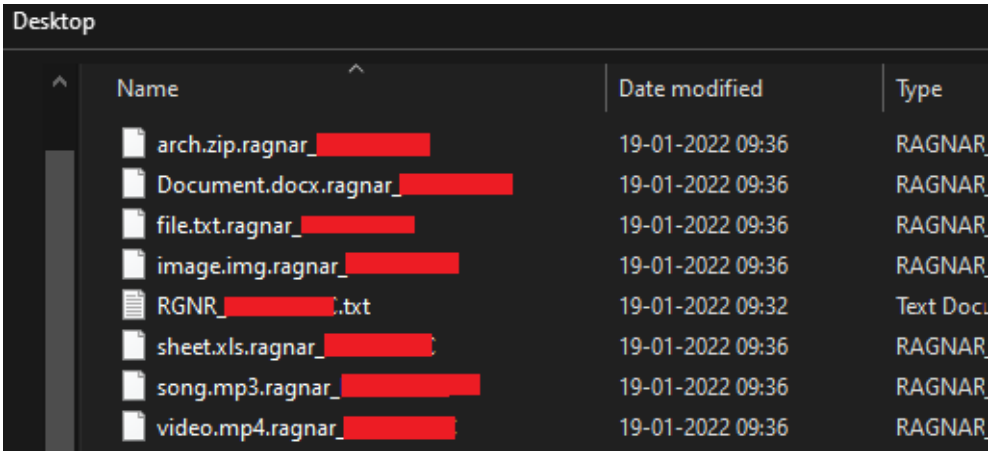


Figure 10 Encrypted Files on the Machine

In their ransom note below, the TAs have instructed victims to contact them via qTox and have also given an Email ID: *cargowelcome@protonmail[.]com* in case the victim cannot contact them through qTox to pay the ransom of 25 Bitcoin (BTC) for the decryption key.

Figure 11 Ransom note

Other Observations

Cyble Research Labs had found that the TAs leaked their victim's details on their leak website when victims did not pay the ransom. The following figure showcases the Ragnar_locker's leak website with recent victims.

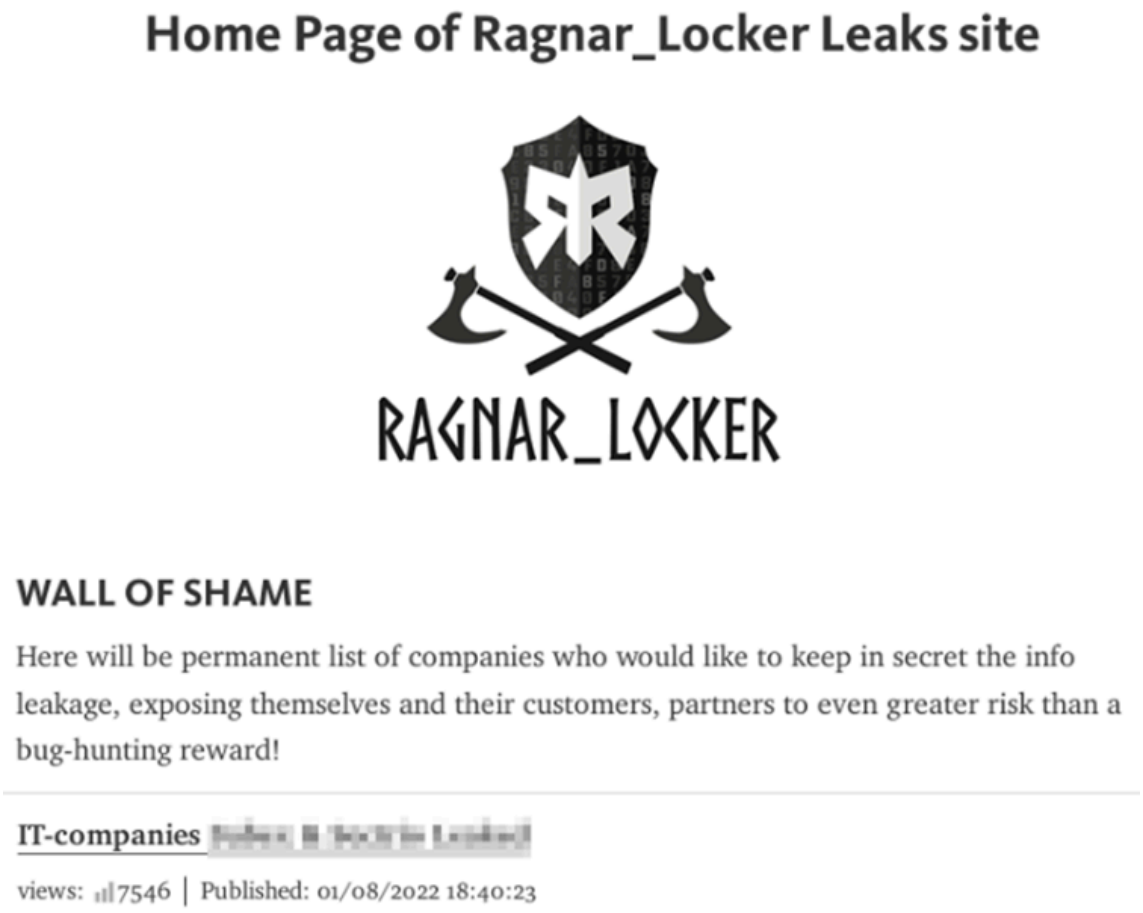


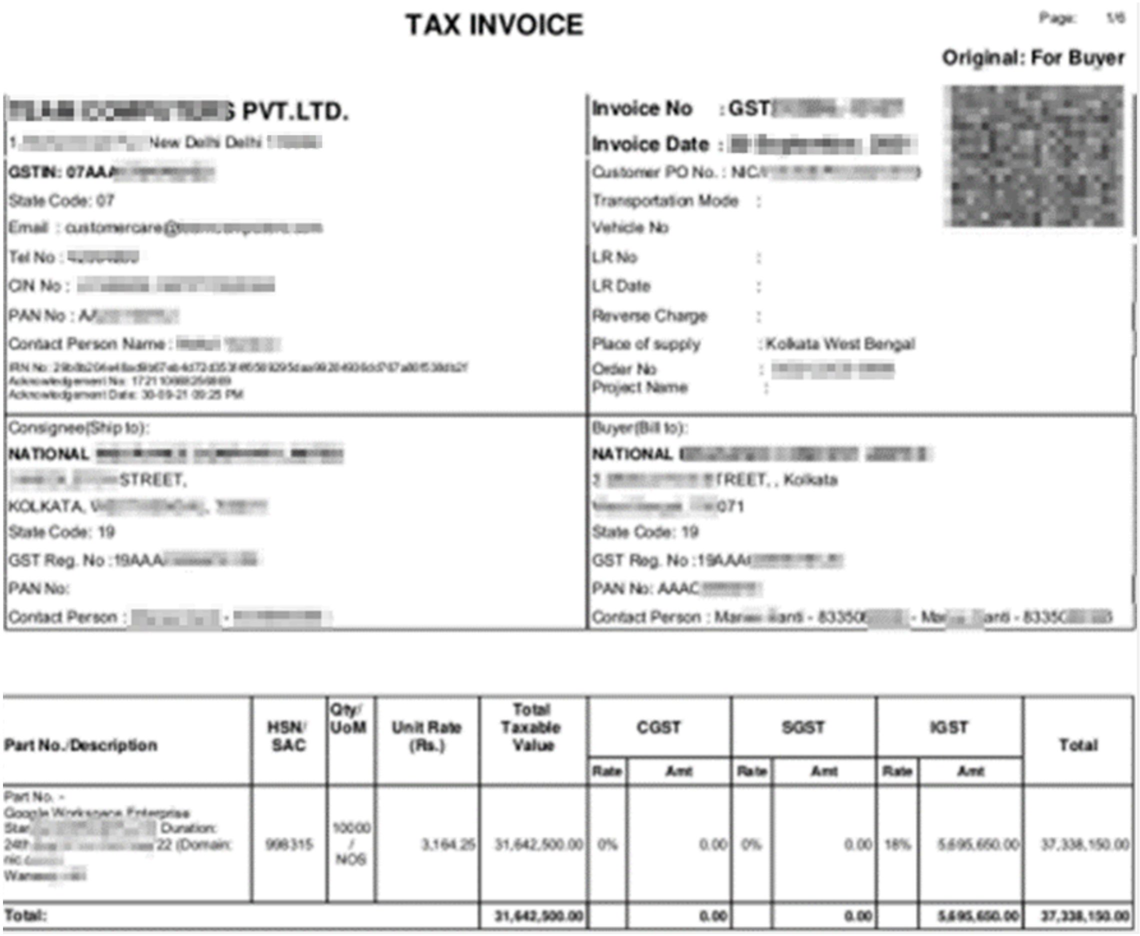
Figure 12 Victims Mentioned on Leak Site

As per their leak site, the Ragnar_locker ransomware group claims to be a team of cyber security enthusiasts working to make a profit.

The group alleges that their primary motivation to attack organizations is to help them improve their security measures. In addition, they want companies to take responsibility for securely storing the personal data of their clients and partners.

In one case, it was observed that the TAs had stolen the data of a victim's machine and shared the same on their leak site. The stolen data claimed by the TAs include name, PAN Number, mobile numbers, GST numbers, etc.

The victim's data posted on the TAs leak site is shown in the figure below.



TAX INVOICE

Page: 1/6

Original: For Buyer

[illegible] PVT.LTD.
1.[illegible] New Delhi Delhi [illegible]
GSTIN: 07AAA[illegible]
State Code: 07
Email : customercare@[illegible]
Tel No : [illegible]
CIN No : [illegible]
PAN No : AA[illegible]
Contact Person Name : [illegible]
IRN No: [illegible]
Acknowledgement No: [illegible]
Acknowledgement Date: 30-09-21 09:25 PM

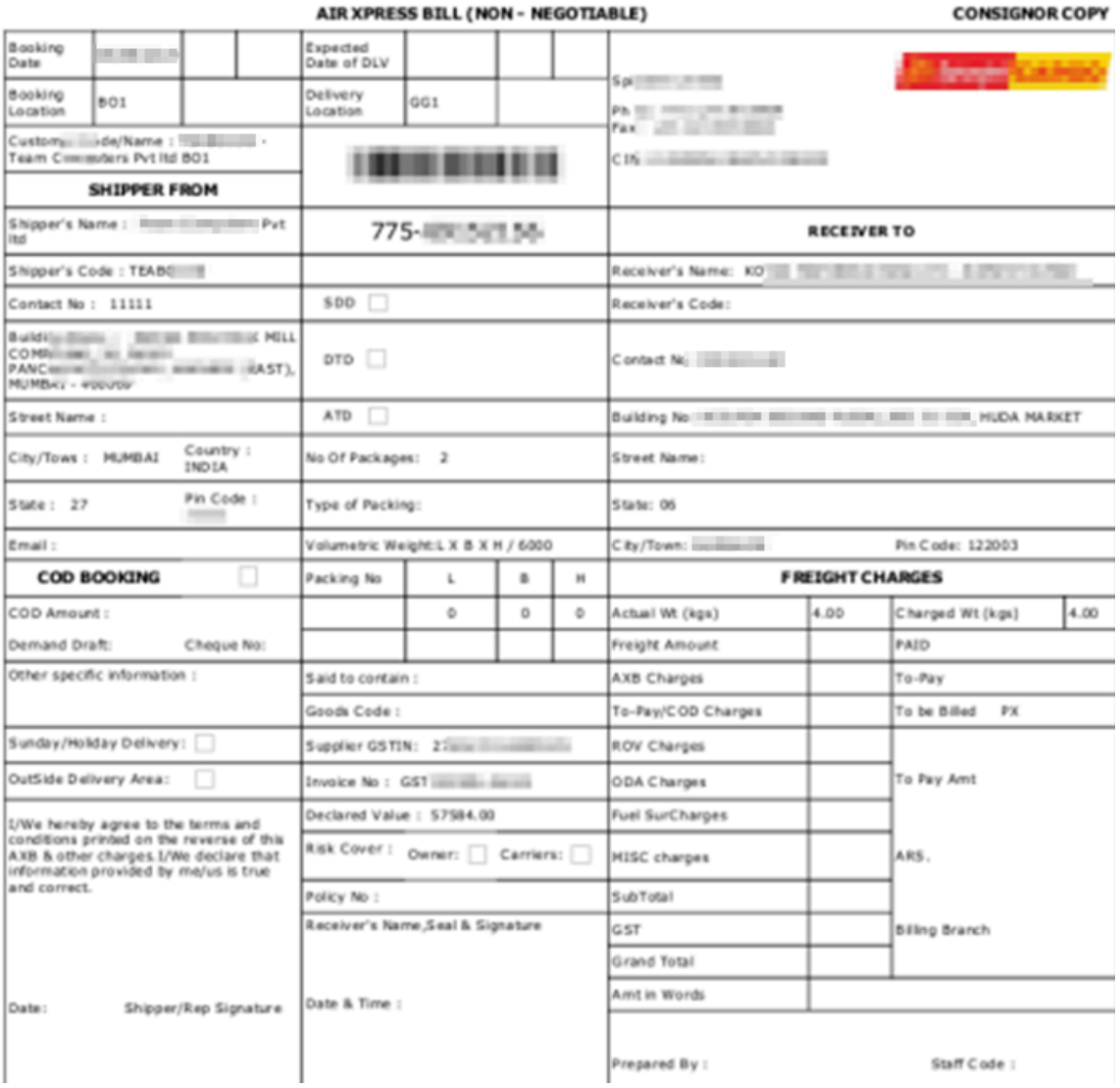
Invoice No : GST[illegible]
Invoice Date : [illegible]
Customer PO No. : NIC/[illegible]
Transportation Mode :
Vehicle No
LR No :
LR Date :
Reverse Charge :
Place of supply : Kolkata West Bengal
Order No : [illegible]
Project Name :

Consignee(Ship to):
NATIONAL [illegible]
[illegible] STREET,
KOLKATA, [illegible]
State Code: 19
GST Reg. No :19AAA[illegible]
PAN No:
Contact Person : [illegible] - [illegible]

Buyer(Bill to):
NATIONAL [illegible]
[illegible] STREET, , Kolkata
[illegible] 071
State Code: 19
GST Reg. No :19AAA[illegible]
PAN No: AAAC[illegible]
Contact Person : Mar[illegible]anti - 83350[illegible] - Ma[illegible]anti - 8335C[illegible]

Part No./Description	HSN/ SAC	Qty/ UoM	Unit Rate (Rs.)	Total Taxable Value	CGST		SGST		IGST		Total
					Rate	Amt	Rate	Amt	Rate	Amt	
Part No. - Google Workspace Enterprise Star[illegible] Duration: 24th[illegible]22 (Domain: nic.[illegible] Wares[illegible]	998315	10000 / NOS	3,164.25	31,642,500.00	0%	0.00	0%	0.00	18%	5,695,650.00	37,338,150.00
Total:				31,642,500.00		0.00		0.00		5,695,650.00	37,338,150.00

Figure 13 Tax Invoice



AIR XPRESS BILL (NON - NEGOTIABLE) CONSIGNOR COPY

Booking Date			Expected Date of DLV						
Booking Location	BO1		Delivery Location	GG1					
Custom ode/Name : Team Couriers Pvt ltd BO1									
SHIPPER FROM									
Shipper's Name : Pvt ltd			775-				RECEIVER TO		
Shipper's Code : TEABO							Receiver's Name: KO		
Contact No : 11111			SDD				Receiver's Code:		
Build MILL COMP PANC (EAST), MUMBAI -			DTD				Contact No		
Street Name :			ATD				Building No HUDA MARKET		
City/Town : MUMBAI	Country : INDIA		No Of Packages: 2				Street Name:		
State : 27	Pin Code :		Type of Packing:				State: 06		
Email :			Volumetric Weight:L X B X H / 6000				City/Town:	Pin Code: 122003	
COD BOOKING			Packing No	L	B	H	FREIGHT CHARGES		
COD Amount :				0	0	0	Actual Wt (kgs)	4.00	Charged Wt (kgs) 4.00
Demand Draft:	Cheque No:						Freight Amount		PAID
Other specific information :			Said to contain :				AXB Charges		To-Pay
			Goods Code :				To-Pay/COD Charges		To be Billed PX
Sunday/Holiday Delivery:			Supplier GSTIN: 2				ROV Charges		
OutSide Delivery Area:			Invoice No : GST				ODA Charges		To Pay Amt
I/We hereby agree to the terms and conditions printed on the reverse of this AXB & other charges.I/We declare that information provided by me/us is true and correct.			Declared Value : 57584.00				Fuel SurCharges		
			Risk Cover : Owner: Carriers:				MISC charges		ARS.
			Policy No :				SubTotal		
			Receiver's Name,Seal & Signature				GST		Billing Branch
							Grand Total		
Date: Shipper/Rep Signature			Date & Time :				Amt in Words		
							Prepared By :		Staff Code :

Figure 14 Airways Bill

Conclusion

There are likely multiple variants of Ragnar_locker ransomware active in the wild. In addition, TAs keep improving their code with new features to evolve their Ransomware-as-a-Service (RaaS) business model with new Tactics, Techniques, and Procedures (TTPs) to target devices. Based on these observations, we can safely assume that there may be further enhancements in upcoming variants of Ragnar_locker.

We continuously monitor Ragnar_locker's extortion campaigns and update our readers with the latest information.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety measures needed to prevent ransomware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.

- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users should take the following steps after the ransomware attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts and cruciality Of Ragnar_locker Ransomware

- Loss of Valuable data.
- Loss of organization's reliability or integrity.
- Loss of organization's businesses information.
- Disruption in organization operation.
- Economic loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1078	– Valid Accounts
Execution	T1059	– Command and Scripting Interpreter
Privilege Escalation	T1548 T1134	– Abuse Elevation Control Mechanism – Access Token Manipulation
Defense Evasion	T1112 T1027 T1562.001	– Modify Registry – Obfuscated Files or Information – Impair Defenses: Disable or Modify Tools
Discovery	T1082 T1083 T1135	– System Information Discovery – File and Directory Discovery – Network Share Discovery
Impact	T1490 T1489 T1486	– Inhibit System Recovery – Service Stop – Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator type	Description

b6663af099538a396775273d79cb6fff99a18e2de2a8a2a106de8212cc44f3e2	SHA256	Ragnar_locker Executable
ac16f3e23516cf6b22830c399b4aba9706d37adceb5eb8ea9960f71f1425df79	SHA256	Ragnar_locker Executable
68eb2d2d7866775d6bf106a914281491d23769a9eda88fc078328150b8432bb3	SHA256	Ragnar_locker Executable
b670441066ff868d06c682e5167b9dbc85b5323f3acfbbc044cabc0e5a594186	SHA256	Ragnar_locker Executable
9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376	SHA256	Ragnar_locker Executable
dd5d4cf9422b6e4514d49a3ec542cffb682be8a24079010cda689afbb44ac0f4	SHA256	Ragnar_locker Executable
63096f288f49b25d50f4aea52dc1fc00871b3927fa2a81fa0b0d752b261a3059	SHA256	Ragnar_locker Executable
a8ee0fafbd7b84417c0fb31709b2d9c25b2b8a16381b36756ca94609e2a6fcf6	SHA256	Ragnar_locker Executable
5fc6f4cfb0d11e99c439a13b6c247ec3202a9a343df63576ce9f31cffcdbaf76	SHA256	Ragnar_locker Executable
1472f5f559f90988f886d515f6d6c52e5d30283141ee2f13f92f7e1f7e6b8e9e	SHA256	Ragnar_locker Executable
ec35c76ad2c8192f09c02eca1f263b406163470ca8438d054db7adcf5bfc0597	SHA256	Ragnar_locker Executable
68eb2d2d7866775d6bf106a914281491d23769a9eda88fc078328150b8432bb3	SHA256	Ragnar_locker Executable

---

Source: https://blog.cyble.com/2022/01/20/deep-dive-into-ragnar-locker-ransomware-gang/