TLP:WHITE

LE RANÇONGICIEL EGREGOR

1.0

11/12/2020

TLP:WHITE

Depuis la mi-septembre 2020, l'ANSSI constate une vaste campagne d'attaques informatiques menées à l'aide du rançongiciel Egregor. À date, au moins 69 organisations, dont certaines entreprises françaises auraient été ciblées [1] [2]. En tant que rançongiciel, Egregor constitue une menace importante dans la mesure où l'activité des organisations victimes est fortement affectée. Les demandes de rançon en bitcoin peuvent être supérieures à 4 000 000 $ [2].

1 Modèle économique

Egregor fonctionne sous le modèle économique du *Ransomware-as-a-service* (RaaS) [3]. Plusieurs groupes d'attaquants peuvent donc mener des attaques délivrant Egregor et les chaînes d'infection peuvent différer d'une compromission à l'autre. Les opérateurs du rançongiciel ne sont pas nécessairement ses développeurs.

Egregor est issu de la famille de logiciels malveillants Sekhmet, découverte en mars 2020 [4]. Ses opérateurs cherchent à s'introduire dans le système d'information de l'organisation ciblée afin de dérober des documents sensibles et de les chiffrer. Les opérateurs cherchent à obtenir le paiement d'une rançon en échange duquel ils déclarent pouvoir déchiffrer ces documents [5].

Les organisations ciblées sont également victimes de chantage à la divulgation de données : en cas de non-paiement de la rançon sous trois jours, les opérateurs menacent de publier les fichiers dérobés sur un site Internet dédié [6]. Afin de faire pression sur les victimes, les opérateurs peuvent également menacer de communiquer une partie des informations dérobées aux médias [7].

Les opérateurs reverseraient 30 % des bénéfices aux développeurs [8].

2 Origines et liens avec les rançongiciels Sekhmet et Maze

La campagne d'attaques délivrant Egregor serait liée à la fin d'activité du groupe d'attaquants à l'origine du rançongiciel Maze [9] [10]. En conséquence, de nombreux affiliés se seraient mis à utiliser Egregor. De plus, certains opérateurs d'autres logiciels malveillants, tel que ceux du RAT Qakbot privilégieraient dorénavant l'utilisation d'Egregor au détriment de Prolock en tant que charge finale [11] [2].

Pour plusieurs chercheurs, Egregor constituerait le descendant direct de Maze. Cette supposition repose sur plusieurs éléments :

- La temporalité : l'expansion d'Egregor est concomitante à la fin d'activité du rançongiciel Maze [6].
- Il existerait plusieurs similitudes de code entre Egregor, Sekhmet et Maze [7] [12] [13] [14]. Sekhmet et Maze utilisent également les mêmes algorithmes de chiffrement (ChaCha et RSA-2048).
- Les notes de rançons Maze, Sekhmet et Egregor sont également très similaires [15]. Outre leur structure proche, certaines parties des notes de rançons d'Egregor sont identiques [6].
- La même infrastructure (IP 185.238.0[.]233) aurait distribué Maze et Egregor, ainsi que des fichiers zip contenant l'outil de synchronisation de fichiers *RClone* et des fichiers de configuration [6].

En outre, Egregor montrerait des similarités avec d'autres rançongiciels et codes malveillants, tels que Clop et TinyMet Payload v0.2 [1].

Commentaire : Il est courant que les différents opérateurs de rançongiciel s'inspirent des tactiques et techniques en vogue. Toutefois, l'ensemble de ces éléments semble indiquer qu'il est probable qu'un ou plusieurs acteurs du groupe Maze travaillent désormais sur Egregor, ou a minima, qu'une partie du code de Maze aurait été revendue ou récupérée par les développeurs d'Egregor.

3 Victimologie

Egregor est mis en œuvre dans le cadre d'attaques ciblant des organisations en raison de leur rentabilité ou de leur capacité à payer des rançons de montants élevés (*Big Game Hunting*).

Tous les secteurs d'activité et toutes les zones géographiques peuvent constituer des cibles potentielles. Toutefois, de nombreuses victimes d'Egregor sont localisées aux États-Unis et appartiennent aux secteurs des services et de l'industrie manufacturière [11] [2].

4 Chaîne d'infection

4.1 Vecteur d'infection

Peu d'éléments sont connus pour le moment à propos du (ou des) vecteur d'infection utilisé. Néanmoins, il semblerait qu'ils utilisent des courriels d'hameçonnage avec une pièce-jointe contenant une macro malveillante [6] ainsi que des accès illégitimes en *Remote Desktop Protocol* (RDP).

4.2 Latéralisation

Le cheval de Troie bancaire Qakbot serait actuellement utilisé pour distribuer Egregor ainsi que le rançongiciel Prolock. Dans au moins un cas, les opérateurs d'Egregor auraient utilisé des documents Microsoft Excel imitant les documents chiffrés DocuSign et le détournement d'échanges par courriel (*email thread hijacking*) afin de distribuer Qakbot [2].

Les chevaux de Troie Ursnif et IcedID auraient également été utilisés par les opérateurs d'Egregor. L'utilisation de ces codes malveillants permet notamment de récupérer des informations facilitant les mouvements latéraux ultérieurs [6]. Les opérateurs auraient également distribué Qakbot sur le réseau à l'aide de l'outil PsExec [2].

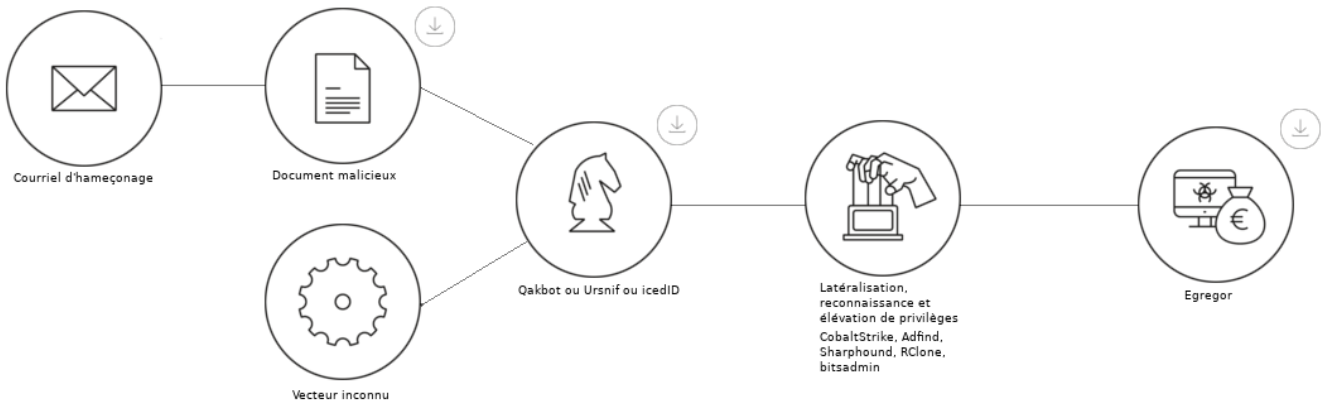

Fig. 4.1 : Schéma simplifié de la chaîne d'infection Qakbot (/Ursnif/IcedID) - Egregor

A mesure que les affiliés de Maze migrent vers Egregor, il est possible que les techniques tactiques et procédures (TTPs) utilisées par les opérateurs d'Egregor évoluent pour correspondre à des TTPs habituellement associées à Maze [2].

Les outils Sharphound ou Adfind auraient été utilisés durant la phase de latéralisation au sein de l' *Active directory* (AD). Pour se déplacer au sein du réseau, les opérateurs d'Egregor utiliseraient des balises SMB *via* l'outil Cobalt Strike ou des accès administrateurs. Les charges utiles de Cobalt Strike peuvent être déobfusquées à l'aide de l'outil *CyberChef* [16]. Les connexions avec le serveur de commande et de contrôle se font *via* le protocole HTTPS.

4.3 Évasion des mesures de défense

Egregor utilise de multiples techniques afin de dissimuler ses activités et de compliquer son analyse, notamment en imitant le processus svchost.exe pour exécuter le client de RClone ainsi que *via* l'injection de code en mémoire pour augmenter sa furtivité (*reflective dynamic-link library injection* [16]).

A ce jour, l'utilisation de techniques d'assombrissement du code (*obfuscation*)[1], de techniques anti-débogage et l'utilisation des API natives de Windows sont avérées. La charge utile ne peut être déchiffrée qu'à l'aide d'un argument spécifique inséré en ligne de commande. Lors d'un incident, cet argument était "-passegregor10" [6]. Durant un autre incident, la commande suivante a été utilisée afin d'exécuter la dll permettant de déchiffrer puis exécuter Egregor [2] :

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

D'après une analyse de CybleInc, la dll d'Egregor aurait été compilé par Microsoft Visual C++ 8.0 et contient 3 fonctions d'export : *DllInstall*, *DllRegisterServer* et *DllUnregisterServer* [1].

4.4 Exfiltration

Le client de l'outil *RClone* permettrait aux opérateurs d'exfiltrer les données à des fins de chantage et de divulgation [2].

4.5 Chiffrement

Egregor cherche à arrêter de nombreux processus afin de s'assurer qu'ils n'accèdent pas aux fichiers durant le chiffrement. Certains processus ciblés (*procmon* et *dumpcat* par exemple) sont habituellement utilisés par des chercheurs et compliquent l'analyse d'Egregor. Les opérateurs tenteraient également de créer un objet de stratégie de groupe (*Group Policy Object*) afin de désactiver Windows Defender [12].

L'outil en ligne de commande *bitsadmin* aurait été utilisé pour télécharger et exécuter la dll malveillante d'Egregor. La charge utile est injectée dans un processus « iexplore.exe » et débute le chiffrement. Lorsque la charge utile est exécutée, elle vérifie dans un premier temps la langue du système d'exploitation [12]. Si le système est configuré dans l'une des langues suivantes, aucun document de la machine ne sera chiffré :

- Arménien (Arménie) ;
- Azerbaïdjanais (Cyrillique, Azerbaïdjan) ;
- Biélorusse (Biélorussie) ;
- Géorgien (Géorgie) ;
- Kazakh (Kazakhstan) ;
- Kirghize (Kirghizistan) ;
- Moldavie (Moldavie) ;

[1] La commande PUSH + JUMP au lieu de RETN est particulièrement utilisée, opérations XOR [12] [16].

- Russe (Moldavie) ;
- Russe (Russie) ;
- Tadjik (Cyrillique, Tadjikistan) ;
- Tatar (Russe) ;
- Turkmène (Turkménistan) ;
- Ukrainien (Ukraine) ;
- Ouzbek (Latin, Ouzbékistan).

Cette pratique est courante dans les rançongiciels. Toutefois, des chercheurs jugent que la méthode de vérification utilisée par Egregor est très similaire à celle de Sekhmet et Maze [2].

Egregor tente de créer un raccourci dans les répertoires afin de vérifier qu'il possède les droits pour en chiffrer le contenu. Ce raccourci est créé avec l'option suivante :

```
FILE_FLAG_DELETE_ON_CLOSE
```

Cette option permet de s'assurer que le raccourci soit automatiquement supprimé [2].

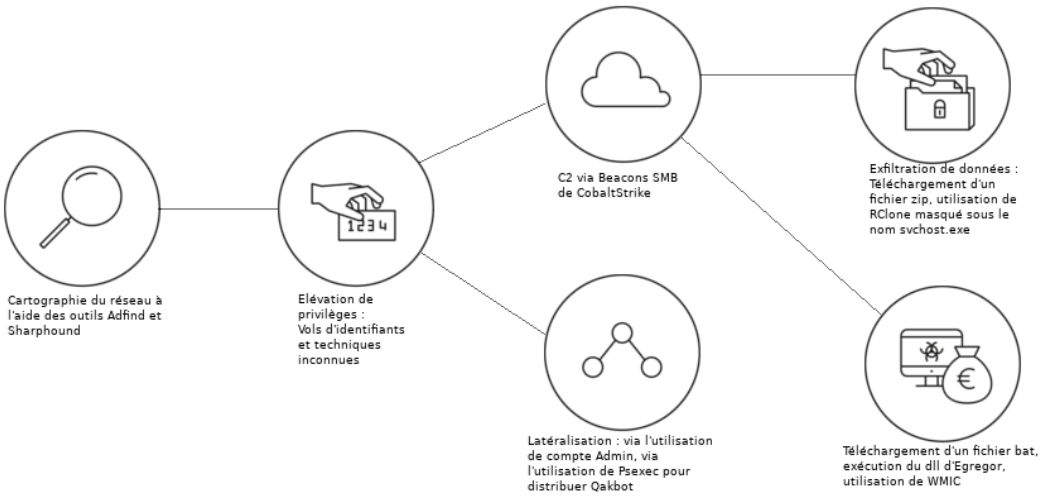

Fig. 4.2 : Schéma de la chaîne d'infection après l'utilisation des chevaux de Troie

Egregor tente également de supprimer les copies fantômes.

Commentaire : A ce jour, l'ANSSI n'est pas en mesure de confirmer l'utilisation de la commande vssadmin par les opérateurs d'Egregor. L'outil Raccine disponible sur Github permet d'intercepter le recours à vssadmin et d'empêcher la suppression des copies fantômes voire dans certains cas de bloquer la chaîne d'infection. Raccine est une solution temporaire uniquement à mettre en œuvre en dernier recours face à une menace imminente de chiffrement. Son utilisation ne remplace pas la mise en œuvre de mesures techniques de sécurité et de défense en profondeur.

Egregor utilise les algorithmes de chiffrement ChaCha et le RSA-2048. Une fois chiffrés, les fichiers sont renommés en ajoutant une nouvelle extension aléatoire correspondant à l'expression régulière suivante [1] :

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

Il n'existe pour le moment pas d'outil capable de déchiffrer les fichiers chiffrés hormis la clé privée possédée par les opérateurs.

Un fichier texte « RECOVER-FILES.txt » contenant la note de rançon est créé dans tous les dossiers contenant des documents chiffrés. Ce fichier contient également la marche à suivre pour contacter les opérateurs du rançongiciel [1]. Le bloc technique à la fin du fichier de rançon contient également des informations concernant le nombre de fichiers chiffrés, le poste de travail et le domaine touché [2].

4.6 Divulgation des données

Plusieurs domaines ont été utilisés par les opérateurs d'Egregor. Les domaines "egregor-support.com", "egregor-sup.com" et "newsegregor.com" sont attribués au rançongiciel Egregor. Les investigations menées par l'ANSSI montrent qu'ils ont tous les trois été déposés chez le registraire Eranet et utilisent les serveurs de noms de DNS-Pod. Ce couple registraire/serveur de noms est relativement peu commun, cependant, il correspond aux habitudes d'enregistrement d'autres domaines de groupes d'attaquants, notamment certains domaines attribués à TA505.

Les domaines "egregor-support.com" et "egregorsup.com" permettent d'entrer en contact afin de déchiffrer des fichiers et/ou de négocier avec les opérateurs. Les domaines "newsegregor.com" et "egregoranrmzapcv.onion" sont utilisés pour divulguer les données.

Commentaire : Cela pourrait indiquer que ces groupes ont des prestataires en commun en ce qui concerne l'enregistrement de domaines. Cet élément confirme la tendance à l'externalisation ainsi qu'à la spécialisation par tâche au sein des groupes d'attaquants cybercriminels.

5 Le groupe Twisted Spider

Le 1er novembre, le groupe Twisted Spider a publié un communiqué de presse indiquant la fin du projet "Maze Team".

Les opérateurs du site d'Egregor menaçaient à la fin du mois d'octobre 2020 de distribuer des données dérobés sur divers forums, sur le darknet ainsi que *via* torrent si leurs domaines continuaient à être ciblés par des attaquants [7]. Durant un incident au moins, des commentaires en langue russe figuraient dans un script PowerShell utilisé par les attaquants [2]. Un opérateur du groupe aurait déclaré en juin 2020 que le groupe coopérait désormais avec d'autres groupes d'attaquants [9].

Commentaire : Il est possible que la forte visibilité acquise par le groupe Maze ait contraint le groupe à mettre fin au projet. Une partie des membres aurait alors développé Sekhmet dans l'éventualité de la fermeture du projet Maze. Sekmhet ayant fait ses preuves, ce dernier serait devenu Egregor à la suite de cette fermeture. Cette hypothèse expliquerait les nombreuses similitudes entre ces trois différents rançongiciels.

6 Récapitulatif de la chaîne d'infection

Au regard des méthodes employées par les affiliés d'Egregor, les TTPs suivantes sont susceptibles d'être employées :

- **Vecteurs d'infection**
  - **T1078** : *Valid Accounts* - Utilisation d'identifiants légitimes obtenus préalablement [11].
  - **T1566** : *Phishing* - Hameçonnage, parfois *via* le détournement d'échanges de courriels [11].

- **Execution**
  - **T1086** : *Powershell* - De nombreux affiliés utilisent Powershell pour l'exécution de leurs scripts et codes sur les réseaux victimes [11].
  - **T1569** : *System Services: Service Execution* - Exécution à l'aide des services système [11] [16].
  - **T1053.005** : *Scheduled Task* - Exécution *via* des tâches planifiées [16].
  - **T1047** : *Windows Management Instrumentation* - Utilisation du *Windows Management Instrumentation* [16].

- **Persistance**
  - **T1543.003** : *Create or Modify System Process, Windows Service* - Création ou modification de processus système, notamment de Windows Service [16] [11].
  - **T1098** : *Account Manipulation* - Manipulation de compte [11].

- **Élévation de privilèges**
  - **T1548** : *Abuse Elevation Control Mechanism* - Abus du mécanisme de contrôle de l'élévation, contournement du contrôle d'accès utilisateur [11].

- **Évasion de la défense**
  - **T1562.001** : *Disable or Modify Tools* - Désactivation de Windows Defender *via* la création d'un Group Policy Object [16].
  - **T1222** : *File and Directory Permissions Modification* - Modification des droits sur les fichiers [11].
  - **T1001** : *Data Obfuscation* - Assombrissement du code, notamment *via* l'utilisation de JUMP [11].
  - **T1027.004** : *Compile After Delivery* - Compilation après la distribution, utilisation d'un mot de passe pour déchiffrer et exécuter la dll d'Egregor [11].

- **Accès aux informations d'identification**
  - **T1110** : *Brute Force* - Utilisation de la force brute [11].
  - **T1552** : *Unsecured Credentials* - Récupération des informations d'identification *via* le registre [11].

- **Latéralisation**
  Les attaquants utilisent notamment les outils Adfind et Sharphound afin de cartographier le réseau.
  - **T1087** : *Account Discovery* - Reconnaissance de comptes admin [16], [11].
  - **T1482** : *Domain Trust Discovery* - Reconnaissance des permissions de domaine [16].
  - **T1069.001** : *Permission Group Discovery* - Reconnaissance des permissions de groupe [16].
  - **T1082** : *System Information Discovery* - Reconnaissance sur le système d'information [11].
  - **T1057** : *Process Discovery* - Reconnaissance de processus [11].

  - **T1021.001** : *Remote Desktop Protocol* - Au sein des réseaux compromis, certains attaquants utilisent des sessions RDP pour se propager, notamment à l'aide du fichier batch rdp.bat afin de modifier le registre et les règles du pare-feu pour autoriser les connexions RDP [2].
  - **T1021.002** : *SMB/Windows Admin Shares* - Utilisation des Remote Services, notamment SMB/Windows Admin Shares [16].

- **Command and Control**
  - **T1071** : *Application Layer Protocol* - Utilisation de Beacon SMB *via* Cobalt Strike [16].

- **Exfiltration**
  - **T1567.002** : *Exfiltration to Cloud Storage* - Exfiltration des données, principalement à l'aide de RClone [16].

- **Impact**
  - **T1486** : *Data Encrypted for Impact* - Le chiffrement des données constitue l'objectif principal des opérateurs d'Egregor [11].
  - **T1490** : *Inhibit System Recovery* - Les copies cachées Windows sont supprimées [11].

7 Recommandations

Afin de se prémunir et de bien réagir contre ce type d'attaque l'ANSSI recommande de se référer au guide *Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident?*.

Pour réduire le risque d'attaque par rançongiciels, et notamment par Egregor :

- sauvegarder les données régulièrement, déplacer physiquement la sauvegarde de votre réseau et la placer en lieu sûr tout en s'assurant qu'elle fonctionne ;
- être en mesure de détecter et bloquer l'utilisation de Cobalt Strike sur le réseau ;
- être particulièrement vigilant sur les connections RDP ainsi que sur l'utilisation de BITS, wmic et PowerShell sur le réseau ;
- maintenir à jour les logiciels et systèmes. Une attention particulière doit être portée aux solutions VPN et à leurs mises à jour afin de permettre l'accès à distance de vos employés ;
- si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera la propagation des rançongiciels *via* les vulnérabilités des applications ;
- chiffrer les documents sensibles sur votre réseau afin de prévenir une éventuelle divulgation de ces documents [17] ;
- utiliser et maintenir à jour les logiciels antivirus ;
- cloisonner le système d'information ;
- limiter les droits des utilisateurs et autorisations des applications ;
- si possible, ne pas exposer les services de bureau à distance (comme le RDP) sur des réseaux publics et utiliser des mots de passe complexes sur ces services ;
- maîtriser les accès Internet ;
- mettre en œuvre une supervision des journaux ;
- sensibiliser les collaborateurs ;
- évaluer l'opportunité de souscrire à une assurance cyber ;
- mettre en œuvre un plan de réponse aux cyberattaques ;
- penser sa stratégie de communication de crise cyber.

Les conseils de l'ANSSI pour bien réagir en cas d'attaque :

- s'assurer que les attaquants ne se sont pas latéralisés en cas de détection de Qakbot, Ursnif ou IcedID sur le réseau ;
- piloter la gestion de la crise cyber ;
- trouver de l'assistance technique ;
- déconnecter immédiatement les machines du réseau sans en supprimer les données ;
- communiquer au juste niveau ;
- ne pas payer la rançon ;
- déposer plainte ;
- restaurer les systèmes depuis des sources saines.

8 Bibliographie

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

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

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

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

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

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

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

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

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

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

[11] lauren-place. *Egregor : The New Ransomware Variant to Watch | Digital Shadows*. 24 nov. 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 !” 11 nov. 2020. In : (11 nov. 2020).

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

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

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

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

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

1.0 - 11/12/2020

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