

Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone

 labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/

Jim Walter



Overview

Egregor ransomware is an offshoot of the Sekhmet malware family that has been active since mid-September 2020. The ransomware operates by compromising organizations, stealing sensitive user data, encrypting said data, and demanding a ransom to exchange encrypted documents. Egregor is ransomware associated with the cyberattacks against GEFCO and Barnes & Noble, Ubisoft, and numerous others.

As with other modern ransomware groups, the actors behind Egregor exfiltrate victim data and threaten to expose it publically should the victim fail to comply with the ransom demands.

Egregor Distribution Methods

The primary distribution method for Egregor is Cobalt Strike. Targeted environments are previously compromised through various means ([RDP exploit](#), [Phishing](#)) and once the Cobalt Strike beacon payload is established and persistent, it is then utilized to deliver and launch the Egregor payloads.

That being said, since Egregor is a RaaS with multiple affiliates, delivery and weaponization tactics can therefore vary. There have been limited and uncorroborated reports of Egregor utilizing [CVE-2020-0688](#) (a remote code execution flaw in Microsoft Exchange). [Some sources](#) also report the possible exploitation of [CVE-2018-8174](#) (VBScript Engine), [CVE-2018-4878](#) (Adobe Flash Player) & [CVE-2018-15982](#) (Adobe Flash Player). They have also been shown to use [LOTL](#) (Living off the Land) tools such as bitsadmin to download or update DLL components. In addition, some larger malware families and frameworks such as QBot have been observed distributing Egregor in [recent campaigns](#).

Egregor Payload Analysis

Egregor payloads (DLLs) are highly obfuscated, including Salsa20 encrypted configuration data. File encryption is achieved via a combination of the ChaCha stream cipher and RSA. Each payload contains a RSA-2048 public key.

DLL-based payloads require a key/password upon launch, with that key being specific to each sample. The `-p` parameter is passed to the payload concatenated with said key. For example, if the key is `123EVILBADGUYS` the parameter `-p123EVILBADGUYS` is required to successfully launch the payload.

This methodology also adds to the malware's ability to evade analysis by way of humans and dynamic systems. Without the valid key passed, the payload will decrypt incorrectly and fail to launch or terminate. This is a critical point to consider in the context of static and dynamic analysis of Egregor payloads. With no key, voluntary detonation and dynamic analysis become far more complex if not infeasible.

Additional parameters appear to be present in memory when the payloads are launched. Some of these are borderline self-explanatory, while others are still undergoing analysis. We have summarized the parameter usage below where possible.

```
--nomimikatz
--fast
--full ; encryption of entire system (local & network-accessible), no exclusions
--multiproc
--killrdp
--nonet ; exclude encryption of network drives
--path ; encrypt only specific path in this parameter
--target
--append ; customize the file extension to be used for encrypted files
--norename ; skip the process of renaming encrypted files
--greetings ; directly address target (by victim company name, typically)
--samba
```

Initial analysis of Egregor payloads indicates that the ransomware will avoid encrypting systems where the primary device language is one of the following:

- Armenian
- Azerbaijani
- Belarusian
- Georgian
- Kazakh
- Kyrgyz
- Romanian
- Russian
- Tajik
- Tatar
- Turkmen
- Ukrainian
- Uzbek

The primary method of data exfiltration appears to be Rclone, which is an open source utility that can be used to manage remote storage. Egregor payloads deposit their own copy of Rclone along with unique configuration data, controlling the exfiltration process.

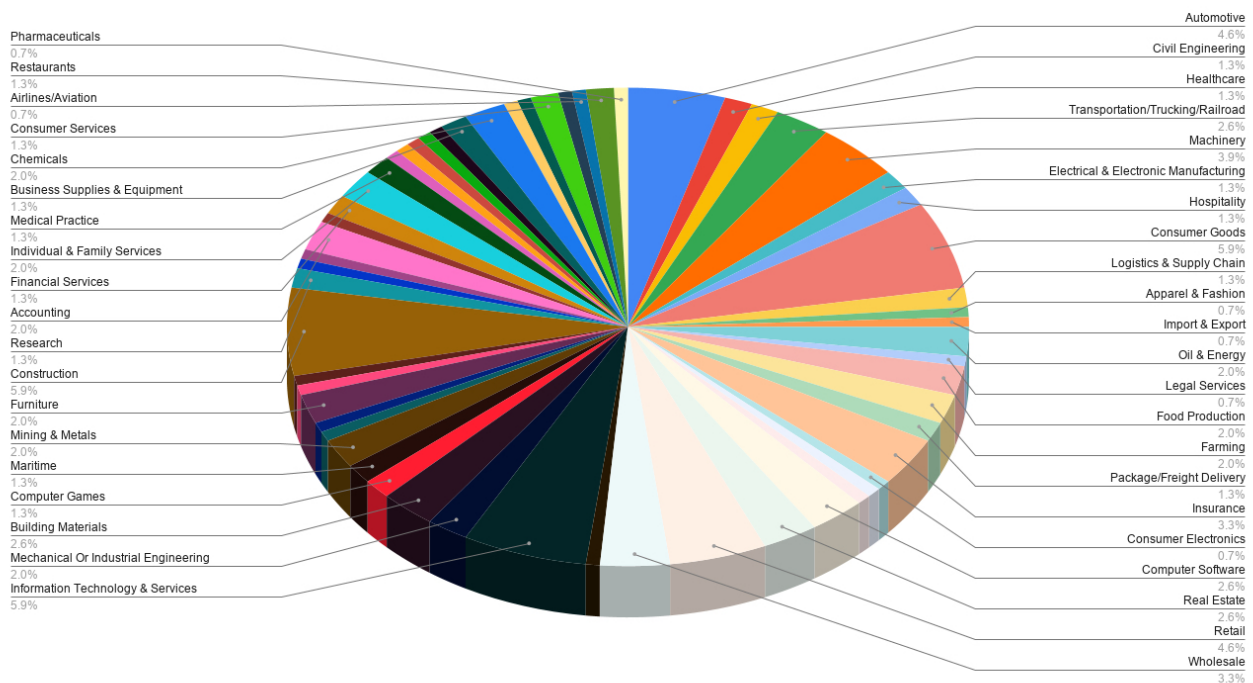


Post-Compromise Behavior

Egregor maintains a victim blog, which they use to threaten victims and post exfiltrated data in the event that victims fail to comply with their ransom demands. As of November 24th, 2020 there were 152 companies listed on the Egregor blog, spanning numerous industries across the globe. They do not appear to discriminate when it comes to industry or geography. The most frequently represented industries are:

- Information Technology and Services
- Construction
- Retail
- Consumer Goods
- Automotive

Egregor Victims: Industry %





The next time you are going to kill our domain name, you need to think about problems for companies in case of data distribution between different forums and darknet websites and torrent trackers. The guilty will be only yours.

Crytek

Published: 100%

Crytek has been locked by Egrogor

ransomware

Visited: 11834

Read more -->

Ubisoft

Published: 50%

Ubisoft has been compromised by Egrogor. We have sources of new Watch Dogs: Legion. Now we add TORRENT file for download.

ransomware

Visited: 13618

Read more -->

Hole of the month

This month two game industry major companies are nominated for the Hole of the Month Award

1. Game software developer Crytek (<https://www.crytek.com>).

That is amazing that while declaring to be the leader of the market this software is careless about its own security.

We were not able to pass the Australia size hole and take a look inside. What did we find there? Passwords in free access, security at the cavemen level, unencrypted chats, files with contracts, researches, engine source code and new developments.

We have also find development plans, bookkeeping and a lot more.

Some parts of that info will be published soon. Some parts will be sold to one of those who are very interested.

2. Game software developer Ubisoft (<https://www.ubisoft.com/>).

This developer if nominated not just for Hole of the Month. But also for the Clown of the Month Award.

We found source codes in free access in the main network. Passwords in the doc files without any protection, all the employees and developers data and personal information, contract, game engines and a lot of more.

Guys, if the goal of the last mission in your game about hackers was the hack of your company, we've done it. There's our prize?

The game WATCH DOGS: LEGION was completely downloaded from your company servers.

There's a possibility that soon we will make a present to all fans. We will compile and upload the game to public access.

The games of such level should be distributed freely. Nobody should take money for this

The Egregor ransom notes follow a familiar template as other ransomware families. Victims are instructed to visit their TOR-based payment portal for further instructions. There is also an encrypted blob at the bottom of each ransom note containing victim-specific system data, along with the encoded RSA public key.

Example:

---EGREGOR---

pWEzuKkw9nY82VRKYfrw4f4wvrnfnKEApQ5JTkf/YQPzxJtJmwKUjXV759aYQnPIZdGN1RUckdpMZWiYGmsWFY

---EGREGOR---

This 'blob' includes data pertaining to the victim's available local drives, the space and total size of those drives, the hostname, the names of any AV or Security products discovered, and the user/domain context. The 'blob' is primarily base64-encoded. When decoded the pertinent data is visible at the end of the plaintext.

```
NI 4 7
'""Q J'IU filh.x } YH>□kts Ju ! :nu i(jF; (br& |X
V kx >)a w?Dö o\K~o$
K
E C Df=U(!{N rpꠄ[ATgX>eй "o b*
718 A V)G~3->F)L#/8~3. X:RK>WJ( Q
Y2 7Xb?7 jzY %W0#HK Xi i?LHlg8Sc{gjk? JY/ m v/|<=_SBf~** 3o OG7wy++.ꠄ*AO| 0Ufd)~< `/ꠄ-R8j\ zkC ɔj i^ ;w-@cX
+;/ 7$" 送:emj:WGS } b ɔ lw/&!*d <0ZI B\vvP a63#Z" )3?_B/ZM.DZu O%bh g, z
`M \YO+
': #hHk i. :0 HW (: [REDACTED] 5B [REDACTED] 1Jf|A:R_0/0|C:F_10439/60937|D:F_71707/102269|E:C_0/0|
R SYSTEMh r:Windows Server 2016 Standardz [REDACTED]
```

Conclusion

Egregor is one of the more aggressive and complex ransomware families to hit in the last 6 to 8 months. As with other contemporary threats, the damage being done extends well beyond the cost of the ransom (which you should avoid), and now also includes any penalties associated with data breaches, public posting of private data, GDPR / compliance fallout, and beyond.

The SentinelOne Singularity Platform fully protects our customers from this ransomware and related families.

Indicators of Compromise

SHA256 Hashes

```
8483aaf9e1fa5b46486c9f2a14c688c30d2006e88de65d0295a57892de0bf4c9
3fd510a3b2e0b0802d57cd5b1cac1e61797d50a08b87d9b5243becd9e2f7073f
2b3518937fd231560c7dc4f5af672a033b1c810d7f2f82c8151c025ce75775bf
444a6897058fd4965770167b15a2ab13e6fd559a3e6f6cf5565d4d3282587459
c3c50adcc0a5cd2b39677f17fb5f2efca52cc4e47ccd2cdbbf38815d426be9e1
004a2dc3ec7b98fa7fe6ae9c23a8b051ec30bcfcd2bc387c440c07ff5180fe9a
608b5bf065f25cd1c6ac145e3bcdf0b1b6dc742a08e59ec0ce136fe5142774e9
3e5a6834cf6192a987ca9b0b4c8cb9202660e399ebe387af8c7407b12ae2da63
4ea8b8c37cfb02ccdba95fe91c12fb68a2b7174fdcbef7ddaadded8ceb0fdf97
9017c070ad6ac9ac52e361286b3ff24a315f721f488b53b7aaf6ac35de477f44
ee06c557f1acd5c4948b1df0413e49f3885f8ac96185a9d986b91a1231444541
765327e1dc0888c69c92203d90037c5154db9787f54d3fc8f1097830be8c76ab
14e547bebaa738b8605ba4182c4379317d121e268f846c0ed3da171375e65fe4
3fc382ae51ceca3ad6ef5880cdd2d89ef508f368911d3cd41c71a54453004c55
f0adfd3f89c9268953f93bfdfefb84432532a1e30542fee7bddda14dcb69a76c
a9d483c0f021b72a94324562068d8164f8cce0aa8f779faea304669390775436
3aad14d200887119f316be71d71aec11735dd3698a4fcaa50902fce71bdccb07
6ad7b3e0873c9ff122c32006fdc3675706a03c4778287085a020d839b74cd780
932778732711cd18d5c4aabc507a65180bf1d4bd2b7d2d4e5506be4b8193596e
```


SHA1 Hashes

3c03a1c61932bec2b276600ea52bd2803285ec62
f0215aac7be36a5fedeea51d34d8f8da2e98bf1b
948ef8caef5c1254be551cab8a64c687ea0faf84
50c3b800294f7ee4bde577d99f2118fc1c4ba3b9
38c88de0ece0451b0665f3616c02c2bad77a92a2
95aea6b24ed28c6ad13ec8d7a6f62652b039765e
3cc616d959eb2fe59642102f0565c0e55ee67dbc
5c99dc80ca69ce0f2d9b4f790ec1b57dba7153c9
beb48c2a7ff957d467d9199c954b89f8411d3ca8
03cdec4a0a63a016d0767650cdaf1d4d24669795
c9da06e3dbf406aec50bc145cba1a50b26db853a
ceca1a691c736632b3e98f2ed5b028d33c0f3c64
f6ad7b0a1d93b7a70e286b87f423119daa4ea4df
56eed20ea731d28d621723130518ac00bf50170d
fa33fd577f5eb4813bc69dce891361871cda860c
f7bf7cea89c6205d78fa42d735d81c1e5c183041
f1603f1ddf52391b16ee9e73e68f5dd405ab06b0
8768cf56e12a81d838e270dca9b82d30c35d026e
ac6d919b313bbb18624d26745121fca3e4ae0fd3

IP Addresses

45[.]153.242.129
217[.]8.117.148
45[.]153.242.129
45[.]11.19.70
49[.]12.104.241:81
185[.]238.0.233

Full URL Examples

h t t p://185.238.0[.]233/p.dll
h t t p://185.238.0[.]233/b.dll
h t t p://185.238.0[.]233/sed.dll
h t t p://185.238.0[.]233/hnt.dll
h t t p://185.238.0[.]233/88/k057.exe
h t t p://185.238.0[.]233/newsvc.zip

Victim Blog / Archive

h t t p://egregoranrmzapcv[.]onion
h t t p s://egregornews[.]com/

Payment Portal

h t t p://egregor4u5ipdzhv[.]onion/

MITRE ATT&CK

Indicator Removal on Host: File Deletion [T1070.004](#)

Modify Registry [T1112](#)

Query Registry [T1012](#)

System Information Discovery [T1082](#)

Native API [T1106](#)

Hijack Execution Flow: DLL Side-Loading [T1574.002](#)

Process Injection [T1055](#)

Masquerading [T1036](#)

System Time Discovery [T1124](#)

Archive Collected Data [T1560](#)

Virtualization/Sandbox Evasion [T1497](#)

Software Discovery: Security Software Discovery [T1518.001](#)

Peripheral Device Discovery [T1120](#)

Inhibit System Recovery [T1490](#)

Create or Modify System Process: Windows Service [T1031](#)

Exfiltration [TA0010](#)

Miscellaneous

Ransom Note example (RECOVER-FILES.txt)