Découvrez la face cachée de « Maze »

LE RAPPORT D'INVESTIGATION ET L'ANALYSE D'UN RANÇONGICIEL ET DE SON MODÈLE D'AFFAIRES VUS DE L'INTÉRIEUR.

BANCAL DAMIEN

Date : 2020-03-05

Ce qu'il faut savoir avant de commencer…

Les pertes de production liées aux rançongiciels coûtent aux organisations plus de 64 000 dollars US en moyenne par attaque. (Source : Coveware). Les rançongiciels coûtent aux entreprises plus de 75 milliards de dollars US par an. (Source : Datto). Nous avons tous lu, relu et parfois même été victimes de cyberattaques se transformant en cyber-extorsions. Ces statistiques fleurissent depuis 2014 sur le web et chaque année est une année record. Nous avons banalisé ces chiffres, ils font partie de notre quotidien. Les entreprises pensent comprendre de mieux en mieux comment ils impactent leurs modèles d'affaires, mais ce dossier vous montrera l'envers du décor et l'ampleur du cycle de vie de la victimisation.

Nous oublions trop souvent que cette menace évolue pour continuer à nous prendre par surprise. Cette menace a une intelligence propre et multiple, un modèle d'affaires bien « huilé », tel un engin dédié à la compétition, forgé pour la performance et l'efficacité. Nous occultons trop souvent la compréhension de ces organisations criminelles pour simplement les désigner par un « grand tout » : « ils », « les hackers », « les pirates » … Mais ce sont des industries à part entière en quête d'innovation, de parts de marché, d'efficacité et en perpétuel amélioration de processus.

L'entreprise The 8Brains se spécialise dans l'analyse de ces épiphénomènes pour donner aux organisations la compréhension et les tendances de cybersécurité à observer, afin de les aider à aiguiser leur stratégie de cyberdéfense, à améliorer leur posture de cyber-résilience et à éduquer leurs équipes. L'objectif a pour but de mieux appréhender et mieux répondre à ces menaces pour être préparés à une éventuelle cybercrise.

Dans ce dossier, nous revenons sur la menace appelée « Maze » pour vous faire découvrir l'une de ses faces cachées, directement en lien avec le modèle d'affaires que les cybercriminels ont envisagé pour améliorer leur rentabilité et leur impact sur leurs victimes.

Revenons un peu sur nos pas. Novembre 2013, un cryptolocker touche de multiples ordinateurs de la police de la ville de Swansea dans le Massachusetts (1). A l'époque, le code malveillant ou rançongiciel réclame 750 dollars US pour déchiffrer les contenus pris en otage. C'était l'un des premiers cas de rançongiciel rendus publics (2). En sept ans, les logiciels de rançonnage sont devenus les nouveaux outils indispensables dans l'arsenal des pirates informatiques. Parmi eux, l'un des plus récent le ransomware « Maze ». Depuis mai 2019, ce « kit pirate » provoque de nombreux dégâts dans les entreprises impactées. Avec plusieurs centaines de victimes, les cybercriminels, que nous appellerons « opérateurs » derrière Maze ont mis en place une structure de chantage numérique qui offre la possibilité de collecter, selon les autorités américaines, plusieurs millions de dollars par mois. Le Pôle Cyber Intelligence de The 8Brains vous propose son analyse liée à cette opération de cyber attaque d'envergure. Elle reprend les informations diffusées par Maze sur les différents sites que cette organisation cybercriminelle administre (News 1, News 2, News 3 ainsi que sur des forums pirates et via des conversations de cybercriminels auxquelles The 8Brains a pu avoir accès).

Table des matières

ANALYSE **4**

1. Le cycle d'affaire de Maze 5
2. Le fonctionnement global de Maze 7
3. Les victimes de Maze 8
4. Les ouils e-business qui composent Maze 10
   - 4.1. Le RaaS ou « tableau de bord infonuagique cybercriminel » 10
   - 4.2. Les espaces de communication entre cybercriminels et victimes 11
   - 4.3. Les espace de diffusions et de publications des données volées 15
5. L'organisation criminelle et sa logique 16
6. Comment se protéger? Notre top#15 des recommandations 19

RÉFÉRENCES & BIBLIOGRAPHIE **22**

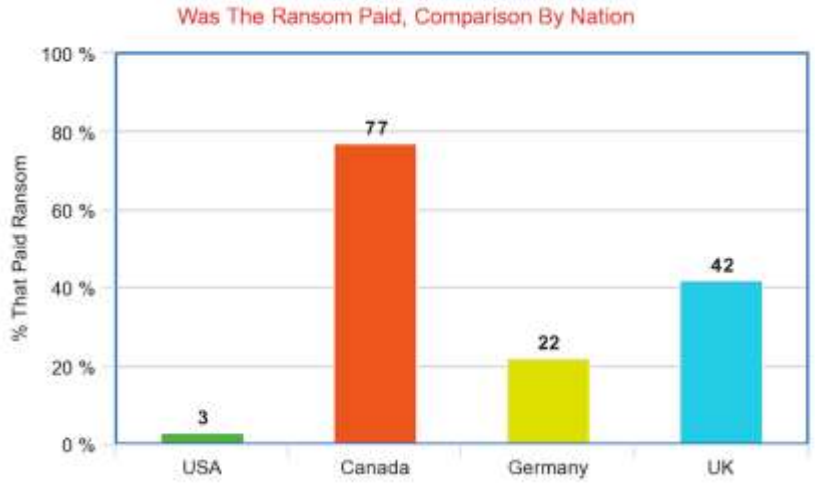
ANALYSE

8brains Canada Ltée
442 rue St Gabriel, #002
Montréal, QC, H2Y 2Z9
+1 (514) 798-9196
contact@8brains.ca

1. Le cycle d'affaire de Maze

Maze est un logiciel pirate destiné à la prise d'otage d'un ou plusieurs systèmes informatiques, et de leurs fichiers. Il est commercialisé dans plusieurs blackmarkets russes sous forme de location. Un service malveillant infonuagique pour pirates de type « Ransomware-As-A-Service ». Il permet aux pirates qui l'opèrent d'exploiter la boite à outil complète fournie avec le rançongiciel lors de l'infiltration des systèmes. Tout comme d'autres logiciels de ce type (Dharma, GandCrab, Sodinokibi, …), Maze offre un grand nombre d'options pour les opérateurs souhaitant l'utiliser : chiffrer, converser avec les « clients » et commercialiser la clé de déchiffrement. C'est littéralement un outil « clefs-en-main » pour développer son modèle d'affaire cybercriminel.

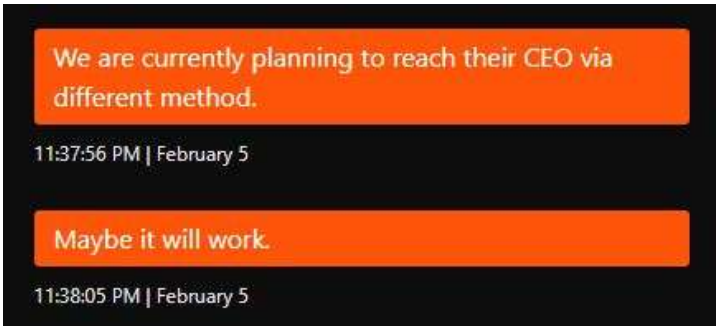
En plus de chiffrer les informations dans le but d'obtenir un paiement sous forme de rançon pour permettre à la victime de récupérer les données prises en otage, ce type de rançongiciel est utilisé par ses opérateurs dans une seconde vague de chantage appelée communément dans le jargon de la cyberdéfense : le « Double-Dip ». La pratique du « Double Dip » s'est beaucoup répandue récemment, et ce surtout au Canada, via deux phénomènes : le paiement trop rapide et facile des victimes, mais aussi la revente des « dossiers » des victimes entre organisations cyber-criminelles.



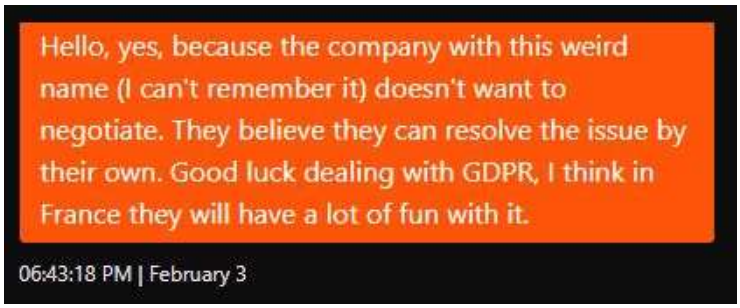
Source : Phoenixnap 2019

L'une des questions la plus fréquemment posée par les victimes lors des investigations menées par les équipes de The 8Brains : « Que se passe-t-il du côté des cybercriminels si l'entreprise ciblée est capable de récupérer ses informations par le biais de sauvegardes ? ». Beaucoup de départements informatiques des victimes pensent, à tort, que « la partie est gagnée » s'ils peuvent restaurer les fichiers à partir des sauvegardes et que les cybercriminels n'auront pas gains de cause. Cependant nous avons constaté que même dans ce type de cas, les opérateurs de Maze contactent les directions des entreprises victimes afin de les menacer et les faire chanter une seconde fois.

En un exemple de discussion entre opérateurs Maze :



Dans ce second cycle malveillant, les pirates réclament de l'argent pour ne pas divulguer les informations qu'ils ont collectées avant le chiffrement des données. Les opérateurs de Maze n'hésitent pas à actionner le levier lié au Règlement Général des Données Personnelles (RGPD/GDPR) afin d'inciter leurs victimes à payer.



En effet, en plus du chiffrement des systèmes et de leurs données, s'ajoute la fuite d'informations pouvant être très sensibles, comme des fiches de Ressources humaines (données privées et photographies des employés, des familles, des fiches de paie, des Numéros d'Assurance Sociale ou de comptes bancaires, etc.), des documents internes et liés aux affaires (factures, données bancaires, contrats, etc.)

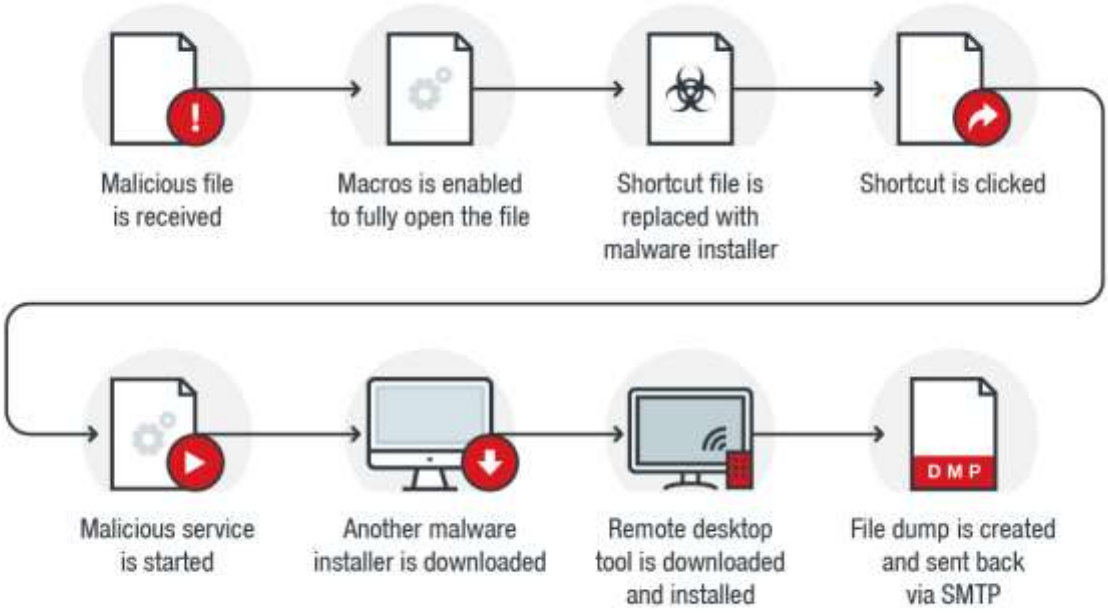
Cette pratique, devenue courante au travers des rançongiciels récents (2018) s'appelle « attaque à agendas multiples ». Cette méthode a été démocratisée depuis l'apparition d'AnglerJS, qui avant de se révéler comme rançongiciel, dérobe d'abord de façon furtive les identifiants et mots de passe de la machine infectée :

En 2020, il est donc hautement peu probable qu'une victime d'un rançongiciel n'aie pas eu de données dérobées et ne soit pas ciblée rapidement par une deuxième, voir une troisième vague de rançonnage : « Payer n'assure pas la paix aux victimes ! Ce n'est au contraire que le début » puisqu'une victime qui paie est une victime rentable et donc, idéale.

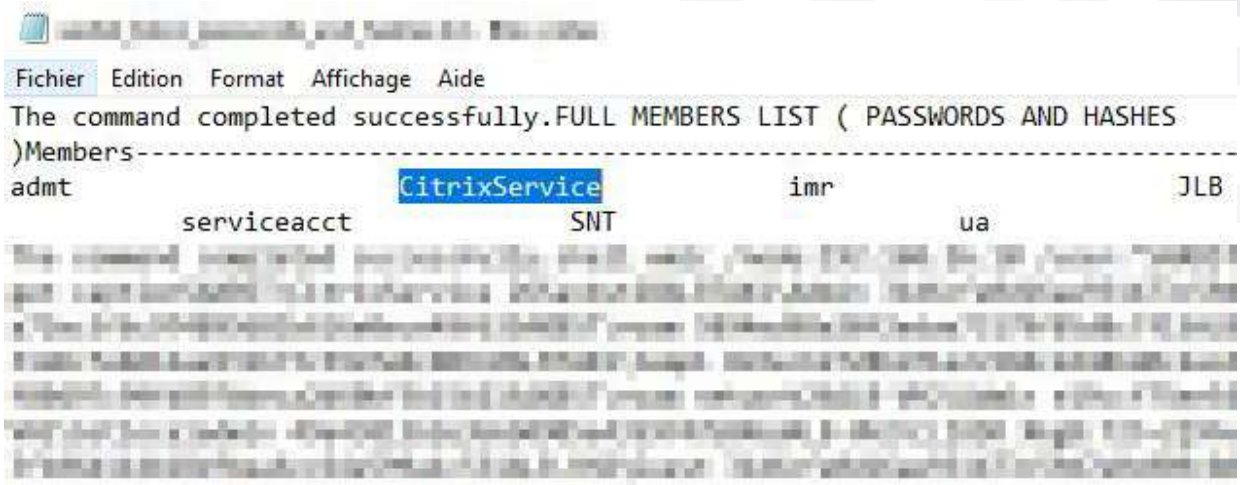
2. Le fonctionnement global de Maze

Selon les informations de The 8Brains et de nombreux experts de par le monde (3), les méthodes employées par Maze et consort sont les suivantes :

- Phishing ;
- Injection de code malveillant dans le système infiltré via un fichier Doc, Excel ou PDF piégé par exemple ;
- Utilisation de failles applicatives récentes (Citrix, SharePoint, Flash, IE, Chrome …) ;
- Redirection vers de faux sites web.



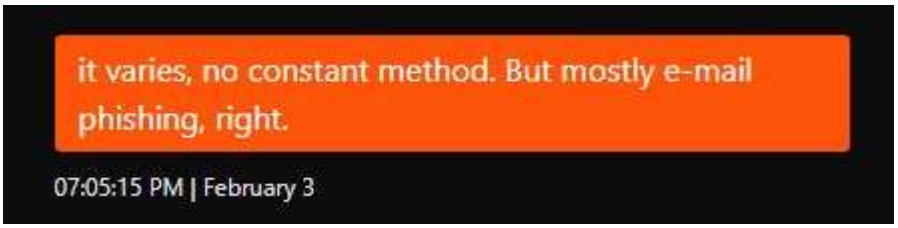
Source : Trendmicro



Document diffusé par Maze

Les opérateurs de Maze sont évidemment peu prolixes sur leurs méthodes, mais nous avons cependant pu découvrir qu'ils ont une prédilection pour les infiltrations par le biais de courriels piégés et faux sites d'hameçonnage. La raison est simple : efficacité et rentabilité maximisées. La cyberattaque débutée via un courriel permet une campagne de masse à faible coût et la validation de cibles faciles. En effet, un courriel ayant réussi sa percée laisse présager d'une victime peu protégée car toujours vulnérable à un modèle d'attaque existant depuis plus d'une décennie.

La victime est considérée comme très accessible par les cybercriminels : beaucoup d'employés et peu de sensibilisation à la cybersécurité ou petite structure et peu de solutions de cyberdéfense en place.

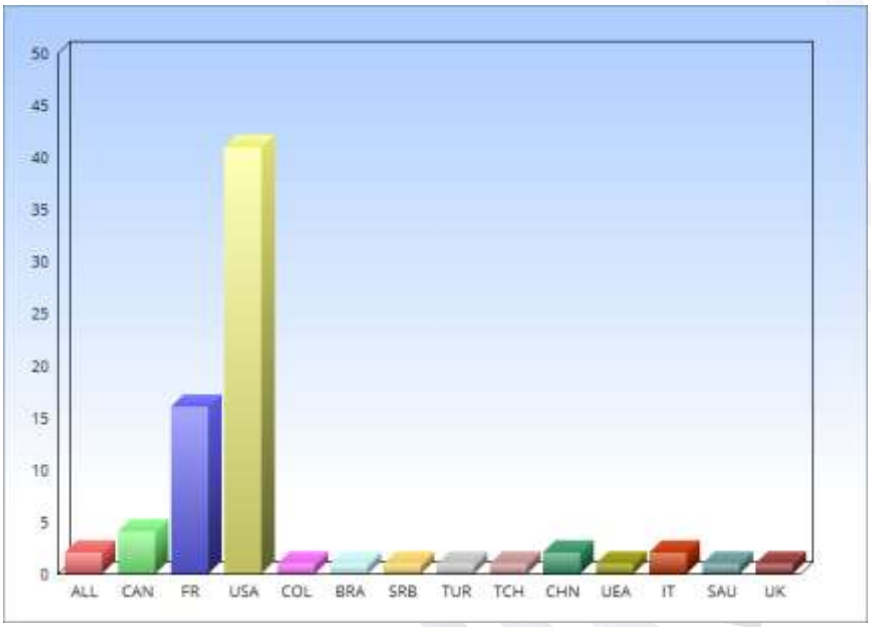


Une fois l'infiltration réussie (4), les opérateurs de Maze visitent et copient le maximum de données qu'ils peuvent rencontrer. Cette infiltration peut durer de plusieurs jours à plusieurs semaines. Cette phase est donc volontairement furtive et n'a pour seul objectif que de voler un maximum de données sans éveiller les soupçons de la victime.

Une fois la collecte terminée, ils orchestrent la seconde partie de leur attaque : le chiffrement des systèmes et des fichiers de leur victime. Un fichier texte baptisé « DECRYPT-FILES.txt » signe l'infiltration et la prise d'otage. Ce fichier permet la prise de contact entre les pirates et les victimes. Chaque victime possède son numéro de « client » unique.

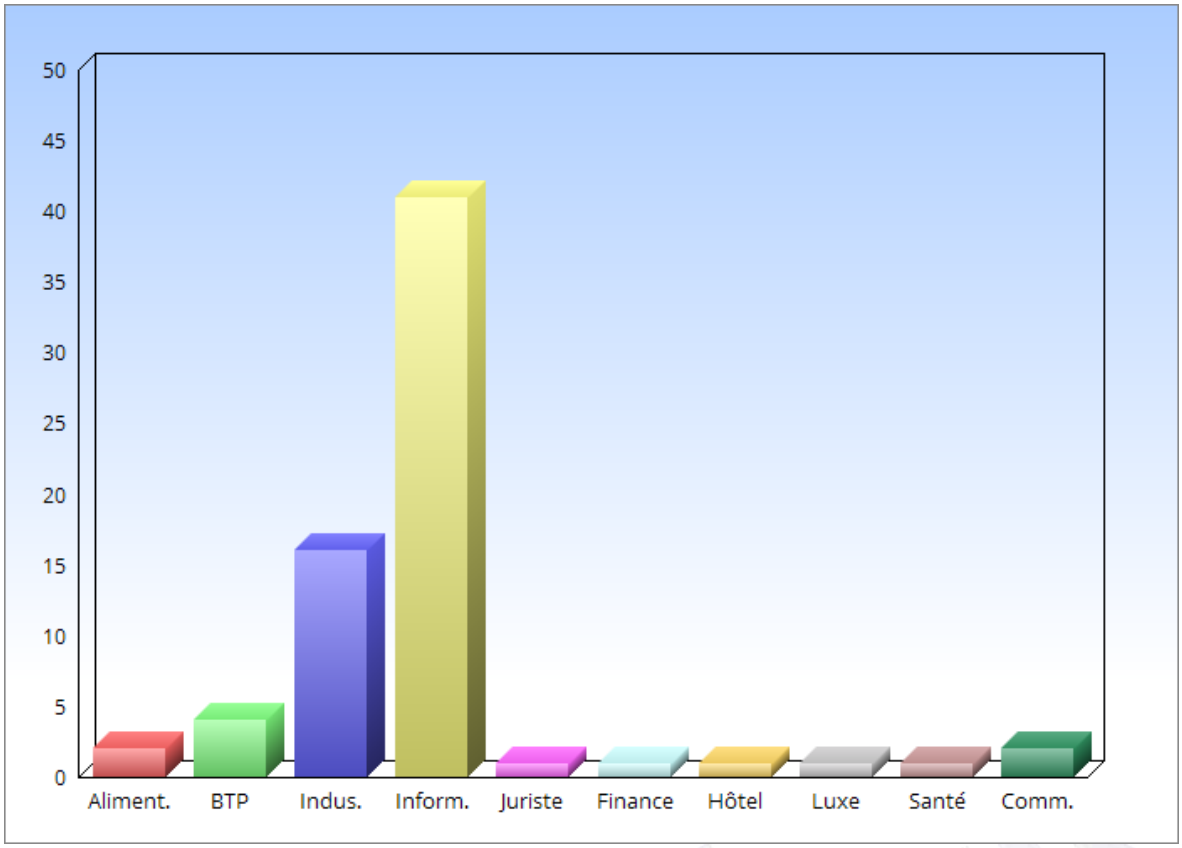
3. Les victimes de Maze

Il est impossible de connaitre le chiffre exact des entreprises impactées par le ransomware Maze dans sa première instance de rançonnage. Cependant, en ce qui concerne la seconde phase de chantage, The 8Brains a pu analyser 75 cas, la grande majorité concernant des entreprises nord-américaines.



8brains Canada Ltée
442 rue St Gabriel, #002
Montréal, QC, H2Y 2Z9
+1 (514) 798-9196
contact@8brains.ca

Nous avons cherché à comprendre si des secteurs d'affaires étaient plus touchés que d'autres. Cependant Maze ne semble pas cibler directement des entreprises particulières. C'est l'analyse des données volées qui permet aux opérateurs de Maze de tirer le fil les amenant vers de nouvelles victimes. Une méthode qui apparait clairement dans leurs vagues visant, une fois le secteur de la santé, une autre fois le secteur de la construction et de l'ingénierie (Berry Companies, BIRD, Bouygues Construction, Condie Construction Compagny, Massey Service), ou encore le secteur industriel lourd (Bilton, Continental NH3, DV Group , Einhell, Electricaribe, Grec Auto, Groupe Europe Handling, Johnson Air Products, LOC Group compagnies, NMF Filter, North American Roofing, Prudential Overall Supply, Ramtek, Southwire, Talon Logistics, Vernay) et de l'hôtellerie.



Ces secteurs sont malheureusement connus pour abriter des PMEs ou des grandes organisations à écosystèmes informatiques multiples et inégaux comportant de la donnée confidentielle, compétitive ou privée.

En cas de non-paiement de la somme réclamée, les pirates orchestrent la troisième partie de leur chantage : la demande de rançon afin d'éviter la divulgation publique des données volées.

Le montant des rançons est très fluctuant allant de 500 à 5 000 dollars US par machine infectée (7). Nous suspectons des rançons potentiellement plus élevées dans des cas particuliers en fonction, évidemment, du volume de systèmes infectés, mais surtout de la sensibilité des systèmes et des données chiffrées. L'Agence Nationale de Sécurité des Systèmes d'Information Française – ANSSI (5) indique que les cybercriminels s'appliquent à se déployer manuellement au sein du réseau victime afin de rester discrets et d'atteindre les ressources identifiées comme clés, maximisant ainsi l'impact de l'attaque.

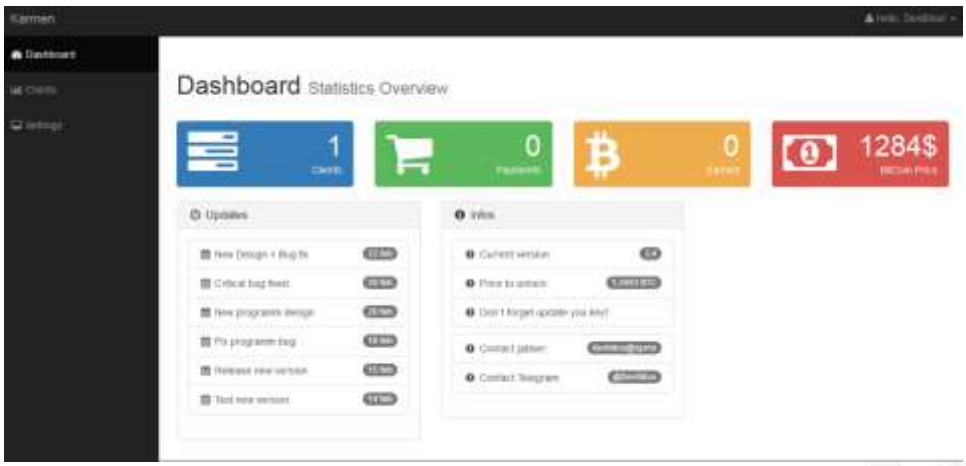
Les opérateurs de Maze ne semblent pas approfondir leur recherche sur les cibles comme l'a prouvé le cas « Internet Routing Registry ». Annoncée comme infiltrée depuis le 23 février 2020, il s'avére que le serveur infiltré n'appartient pas au IRR mais à un ancien partenaire.

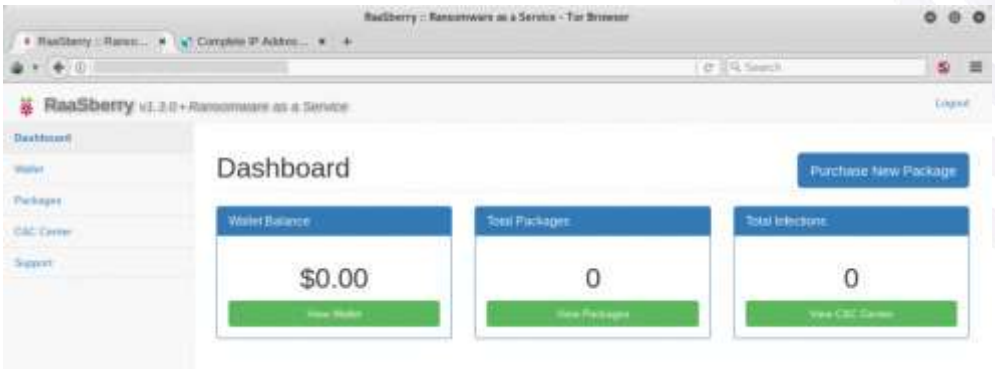
4. Les ouils e-business qui composent Maze

On perçoit souvent les cybercriminels comme des prédateurs solitaires cachés dans leur garage, mais en 2020, cette image est très loin de la vérité. Comme n'importe quelle organisation, les cybercriminels ont développé et mis en place des stratégies d'attaque du marché, de développement, de protection de leurs infrastructures et des outils de suivi de leurs performances leur permettant de mieux gérer leurs « campagnes ».

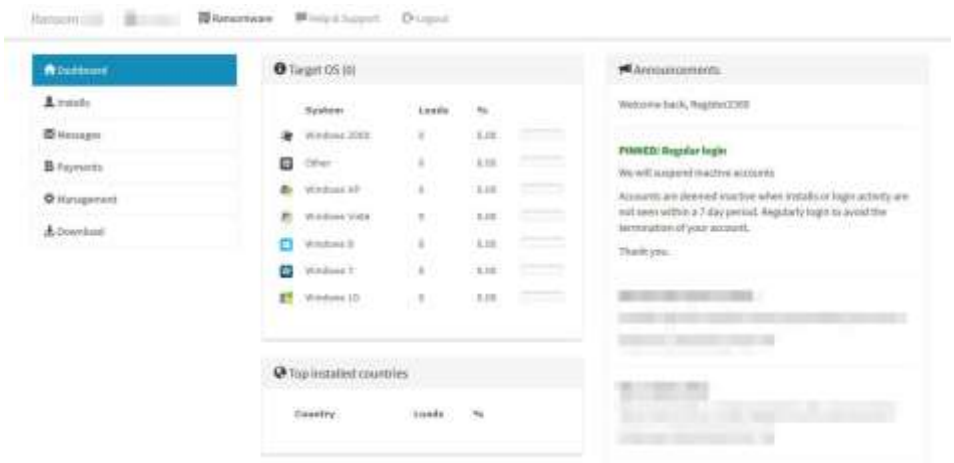
4.1. Le RaaS ou « tableau de bord infonuagique cybercriminel »

L'outil Maze, se compose de plusieurs parties. D'abord le ransomware et son tableau de bord de rentabilité des campagnes. Il en existe plusieurs, en voici trois exemples dont « Karmen » et « RaaSberry » :

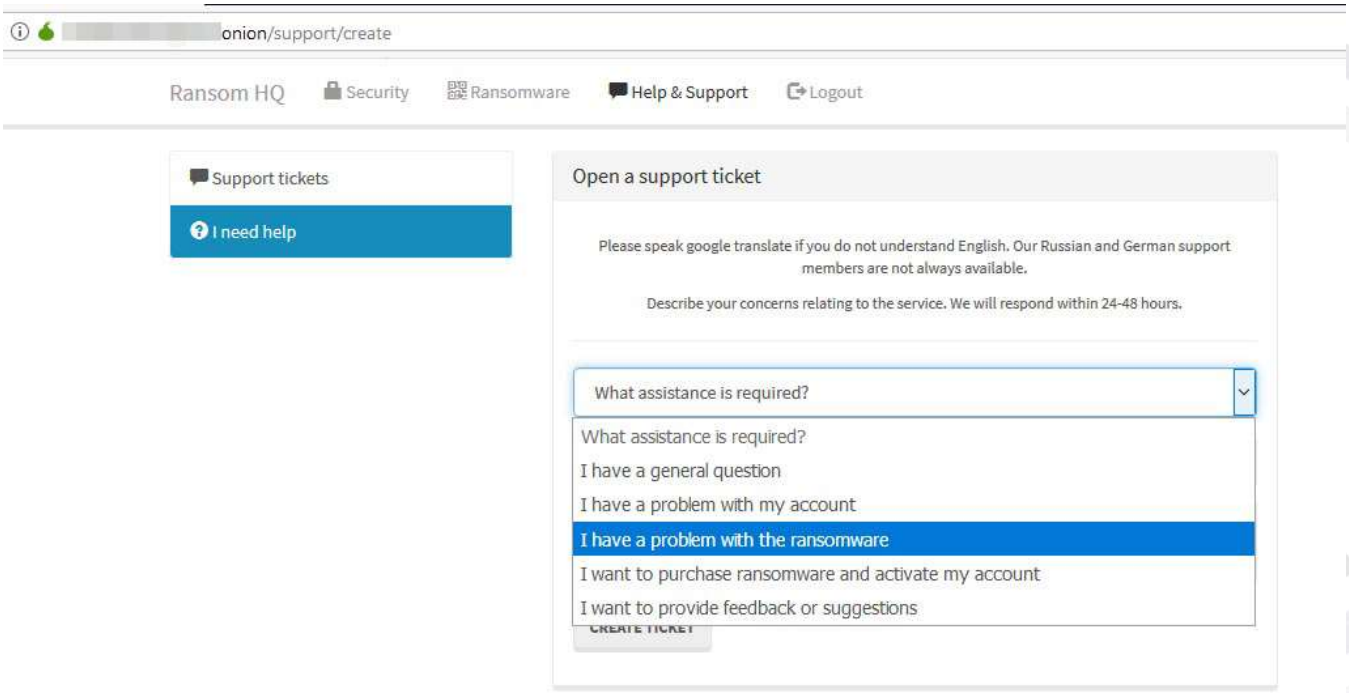




8brains Canada Ltée
442 rue St Gabriel, #002
Montréal, QC, H2Y 2Z9
+1 (514) 798-9196
contact@8brains.ca



Ces outils ne sont pas spécifiques à Maze, les outils d'exploitation et de gestion de campagne cybercriminels sont maintenant très connus et ont fait l'objet de plusieurs analyses que nous vous recommandons vivement de consulter (6).



Nous allons nous pencher sur la seconde phase de cette cyber-attaque. Cette seconde phase correspond aux outils de communication/marketing.

4.2. Les espaces de communication entre cybercriminels et victimes

Maze propose plusieurs vecteurs de communication. Ils sont tous mis en place pour entrer en relation avec leur client-victime. Leur mission : aider au paiement ; proposer des réductions ; infliger des « amendes » ; fournir des preuves ; accentuer la pression, l'angoisse et l'urgence d'agir.

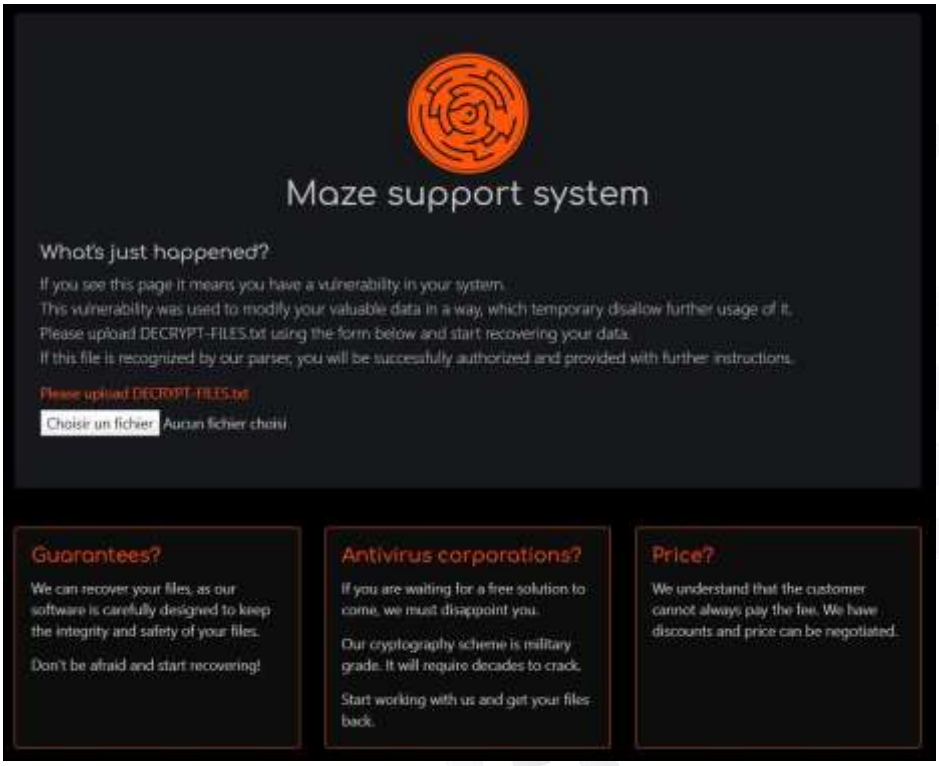
Ils proposent :

- Deux espaces de contact pour les victimes (Web et Darknet via Tor) : *mazedecrypt.top*;
- Trois sites web diffuseurs des informations volées : *News 1, News 2 et News 3* ;
- Des courriels : *yourrealdecrypt@airmail.cc; filedecryptor@nuke.africa; koreadec@tutanota.com; Fastrecovery@airmail.cc; decryptmaze@airmail.cc* … A noter que cette dernière adresse a aussi été exploitée dans la diffusion du rançcongiciel Gandcrab (11) qui s'attaque particulièrement aux entreprises situées en Inde.
- Tchat
- Forums pirates

Une fois les machines et les fichiers pris en otage, Maze propose aux victimes (Maze les nomme : clients) un espace numérique baptisé *mazedecrypt.top*.

Cette page affiche un avertissement à destination du visiteur « *Qu'est-ce qui vient de se passer ? Si vous voyez cette page, cela signifie que vous avez une vulnérabilité dans votre système. Cette vulnérabilité a été utilisée pour modifier vos précieuses données d'une manière qui empêche temporairement leur utilisation ultérieure.* »

A partir de cet espace, il est proposé à la victime de fournir le fichier texte « decrypt-files.txt ». Un fichier sauvegardé dans l'ensemble des dossiers et machines pris en otage. Il contient la signature unique permettant d'identifier « le client ».

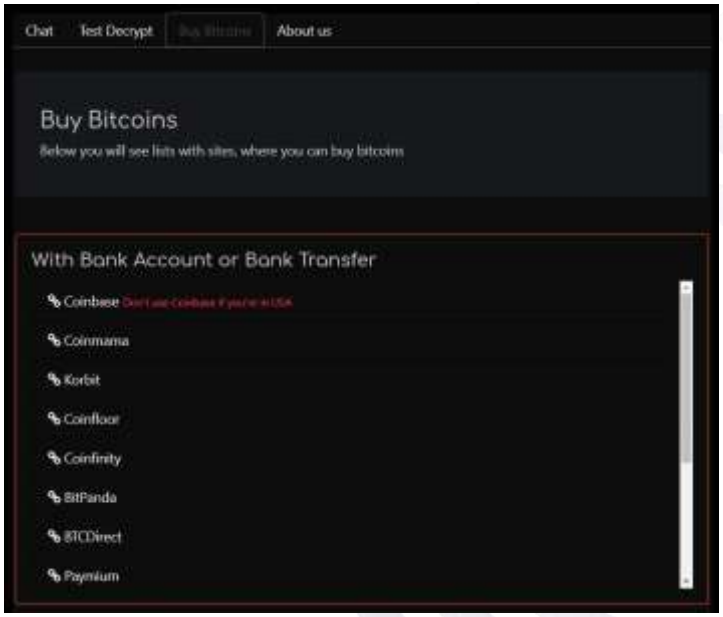


Cet espace indique « fournir des garanties » : « *Nous pouvons récupérer vos fichiers, car notre logiciel est soigneusement conçu pour préserver l'intégrité et la sécurité de vos fichiers. N'ayez pas peur et commencez à récupérer! […] Si vous attendez une solution gratuite, nous devons vous décevoir. Notre schéma de cryptographie est de qualité*

militaire. Il faudra des décennies pour le fissurer. Commencez à travailler avec nous et récupérez vos fichiers. Nous comprenons que le client ne peut pas toujours payer les frais. Nous avons des remises et le prix peut être négocié. »

Une fois le fichier transmis, la page « Decrypt » propose de communiquer trois documents chiffrés via un formulaire dédié. Une proposition permettant à Maze de confirmer sa main mise sur le déchiffrement. « *Nous fournissons 3 décryptages tests, pour prouver que nous pouvons récupérer vos fichiers […] Nous ne décryptons gratuitement que les fichiers d'images, car ils n'ont aucune valeur significative pour vous.* »

Ensuite, un espace « commercial » qui explique comment payer en offrant liens et commentaires sur toutes les plateformes permettant d'acquérir de la crypto monnaie. Maze se fait payer en Bitcoins. Selon nos informations, plus d'une vingtaine d'entreprises ont payé le silence. Impossible de connaître le nombre réel de victimes avant la seconde phase de Maze.

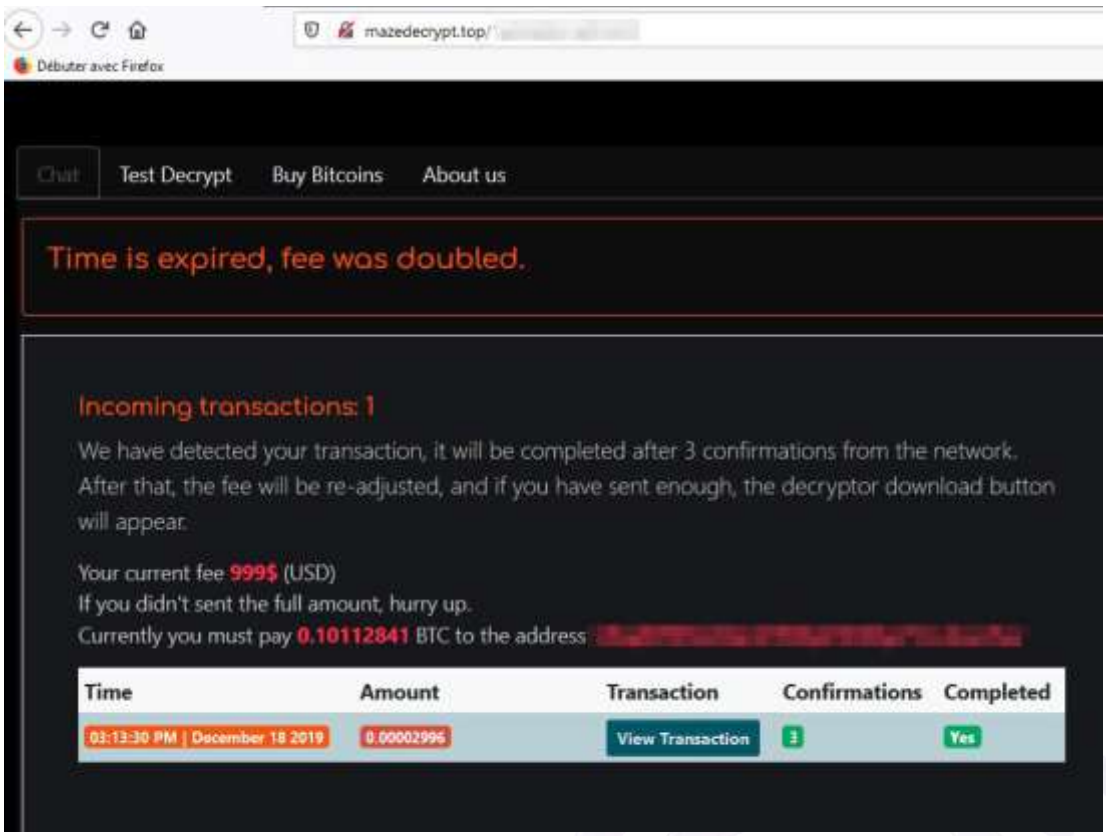


Un troisième espace « About Us » affiche des articles de presse revenant sur les actions de Maze.

Enfin, le dernier accès est un espace de discussion qui permet aux victimes de converser avec leurs ravisseurs.

C'est par ce biais que nous avons pu rentrer en relation avec Maze lors de nos cyber-investigations.

Il est intéressant de noter que les victimes peuvent se retrouver bannies de ces espaces de discussion pour divers motifs : agressivité du client, tentative d'ingénierie sociale, ou pire un bannissement qui multiplie par deux le prix de la rançon !



« *Vous devez vous dépêcher car votre réduction de 50 % expirera lorsque le compteur en haut de cette page atteindra zéro. Si vous ne payez pas avant ce moment, les frais seront augmentés de 2 fois (doublés), donc si c'était 2400 USD, ils deviendront 4800 USD. Vous pouvez envoyer l'argent par morceaux (parties), les frais seront recalculés à chaque transaction réussie. La transaction sera terminée après 3 confirmations du réseau.* »

4.3. Les espace de diffusions et de publications des données volées

Les pirates n'hésitent pas à diffuser des « échantillons » d'informations dérobées dans des espaces publics en cas de fin de non-recevoir ou de silence persistant des victimes. Cette diffusion se fait via plusieurs espaces web que nous avons baptisés News 1, News 2 et News 3.

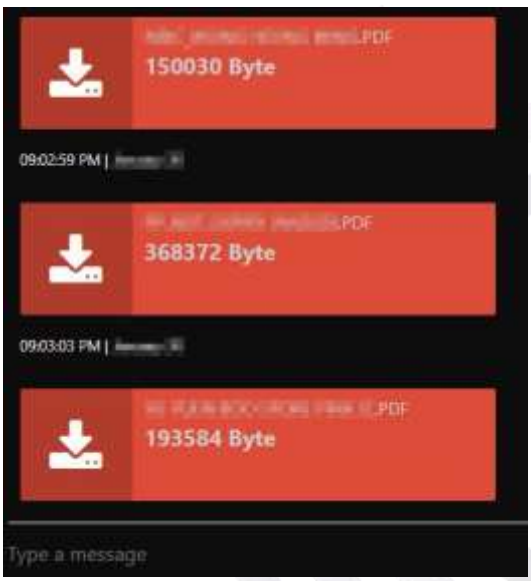
D'abord sous forme « d'échantillons ». Mission, convaincre l'entreprise piégée de payer.

Certains fichiers diffusés sont protégés par mot de passe (Berretta, Bouygue Construction, …)

Maze communique le mot de passe aux « clients ».

L'entreprise ne paie pas ? Maze diffuse l'intégralité des informations volées.

Les opérateurs de Maze diffusent également des preuves via le tchat qu'ils mettent en place avec les victimes comme le montre l'exemple ci-dessous, des données privées et personnelles des employés d'une importante entreprise internationale.



5. L'organisation criminelle et sa logique

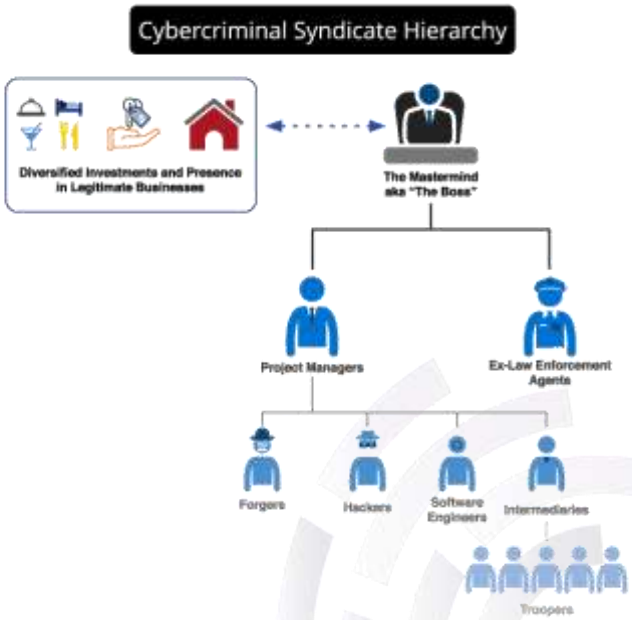
Il est certes difficile de parler d'humanité à la lecture des exactions de Maze. Cependant, les équipes de The 8Brains ont pu identifier les humains et leur rôle au sein de leur microcosme. Selon nos différentes investigations, nous pouvons confirmer la présence d'au moins trois individus. Nous les avons classés comme suit :

- Le gestionnaire ;
- Le développeur ;
- L'opérateur ;

Le gestionnaire gère les sites web et les fichiers ; le développeur se charge des opérations techniques à l'encontre des entreprises et des sites web ; l'opérateur est à la commande du site web et du tchat « Decrypt ».

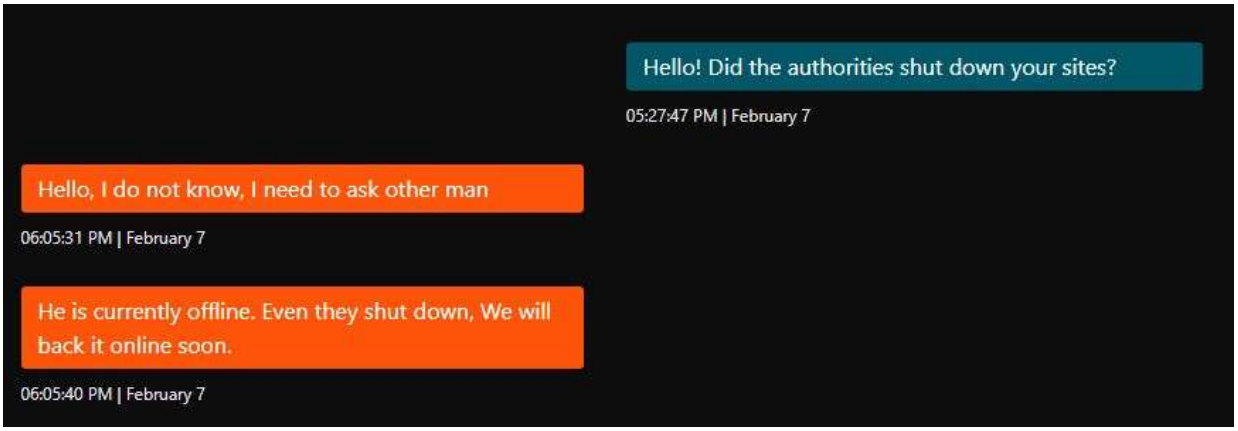
Seulement trois personnes ? Nous nous basons sur les propos tenus par le/les individus rencontrés. Sachant que Maze est un outil qui se loue, à cela doit se rajouter les intermédiaires qui lancent les cyber-attaques ; blanchissent l'argent (les « e-Mules » ou « Troopers ») … Une même structure qui peut être tenue par une seule personne.

Il est très commun de voir ces organisations cybercriminelles hiérarchisées et segmentées en fonction des besoins d'affaires comme le sont les entreprises légitimes. En voici un exemple :



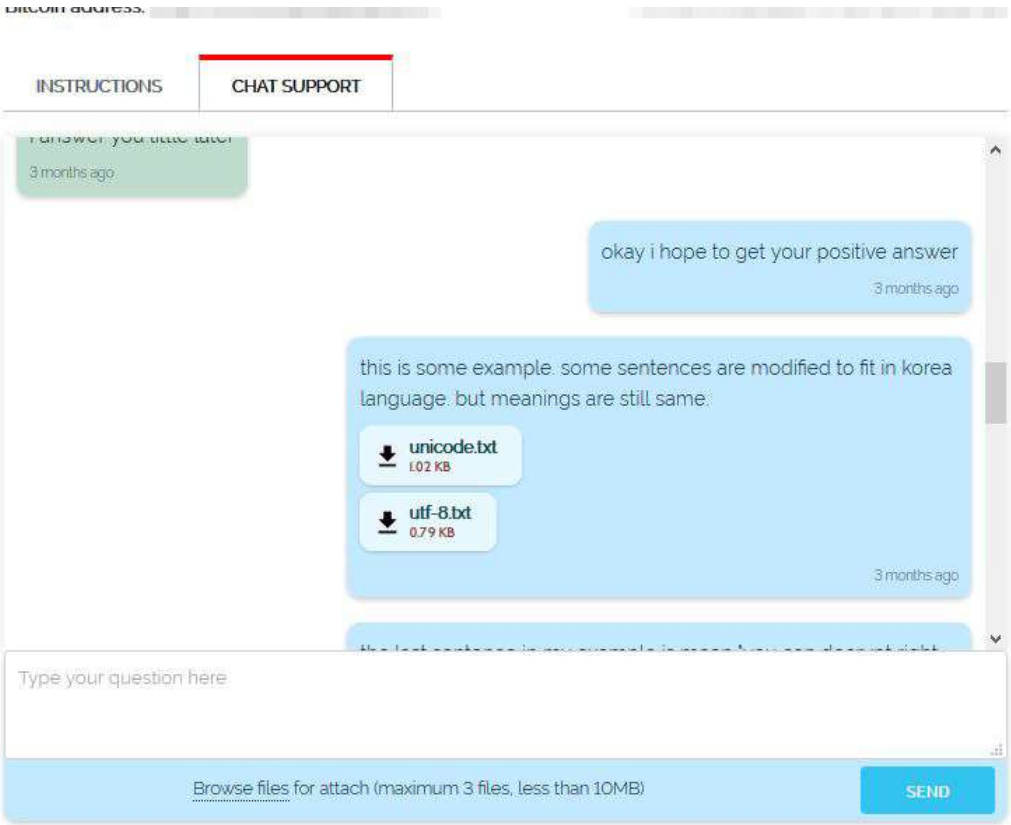
Source : RecordedFuture

Lors de la fermeture du site « public » de Maze, en décembre 2019, par les autorités américaines et irlandaise à la suite de la plainte auprès du département de la justice US par l'industriel Southwire (8), l'opérateur a indiqué demander à une « autre personne la date de retour du portail « public », ce qui laisse présager une plus grande organisation.



Comme nous l'avons expliqué précédemment : les créateurs de Maze ont mis en place plusieurs sites « publics » que nous avons baptisés News 1, News 2 et News 3. Des espaces web leur permettant d'annoncer la liste des « clients » récalcitrants. Des pages qui affichent les noms des entreprises victimes, les machines impactées, la taille des disques durs, le poids des fichiers chiffrés et des exemples de documents volés. Une méthode éprouvée par un autre « Ransomware-As-A-Service », Sodinokibi.

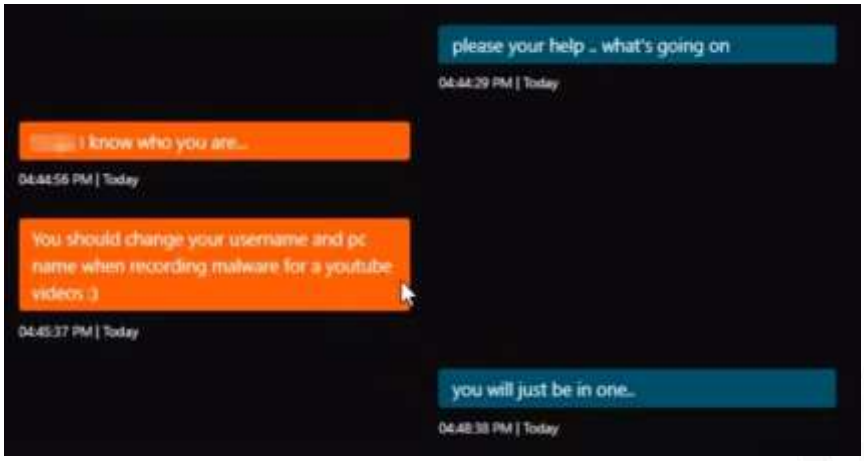
Le tchat permet aux opérateurs de Maze de prendre contact et de « commercialiser » leur service. Lors d'une discussion que nous avons pu intercepter entre Sodinokibi et une victime (ci-dessous), un « employé » d'une entreprise ciblée proposait ses services de traduction à Maze. L'opérateur a précisé en référer au développeur.



```
Your computer has been infected!
당신의 컴퓨터는 랜섬웨어에 감염되었습니다!

Your documents, photos, databases and other important files encrypted
당신의 문서와 사진, 그리고 자료들과 다른 중요한 파일들이 모두 암호화되었습니다.

To decrypt your files you need to buy our special software - ly8haaw32-Decryptor
당신의 파일들을 원래대로 복구하려면 저희의 특별한 복구툴인 ly8haaw32-Decryptor를 구매하셔야 합니다.

You can do it right now. Follow the instructions below. But remember that you do not have much time
당신은 지금 당장 복구할 수 있습니다, 하단의 설명만 잘 따라주신다면 말이죠. 그러나 기억하세요. 당신은 시간이 얼마 남지 않았을걸요?
```

La proposition d'un « employé » d'une entreprise victime

Les opérateurs de Maze bannissent rapidement les discussions qu'ils considèrent comme stériles à leurs affaires. Un bannissement qui double le montant réclamé pour déchiffrer les informations. La discussion peut reprendre après un premier versement.



Maze diffuse des informations personnelles pour « convaincre » le client !

Le second espace (9), un site web public qui évolue avec le temps. Il n'est pas rare de voir disparaitre des noms de sociétés. Selon Maze, elles auraient payé.

Pas d'idéologie ; de règle ; de tactique ou de pitié. Leurs propos concernant les employés et leurs familles impactées sont souvent sans concession : « *They did. They did bad security at least. If they did really nothing, then they can be blamed for something other in their life. There is no people without sins, without bad thoughts among all of those who live the regular life. People without sins are usually either praying or mediating in Monastery or sitting in samadhi somewhere in Indian cave. They are not our victims. So don't say that we hurt people who haven't done anything :) […] Families. If we destroyed someone family it was a bad family, wasn' it? If someone's family is still alive, then it is a good family and love in it's much stronger now. What is the problem about families? Or are you talking about the children who probably could grow up without money? Is it really bad? Why should they be "Top notch", just because they were born in the western country? Elon Musk were born in south africa. I can bet if he were born in US he wouldn't become a businessman. Sometime problems are the way to become something greater.* »

Ce type de cyber-attaque est à tranchants multiples. En plus d'avoir mis à mal l'infrastructure de l'entreprise, les données volées sont perdues. Rien ne confirme la destruction des informations copiées après le paiement de la rançon réclamée, comme l'indique le FBI.

Il faut même s'attendre à d'énièmes phases de monétisation par revente des dossiers « clients » ou victimes, incluant les données volées, à d'autres organisations cybercriminelles dans le but de perpétrer d'autres types d'attaques via ingénierie sociale, par exemple, ou de cyber-extorsions connexes liées aux données volées auprès des clients ou partenaires concernés par le contenu des données dérobées à la première victime.

Ce type de cyber prise d'otage peut impacter toute une chaîne de production des entreprises sous-traitantes (supply chain attack) pouvant provoquer des perturbations, voir des ruptures dans l'approvisionnement de matières premières, services, etc.

Sans oublier cette dernière étape, la divulgation d'informations internes et sous la responsabilité de l'entreprise victime, obligeant la notification légale auprès des instances gouvernementales, des clients, des employés et des partenaires économiques.

6. Comment se protéger? Nos 15 recommandations

Évidemment, la toute première des choses est de sensibiliser vos utilisateurs à la réalité et la créativité des cybermenaces, il est important que chaque employé, chaque intervenant soit conscient des risques. Il ne s'agit pas ici de croire ou de ne pas croire en une potentielle attaque cybercriminelle, ni de se dire « je ne suis pas une cible intéressante », non, chaque entreprise est une cible potentielle. Si vous ne voyez pas la valeur de vos données, d'autres la voient très bien.

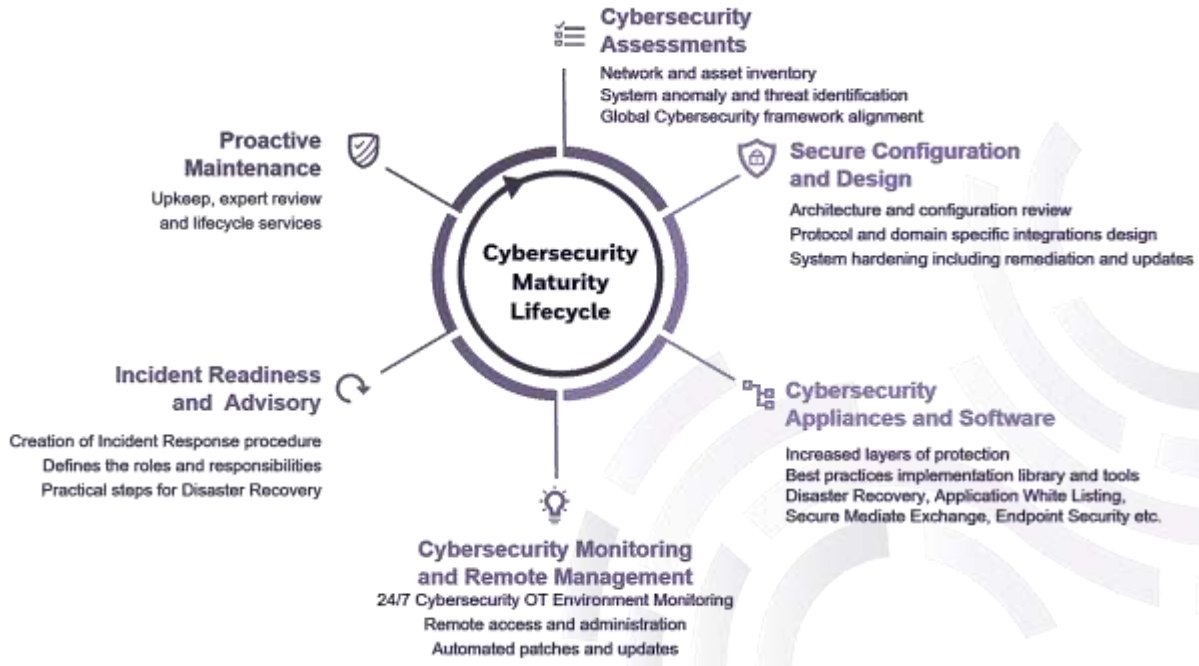
Il est important de rappeler que ce type d'attaque peut être contré, en suivant des principes simples et élémentaires de cybersécurité :

1. **Mettre à jour** l'ensemble des systèmes d'exploitation et applicatifs et limiter l'installation et l'utilisation uniquement à des applications et versions corporatives autorisées : « Application whitelisting » ;
2. **Limiter et surveiller** les accès réseaux internes depuis les espaces corporatifs publiques : « Rogue Wifi detection & NAC » ;
3. **Bannir** l'utilisation de navigateurs obsolètes et limiter l'utilisation de composants ou extensions de navigateur ; en particulier bannir l'utilisation d'Adobe Flash et forcer les mises à jour des autres composants d'Adobe ;
4. **Surveiller** les accès utilisateurs régulièrement, auditer la santé des annuaires et limiter l'utilisation directe des comptes super-utilisateurs ou privilèges équivalent : « SIEM » ;
5. **Utiliser des solutions antipourriels** récentes permettant le test, l'analyse et la réécriture des URLs et pièces jointes dans les messages ;
6. **Utiliser une solution antivirus/anti-maliciel** nouvel génération, incluant une solution anti-rançongiciel et limitater l'utilisation des ports USB (cibler en priorité les machines critiques et serveurs de fichiers) : « EDR / Next-Gen EPP » ;
7. **Autoriser la navigation uniquement** vers les sites autorisés par l'entreprise et justifiés par son modèle d'affaire : « Websites whitelisting & URL filtering » ;
8. **Marquer** les données confidentielles de l'organisation en y insérant des métadonnées spécifiques et identifiables ;
9. **Activer** l'inspection SSL au périmètre et aux points terminaux afin de détecter toute fuite de donnée via le marquage : « DLP » ;

10. **Maximiser** l'authentification à facteurs multiples sur tous les types accès à distance des données de l'organisation (RAS, Webmail, Remote storage, RDP, Remote terminals…etc.) ;
11. **Démocratise**r l'utilisation de gestionnaires de mots de passe corporatifs ;
12. **Évaluer** les données de votre organisation et celles de vos partenaires d'affaires critiques déjà dérobées et disponibles à la cybercriminalité ;
13. **Simuler** régulièrement des scénarios de cyberattaques incluant différents vols de données ainsi que l'indisponibilité de différents systèmes de l'organisation : « Purple teaming » ;
14. **Contracter** ou réviser les contrats de cyber-assurance de votre organisation afin d'aligner les garanties aux résultats et besoins identifiés par vos simulations ;
15. **Identifier** une entreprise de cyberdéfense afin qu'elle soit prête à vous aider avant, pendant et après un cyber-incident majeur, ainsi qu'à se substituer à l'organisation pour toute communication avec les cybercriminels : « BreachCoach ».

Les équipes de The 8Brains sont prêtes à vous aider et à s'impliquer pour que ces 15 actions obligatoires et critiques pour votre organisation deviennent une réalité et fassent partie de l'hygiène naturelle de tous vos processus d'affaires.

Définissez vos objectifs et le cycle de vie de la cyberdéfense de votre organisation, voici l'exemple d'Honeywell :



Source : Honeywell

Faites appel à nos équipes d'experts et de stratèges certifiés :

- Cybersécurité ;
- Cyberdéfense ;
- Cyber-intelligence ;
- Cyber-investigation ;

- Pentesteurs et Analystes Deep/Darkweb ;
- Chef de projets spécialisés en Sécurité ;
- BreachCoachs et avocats spécialisés ;
- Formateurs ;

La sécurité n'est plus une option et la négligence n'est plus un processus d'affaire valide !

8brains Canada Ltée
442 rue St Gabriel, #002
Montréal, QC, H2Y 2Z9
+1 (514) 798-9196
contact@8brains.ca

Références & bibliographie

https://www.heraldnews.com/x2132756948/Swansea-police-pay-750-ransom-after-computer-virus-strikes

https://statescoop.com/ransomware-map/?__hstc=143679850.5b718c0985e0dc501d4d93518b9ab22e.1581102561614.1581102561614.1581102561614.1&__hssc=143679850.1.1581102561614&__hsfp=562375532

https://blog.malwarebytes.com/threat-analysis/2019/02/exploit-kits-winter-2019-review/

https://securityboulevard.com/2019/11/maze-ransomware-exploiting-exploit-kits/

https://www.youtube.com/watch?time_continue=147&v=MTed3ffpmNY

https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

https://cert.ssi.gouv.fr/ioc/CERTFR-2020-IOC-001/

https://www.blockchain.com/btc/tx/87124e412abf82cefca042567f544f710c0175de65328d69d83a9562fa560e0b

https://www.law.com/dailyreportonline/2020/01/02/southwire-sues-anonymous-hacker-for-ransomware-attack/

Visualisation de quelques infiltrations de Maze https://www.cert.ssi.gouv.fr/ioc/CERTFR-2020-IOC-001/ consultable via https://oasis-open.github.io/cti-stix-visualization/

https://answers.microsoft.com/en-us/protect/forum/all/virus-and-malaware/24d778ad-29de-4fdd-9b86-e220e0ffec94

https://phoenixnap.com/blog/ransomware-statistics-facts

https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-macro-hijacks-desktop-shortcuts-to-deliver-backdoor/

https://www.govtech.com/security/RSA-2020-How-the-FBI-Thinks-About-Responds-to-Ransomware.html