TLP:WHITE

EGREGOR RANSOMWARE

1.0

02/03/2021

TLP:WHITE

Since mid-September 2020, the ANSSI (French National Cyber Security Agency) has observed a vast campaign of attacks using the Egregor ransomware. At least 69 organisations, including some French companies, are believed to have been targeted [1] [2]. As ransomware, Egregor poses a significant threat since the activity of victim organisations is deeply affected. Bitcoin ransom demands can be in excess of $4,000,000 [2].

1 Business model

Egregor is operated using the Ransomware-as-a-service (RaaS) [3] business model. Several attacker groups may therefore carry out attacks delivering Egregor and the kill chain may vary from one attack to the other. The ransomware operators are not necessarily its developers.

Egregor is part of the Sekhmet malware family, discovered in March 2020 [4]. Its operators attempt to break into the target organisation's information system to steal sensitive documents and encrypt them. They then seek the payment of a ransom in exchange for which they claim to be able to decrypt these documents [5].

Targeted organisations are also blackmailed with the threat of disclosure of their data: if the ransom is not paid within three days, operators threaten to publish the stolen files on a dedicated website [6]. To increase the pressure on victims, operators may also threaten to release some of the stolen information to the media [7].

Operators reportedly pay 30% of the profits to the developers [8].

2 Origins and links with the Sekhmet and Maze ransomwares

attacks campaign delivering Egregor is believed to be linked to the end of the activity of the attacker group behind the Maze ransomware [9] [10]. As a result, many previous Maze affiliates are believed to have started using Egregor. Furthermore, some operators of other malware, such as those of the Qakbot RAT are now believed to prefer Egregor over Prolock as the final payload [11] [2].

Many researchers consider Egregor the direct descendant of Maze. This assumption is based on several factors:

- Chronology: Egregor's expansion coincides with the end of activity of the Maze ransomware [6].
- There are thought to be several code similarities between Egregor, Sekhmet and Maze [7] [12] [13] [14]. Sekhmet and Maze also use the same encryption algorithms (ChaCha and RSA-2048).
- The ransom notes of Maze, Sekhmet and Egregor are also very similar [15]. In addition to their similar structure, parts of Egregor's ransom notes are identical [6].
- The same infrastructure (IP 185.238.0[.]233) is believed to have distributed both Maze and Egregor, as well as zip files containing the file synchronisation tool RClone and the configuration files [6].

Furthermore, Egregor reportedly shows similarities with other ransomwares and malicious codes, such as Clop and TinyMet Payload v0.2 [1].

Comment: It is common for different ransomware operators to be inspired by the latest tactics and techniques. However, all of these factors suggest that it is likely that one or more players in the Maze group is now working on Egregor, or at the very least, that part of the Maze code has been sold on or recovered by Egregor's developers.

3 Victimology

Egregor is used in attacks targeting organisations because of their profitability or their ability to pay high ransom amounts (Big Game Hunting).

All activity sectors and all geographical areas represent potential targets. However, many of Egregor's victims are located in the United States and belong to the service and manufacturing sectors [11] [2].

4 Kill chain

4.1 Infection vector

Little is currently known about the infection vector(s) used. Nevertheless, they appear to be using phishing emails with an attachment containing a malicious macro [6] as well as illegitimate Remote Desktop Protocol (RDP) access.

4.2 Lateral movement

The Qakbot banking Trojan is believed to be currently used to distribute Egregor along with the Prolock ransomware. In at least one case, Egregor operators reportedly used Microsoft Excel documents imitating DocuSign encrypted documents and email thread hijacking to distribute Qakbot [2].

The Ursnif and IcedID trojans are also thought to have been used by the Egregor operators. The use of these malicious codes allow the operators to retrieve information facilitating subsequent lateral movements [6]. The operators are also thought to have distributed Qakbot over the network using the PsExec tool [2].

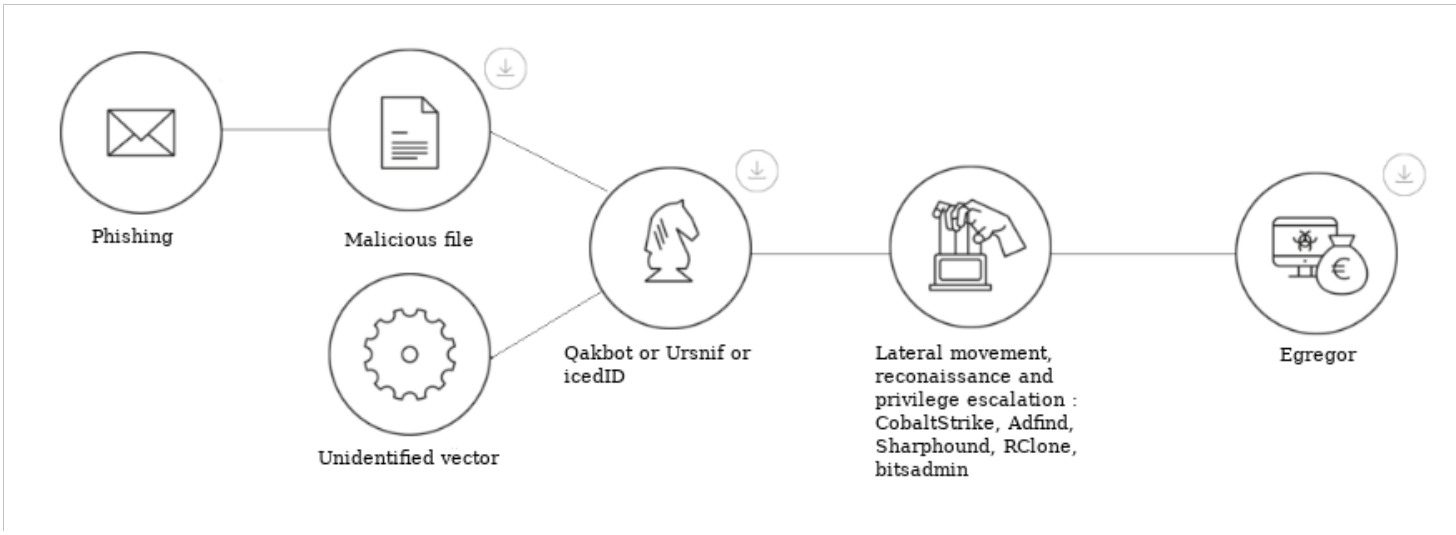

Fig. 4.1: Simplified diagram of the Qakbot (/Ursnif/IcedID) - Egregor kill chain

As Maze affiliates migrate to Egregor, the tactics, techniques and procedures (TTPs) used by Egregor operators may evolve in line with the TTPs usually associated with Maze [2].

The SharpHound or AdFind tools are believed to have been used during the lateral movement phase within the Active Directory (AD). To move around the network, Egregor operators are believed to use SMB beacons *via* the Cobalt Strike tool or administrator access. Cobalt Strike payloads can be deobfuscated using the CyberChef tool [16]. Connections to the command and control server are made *via* the HTTPS protocol.

4.3 Evasion of defensive measures

Egregor uses multiple techniques of obfuscation to conceal its activities and complicate its analysis. In particular, Egregor imitates the svchost.exe process to execute the RClone client and uses the injection of code into the memory to increase its stealth via a reflective dynamic-link library injection [16]).

To date, the use of code obfuscation techniques[1], anti-debugging techniques and the use of native Windows APIs are proven. The payload can only be decrypted using a specific argument inserted in the command line. In one incident this argument was "-passegregor10" [6]. During another incident, the following command was used to run the dll to decrypt and then run Egregor [2]:

```
rundll32.exe C:\Windows\q.dll,DllRegisterServer -password --mode
```

According to an analysis by CybleInc, the Egregor dll was compiled by Microsoft Visual C++ 8.0 and contains 3 export functions: *DllInstall*, *DllRegisterServer* and *DllUnregisterServer* [1].

4.4 Exfiltration

The RClone client is thought to allow operators to exfiltrate data for blackmail and disclosure purposes [2].

4.5 Encryption

Egregor seeks to stop numerous processes to ensure that they do not access the files during encryption. Certain targeted processes (*procmon* and *dumpcat* for example) are usually used by researchers and complicate analysis of Egregor. Operators also reportedly attempt to create a Group Policy Object (GPO) to disable Windows Defender [12].

The Bitsadmin command line tool is believed to have been used to download and execute the malicious Egregor dll. The payload is injected into an "iexplore.exe" process and starts the encryption. When the payload is executed, it first checks the language of the operating system [12]. If the system is configured in one of the following languages, the machine will not be encrypted:

- Armenian (Armenia);
- Azeri (Cyrillic, Azerbaijan);
- Belarusian (Belarus);
- Georgian (Georgia);
- Kazakh (Kazakhstan);
- Kyrgyz (Kyrgyzstan);
- Moldovan (Moldova);
- Russian (Moldova);
- Russian (Russia);
- Tajiki (Cyrillic, Tajikistan);
- Tatar (Russia);
- Turkmen (Turkmenistan);

[1] In particular, the command PUSH + JUMP instead of RETN is used in XOR operations [12] [16].

- Ukrainian (Ukraine);
- Uzbek (Latin, Uzbekistan).

This practice is common among ransomwares. However, researchers believe that the verification method of the language used by Egregor is very similar to that of Sekhmet and Maze [2].

Egregor attempts to create a shortcut in directories to check that it has the privileges required to encrypt their content. This shortcut is created with the following option:

```
FILE_FLAG_DELETE_ON_CLOSE
```

This option ensures that the shortcut is deleted automatically [2].

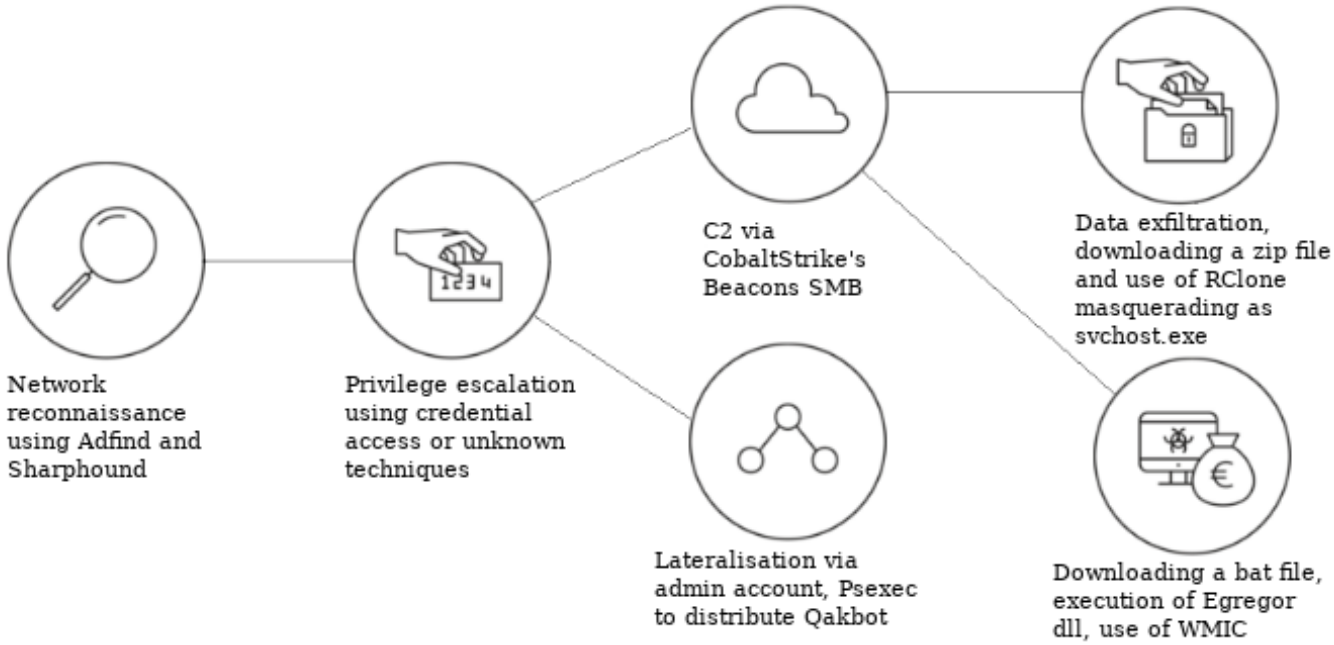

Fig. 4.2: Diagram of the kill chain following the use of trojans

Egregor also attempts to remove shadow copies.

Comment: The ANSSI is not currently able to confirm the use of the vssadmin command by Egregor operators. The Raccine tool available on GitHub can intercept the use of vssadmin, prevent the deletion of shadow copies and even, in some cases, block the chain of infection. Raccine is a temporary solution only to be implemented as a last resort in the face of an imminent threat of encryption. Its use is not a substitute for the implementation of technical security measures.

Egregor uses ChaCha encryption algorithms and RSA-2048. Once encrypted, the files are renamed by adding a new random extension corresponding to the following regular expression [1]:

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

No tool is currently capable of decrypting encrypted files other than the private key held by the operators.

A “RECOVER-FILES.txt” text file containing the ransom note is created in all folders containing encrypted documents. This file also contains the procedure for contacting the ransomware operators [1]. The technical block at the end of the ransom file also contains information about the number of encrypted files, the workstation and the affected domain [2].

4.6 Disclosure of data

Several domains have been used by Egregor operators. The domains “egregor-support.com”, “egregorsup.com” and “newsegregor.com” are attributed to the Egregor ransomware. Investigations carried out by the ANSSI show that all three have been filed with the registrar Eranet and use DNSPod name servers. This registrar/name server pair is fairly uncommon, however it is consistent with the registration habits of other attacker group domains, including some domains attributed to TA505.

The “egregor-support.com” and “egregorsup.com” domains allow contact to be made in order to decrypt files and/or negotiate with operators. The “newsegregor.com” and “egregoranrmzapcv.onion” domains are used to disclose data.

Comment: This could indicate that these groups share the same service providers for domain registration. This confirms the trend towards outsourcing as well as task-based specialisation within cyber criminal groups.

5 The Twisted Spider group

On 1st November 2020, the Twisted Spider group issued a press release indicating the end of the “Maze Team” project.

At the end of October 2020, the Egregor site operators threatened to distribute stolen data on various forums, the darknet and *via* torrent if their domains continued to be targeted by attackers [7]. In at least one incident, comments in Russian were included in a PowerShell script used by the attackers [2]. An operator of the group reportedly declared in June 2020 that the group was now cooperating with other attacker groups [9].

Comment: It is possible that the high degree of visibility acquired by the Maze group may have forced the group to bring the project to an end. Some of the members would then have developed Sekhmet in the event of the Maze project coming to a close. With Sekhmet having proven its worth, it is thought to have become Egregor following this closure. This hypothesis would explain the many similarities between these three different ransomwares.

6 Summary of the chain of infection

With regard to the methods used by Egregor affiliates, the following TTPs are likely to be employed:

- **Infection vectors**
  - **T1078**: Valid Accounts - Use of legitimate identifiers previously obtained [11].
  - **T1566**: Phishing - Sometimes through the hijacking of email exchanges [11].

- **Execution**
  - **T1086**: Powershell - Many affiliates use Powershell for the execution of their scripts and codes on victims' networks [11].
  - **T1569**: System Services: Service Execution [11] [16].
  - **T1053.005**: Scheduled Task [16].
  - **T1047**: Windows Management Instrumentation [16].

- **Persistence**
  - **T1543.003**: Create or Modify System Process, Windows Service [16] [11].
  - **T1098**: Account Manipulation [11].

- **Elevation of privileges**
  - **T1548**: Abuse Elevation Control Mechanism [11].

- **Defence evasion**
  - **T1562.001**: Disable or Modify Tools - Disabling of Windows Defender through the creation of a Group Policy Object [16].
  - **T1222**: File and Directory Permissions Modification [11].
  - **T1001**: Data Obfuscation - in particular through the use of JUMP [11].
  - **T1027.004**: Compile After Delivery - Compilation after delivery, using a password to decrypt and execute the Egregor dll [11].

- **Access to identification information**
  - **T1110**: Brute Force [11].
  - **T1552**: Unsecured Credentials - Recovery of identification information *via* the registry [11].

- **Lateral movement**
  Attackers in particular use the AdFind and SharpHound tools to map the network.
  - **T1087**: Account Discovery - Reconnaissance of admin accounts [16] [11].
  - **T1482**: Domain Trust Discovery [16].
  - **T1069.001**: Permission Group Discovery [16].
  - **T1082**: System Information Discovery [11].
  - **T1057**: Process Discovery [11].
  - **T1021.001**: Remote Desktop Protocol - Within compromised networks, some attackers use RDP sessions for propagation, including using the rdp.bat batch file to modify the registry and firewall rules to allow RDP connections [2].

  - **T1021.002**: SMB/Windows Admin Shares - Use of Remote Services, in particular SMB/Windows Admin Shares [16].

- **Command and Control**
  - **T1071**: Application Layer Protocol - Use of SMB beacon *via* Cobalt Strike [16].

- **Exfiltration**
  - **T1567.002**:Exfiltration to Cloud Storage - Exfiltration of data, mainly using RClone [16].

- **Impact**
  - **T1486**: Data Encrypted for Impact - Data encryption is the main objective of the Egregor operators [11].
  - **T1490**: Inhibit System Recovery - Hidden Windows copies are deleted [11].

7 Recommendations

In order to protect against and react to this type of attack, the ANSSI recommends consulting the *Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident?* (Ransomware attacks, all concerned - How to anticipate them and react in the event of an incident) guide.

To reduce the risk of ransomware attacks, especially by Egregor:

- back up data regularly, physically move the backup of your network and put it in a safe place while ensuring it works;
- have the capacity to detect and block the use of Cobalt Strike on the network;
- be particularly vigilant with RDP connections and the use of BITS, wmic and PowerShell on the network;
- keep software and systems up to date. Special attention must be paid to VPN solutions and their updates to allow remote access for your employees;
- if possible, disable macros in office automation solutions that allow the automated completion of tasks. This rule will prevent the spread of ransomware *via* application vulnerabilities;
- encrypt sensitive documents on your network to prevent their possible disclosure [17];
- use anti-virus software and keep it updated;
- partition the information system;
- limit user privileges and application permissions;
- if possible, do not expose remote office services (such as RDP) on public networks and use complex passwords on these services;
- control Internet access;
- implement the supervision of logs;
- ensure awareness among employees;
- implement a plan to respond to cyber attacks;
- think about the cyber crisis communication strategy.

The ANSSI's advice on how to react in the event of an attack:

- ensure that attackers have not moved laterally if Qakbot, Ursnif or IcedID is detected on the network;
- coordinate the management of the cyber crisis;
- find technical assistance;
- immediately disconnect the machines from the network without deleting their data;
- communicate at the appropriate level;
- do not pay the ransom;
- file a complaint;
- restore systems from healthy sources.

8 Bibliography

[1] Cyble, Inc. “Egregor Ransomware - A Deep Dive into Its Activities and Techniques”. Oct. 31, 2020. In: (Oct. 31, 2020).

[2] Group-IB. *The Locking Egregor*. Nov. 23, 2020. URL: https://www.group-ib.com/blog/egregor.

[3] ZDNet. “As Maze Retires, Clients Turn to Sekhmet Ransomware Spin-off Egregor”. Nov. 4, 2020. In: (Nov. 4, 2020).

[4] Twitter. *@demonslay335*. Sept. 18, 2020. URL: https://twitter.com/demonslay335/status/1307056098596335628.

[5] Dark Reading. “Meet ’Egregor,’ a New Ransomware Family to Watch”. Oct. 5, 2020. In: (Oct. 5, 2020).

[6] Cybereason. “Cybereason vs. Egregor Ransomware”. Nov. 26, 2020. In: (Nov. 26, 2020).

[7] ThreatPost. “Egregor Ransomware Threatens ‘Mass-Media’ Release of Corporate Data”. Oct. 2, 2020. In: (Oct. 2, 2020).

[8] Bleeping Computer. “Largest Global Staffing Agency Randstad Hit by Egregor Ransomware”. Dec. 4, 2020. In: (Dec. 4, 2020).

[9] Bleeping Computer. “Maze Ransomware Shuts down Operations, Denies Creating Cartel”. Nov. 2, 2020. In: (Nov. 2, 2020).

[10] Bleeping Computer. “Maze Ransomware Is Shutting down Its Cybercrime Operation”. Oct. 29, 2020. In: (Oct. 29, 2020).

[11] lauren-place. *Egregor: The New Ransomware Variant to Watch | Digital Shadows*. Nov. 24, 2020. URL: https://www.digitalshadows.com/blog-and-research/egregor-the-new-ransomware-variant-to-watch/.

[12] Kaspersky. “Targeted Ransomware: It’s Not Just about Encrypting Your Data!” Nov. 11, 2020. In: (Nov. 11, 2020).

[13] Security Boulevard. “Egregor: Sekhmet’s Cousin”. Oct. 29, 2020. In: (Oct. 29, 2020).

[14] Unit42. *Threat Assessment: Egregor Ransomware*. Dec. 9, 2020. URL: https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/.

[15] Enigma Software. *Sekhmet Ransomware*. Apr. 2, 2020. URL: https://www.enigmasoftware.com/sekhmetransomware-removal/.

[16] Intrinsec. *Egregor – Prolock: Fraternal Twins ?* Nov. 12, 2020. URL: https://www.intrinsec.com/egregor-prolock/.

[17] Cyware. “Egregor - A New Ransomware Gang on the Rise”. Oct. 25, 2020. In: (Oct. 25, 2020).

1.0 - 02/03/2021
Open License (Étalab - v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN