A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Comment j'ai géré un chiffro-verouilleur

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Stéphane MARIOTTO effectue un retour d'expérience à propos de la cyber-attaque de type *crypto locker* ayant visé le cabinet d'avocats Fidal en 2018. Après avoir exposé le déroulement de l'incident, il présentera le travail conduit par la DSI et ses partenaires afin de résoudre le problème. Un point sera également réalisé à propos de la communication menée dans ce type de crise.

Le contexte

Cette attaque survenue le 28 mai 2018 a rendu inopérant pendant trois jours et demi une grande partie du système d'informations du cabinet Fidal, à l'exception des mails sur les téléphones. Celle-ci aurait pu durer beaucoup plus longtemps. Par ailleurs, plus d'un million de fichiers ont été chiffrés, par le virus tandis que 30 collaborateurs de la, internes et externes, ont été mobilisés durant la crise.

Déroulement de l'incident et résolution DSI

Le lundi 28 mai 2018 à 8 heures 31 du matin, un ticket a été ouvert auprès du support de l'infogéreur ITS Integra indiquant la présence de fichiers chiffrés *.crab sur le partage K:\ du site de Troyes. Personne n'a réagi dans un premier temps. L'ouverture d'une cellule de crise entre Fidal et ITS est intervenue à 9 heures 30. Le SI a été arrêté à 9 heures 53. Le *crypto locker* (ou chiffro verouilleur) avait débuté son « travail » le dimanche à 4 heures 22 du matin. L'attaque est venue d'un seul PC.

En premier lieu, il est apparu nécessaire chercher un expert chez les deux prestataires sécurité historiques, à savoir Orange Cyber Défense (OCD) et SYNETIS. OCD a précisé qu'il était disponible le mardi matin et qu'il ne disposait pas de contrat spécifique pour intervenir rapidement. SYNESTIS qui avait réalisé un audit de sécurité dans le passé a dépêché deux personnes vers midi, mais ces dernières n'étaient pas vraiment compétentes. A 16 heures, un autre intervenant a été déployé. SYNETIS a été mandaté par Fidal pour se joindre à la cellule de crise sur site et apporter son expertise.

Le message du *crypto locker* se rapportait à une demande de rançon. Fidal devait régler 1 200 dollars afin de récupérer les fichiers. Fidal n'a pas essayé de payer n'étant pas certain de récupérer la clé. En parallèle, ITS a tenté d'opérer un décryptage de la clé, mais sans succès.

Int : Avez-vous toutefois été tenté de payer cette somme de 1 200 dollars sous la pression ?
SM : Non. SYNETIS a précisé qu'il était peu probable que Fidal récupère la bonne clé. En outre, le fait de payer peut engendrer de nouveaux *crypto lockers* plus ciblés.

Stéphane MARIOTTO explique ensuite que la « v1 » de Crab est apparue pour la première fois en 2018. Cette attaque se rapportait à la « v3 ». Le virus s'exécute en une seule fois via une clé du registre *RunOnce* et disparaît dans la machine.

Ce *malware* opère un chiffrement d'un maximum de fichiers en *.crab, avec un fichier de demande de rançon par répertoire, mais également un changement du fond d'écran et une utilisation de Tor pour la rançon. Cela se traduit concrètement par un email contenant une pièce jointe infectieuse envoyée à une ou des victimes. Fidal utilise l'outil Proofpoint dont la fonction est de filtrer les liens. Or, cette attaque fait suite à l'utilisation d'un mail personnel sur un PC professionnel. De surcroît, ce *malware* cible des victimes précises (*spear phishing*) en cherchant à les appâter. Sa diffusion ne semble pas être réalisée en masse en envoyant à « tous les utilisateurs du SI » le même email contenant la charge d'infection. Dans le cadre de ce genre de campagne d'attaque, les emails infectieux sont correctement rédigés et formatés.

Les actions conduites par l'infogéreur

Dans un premier temps, l'infogéreur a mis en quarantaine les fichiers. Cette action ne n'est pas avérée très utile au final. Pour autant, elle a permis d'obtenir une liste au moment de la restauration. Fort heureusement, la partie sauvegarde n'a pas été endommagée tandis que tous les fichiers ont pu être récupérés, ce qui a nécessité un certain temps. Aucune perte n'a été constatée.

Actions Forensic

Un script de détection de fichiers suspicieux et relatifs au *malware* GandCrab v3 a été développé par SYNETIS pour surveiller de manière régulière un partage réseau défini. La mise en place d'un « pot de miel » a également été réalisée par ITS et SYNETIS afin de tracer une éventuelle réapparition du *malware*. De plus et afin de limiter les éventuelles nouvelles infections et chiffrements en masse issus d'un poste isolé sur le parc, des règles de filtrages via « IP tables » ont été déployées au niveau des baies NetApp.

Int : Je déduis que vous étiez relativement tranquilles dans la mesure où vous aviez accès aux sauvegardes.
SM : Nous n'étions pas sereins au départ. Une certaine « tranquillité » est apparue lorsque nous avons été en mesure d'être rassurés sur l'état de nos sauvegardes. Nous avons conduit différentes tâches en parallèle. Il importerait d'identifier la source de l'attaque et d'observer si le virus ne se répliquait pas ailleurs. De surcroît, il a fallu répertorier les fichiers perdus et s'assurer de leur sauvegarde.

ITS et SYNETIS ont identifié le 28 mai à 17 heures 30 dans les logs NetApp après la mise en place de la cellule de crise des traces d'authentifications et d'accès répétés entre 4 heures 22 du matin et 8 heures 37 de type CIFS (accès aux partages réseaux), ce qui corrèle par rapport aux « date de dernière modification » et « date de création » des fichiers *.crab de ces partages.

Une analyse du poste de l'avocat suspecté a été effectuée « à chaud ». Aucune trace évidente d'un autre *malware* ne semblait présente. Le poste est jugé sain le 31 mai à 14 heures 52. Le *malware* a effacé toutes ses traces suite à la réalisation de ses méfaits.

Déroulement de l'incident : communication

Une cellule de crise a été constituée avec la Direction générale pour communiquer en interne et auprès des clients. La communication interne a été effectuée par mail pour les avocats dont les mails fonctionnaient sur leur téléphone, mais également par SMS. Des informations étaient transmises deux fois par jour auprès des avocats.

S'agissant de la communication externe, il a été fait en sorte d'agir de manière transparente vis-à-vis des clients. Certains sont revenus vers Fidal afin de s'enquérir d'éventuels risques. Les journaux ont de surcroît été informés. Enfin, Fidal a bénéficié de l'accompagnement d'une agence de communication suite à la souscription, un an auparavant, d'une assurance *Data*.

Impact assurance Data

Cette assurance Data couvre les pertes de chiffre d'affaires, les frais Forensic, etc. Le forfait comprend aussi l'intervention d'une agence de communication afin de correctement échanger avec les clients ou la presse. Une réunion était conduite quotidiennement avec cet acteur. En outre, les heures supplémentaires réalisées au sein de la DSI ont été prises en charge.

En revanche, il s'est avéré délicat de démontrer que le cabinet avait perdu du chiffre d'affaires. En effet, les avocats ont travaillé la nuit et le week-end afin de rattraper leur retard. En conséquence, aucune perte de chiffre d'affaires n'a été constatée. L'ensemble des frais remboursés correspond environ au coût de l'assurance. Au final, le fait de disposer d'une assurance permet seulement de communiquer en direction des clients. En pratique, cette assurance n'a pas apporté de véritable aide.

Int : Il semble que cette assurance data a permis de mobiliser des acteurs.
SM : Oui, mais uniquement sur la partie communication. Au départ, nous n'avons pas pensé à solliciter cette assurance data. Le premier réflexe a consisté à contacter les fournisseurs sécurité. L'assurance aurait pu solliciter des sociétés de sécurité. La partie communication s'est avérée très utile.

Débat

Int : Vous avez précisé au début de votre intervention que la messagerie fonctionnait toujours.
SM : Nous avons rapidement rallumé le serveur Exchange dans la mesure où aucune autre attaque n'a été détectée. Au final, cet évènement a conduit plusieurs acteurs à travailler pendant de nombreuses heures sans interruption.

Int : Quelle serait votre stratégie dans l'hypothèse où ce travail était à refaire ?
SM : Face à un *crypto locker*, il apparaît indispensable d'éteindre le système dès le départ puis de rechercher un expert qui sait de quelle manière agir. Dans notre cas, OCD n'a pas fait suffisamment preuve de réactivité. En outre, il s'est avéré inutile d'isoler tous les fichiers en *.crab.

Int : Pour quelles raisons aviez-vous agi de la sorte ?
SM : Nous espérions peut-être récupérer la clé et la décrypter.

Int : Un dépôt de plainte a-t-il été réalisé ?
SM : Tout à fait. Nous avons rapidement mené les actions idoines avec notre avocat qui occupe la fonction de DPO.
Int : Pourriez-vous préciser le profil des fichiers touchés ?
SM : Il s'agissait de fichiers bureautiques classiques (Word ou PDF).

Int : Dans les process de sécurité déployés *a posteriori*, des maillons faibles ont-ils été identifiés ?
SM : Nous avons ajouté Varonis. Nous continuons d'ajouter des briques de sécurité. Avant l'apparition de ce *crypto locker*, nous étions confrontés à une problématique budgétaire. Désormais, je ne rencontre plus de blocage en la matière.

Int : Que pouvez-vous nous dire concernant les compétences au sein de l'équipe DSI ?
SM : Nous ne disposions pas de RSSI auparavant. Un RSSI de transition expérimenté a été recruté pour une durée d'un an. Ce dernier a formé la personne chargée des réseaux en interne et celle-ci occupe désormais la fonction de RSSI adjoint.

Int : Des vols de données ont-ils été observés ?
SM : Nous n'avons rien constaté.

Int : Un salarié peut-il être « entraîné » en matière de sécurité sur la durée ?
SM : Non. De plus, la population des avocats ne s'intéresse pas vraiment à cette problématique. Ils ne lisent pas les mails de la DSI tandis qu'ils ne s'inscrivent aux formations afférentes à la sécurité que s'ils y sont obligés.
Int : Cet évènement a-t-il conduit à une évolution des mentalités ?
SM : Malheureusement non.
Int : Ces personnes ne se remettent-elles pas en cause à l'occasion des résultats des tests de *phishing* ?
SM : Certaines évoluent, mais il ne s'agit pas de la majorité. Nous constatons par ailleurs que ce type de mail se professionnalise. Ils sont désormais envoyés à nos clients. Cinq ou six cas ont été remontés cette année.

Int : A combien la part dédiée au budget sécurité s'établit-elle sur le budget total SI ?
SM : Nous consacrons un million d'euros à la sécurité sur un budget total de 24 millions, ce qui représente environ 4 %. Par ailleurs, les entreprises anglo-saxonnes envoient un questionnaire très précis à propos de la thématique de la sécurité avant de signer un contrat avec nous. Les cabinets anglo-saxons disposent de collaborateurs dont la mission quotidienne consiste à remplir les questionnaires de sécurité de leurs clients.
Int : Lorsque nous avons des contrats avec de grandes entreprises, nous devons répondre à de très nombreuses questions, dont certaines sont plutôt « limites ».

Int : A l'Inserm les industriels de la pharmacie qui sous-traitent une partie de leur R&D à un laboratoire établissent des clauses contraignantes en matière de cyber.
SM : Aujourd'hui, nous avons des *data room* dont le coût est très onéreux. Il importe de s'assurer que les données sont sécurisées. En province, certaines ETI et PME nous demandent des accès Dropbox, ce qui donne lieu à un refus. D'autres solutions permettent d'envoyer des fichiers importants de manière chiffrée.

Int : Le DSI de Sanofi m'a confirmé qu'il était déjà arrivé à cette entreprise de ne pas conclure de *deal*, quand elle n'avait pas confiance dans la sécurité SI du partenaire. L'industrie pharmaceutique est très sensible à cette thématique.
SM : Cette question sera amenée à devenir de plus en plus sensible.
Int : A titre personnel, je ne souhaite pas forcément communiquer à propos des sujets afférents à la sécurité avec les clients.

Int : Avez-vous décrit un mode d'action dans l'hypothèse où ce type d'attaque se reproduit ?
SM : Oui, le RSSI a rédigé un certain nombre de documents, notamment des procédures qui ont été relues par l'équipe management de la DSI et partagées par l'infogéreur. Ce dernier doit les intégrer au sein de ses équipes.

Présentation des orateurs

Stéphane Mariotto, ingénieur des Mines, *a été DSI dans plusieurs secteurs, accompagnant des transformations Business et Numériques. Il dirige maintenant la DSI de Fidal, premier cabinet d'avocats français (2 500 personnes sur 90 sites), avec des enjeux de numérisation des activités et de passage dans le Cloud.*