mcmillan

Bulletin de cybersécurité

Août 2017

Les logiciels rançonneurs et leurs variantes

Introduction

Le risque - Les cyberattaques sont considérées comme l'un des risques les plus graves qui guettent votre organisation, et les logiciels rançonneurs et leurs variantes sont particulièrement en vogue à l'heure actuelle (comme le montre la cyberattaque récente « *WannaCry* »). Les utilisateurs des logiciels rançonneurs ont accès à votre système, y chiffrent la totalité ou une part importante de vos données, puis offrent de vous remettre la clé de chiffrement contre le paiement d'une somme modeste, habituellement sous forme d'une cryptomonnaie comme le *bitcoin*. Les variantes de ce type de logiciel rançonneur, telles que *NotPetya*, qui sont déguisées en logiciels rançonneurs sont encore plus insidieuses puisqu'elles ne permettent pas la récupération des données, même après le paiement de la rançon. Ces deux types de logiciel rançonneur sont abordés dans le présent document.

Outre la possibilité qu'elle ne reçoive pas la clé après avoir effectué le paiement, votre organisation s'expose au risque que d'autres malfaiteurs explorent de la même façon les vulnérabilités de son système. Vos dirigeants et vos administrateurs devraient considérer qu'une attaque par un logiciel rançonneur pourrait signaler des dangers potentiels, un peu comme les canaris dans les mines de charbon. Si une cyberattaque plus grave a lieu ultérieurement, à quel risque les dirigeants et les administrateurs sont-ils exposés s'ils se sont contentés de verser la rançon et n'ont rien fait de plus?

Jusqu'à maintenant, les autorités n'exigent pas que les intrusions et les versements de rançon soient déclarés et ne jugent pas que les versements de rançon constituent une forme de blanchiment d'argent. Si leur politique changeait à cet égard, les attaques contre rançon comporteraient un niveau de risque tout à fait différent.

WannaCry

Dans la récente attaque mondiale « *WannCry* », une variante de logiciel rançonneur a compromis des centaines de milliers d'ordinateurs en quelques heures seulement, paralysant ainsi de vastes réseaux. Cette attaque a vraisemblablement été introduite dans les réseaux des victimes à l'aide des vecteurs traditionnels des logiciels malveillants, soit des courriels de hameçonnage contenant des pièces ou des liens infectés et/ou l'exploitation des vulnérabilités d'un navigateur ou de modules d'extension désuets lors d'une visite sur un site compromis, et n'a pas été traitée comme une attaque ciblée[1]. *WannaCry* s'est répandue si rapidement que les auteurs de l'attaque n'ont pas été en mesure d'apparier les paiements aux demandes, et bon nombre se sont retrouvés avec des données brouillées.

NotPetya

NotPetya est une variante du virus *Petya*[2] lancé par logiciel rançonneur et identifié en 2016. Bien que ces deux virus se présentent comme un logiciel rançonneur qui cible les systèmes fondés sur Microsoft Windows par le truchement du protocole SMB et dont les origines pourraient remonter à l'exploit EternalBlue prétendument élaboré par la National Security Agency des États-Unis, il existe des différences importantes entre les deux. *NotPetya* ne contient pas de code qui lui permettrait de déverrouiller le chiffrement. Par conséquent, même si la rançon exigée est versée, les données chiffrées ne peuvent être récupérées.

NotPetya s'est manifesté pour la première fois dans une attaque mondiale qui visait principalement l'Ukraine, la veille de son Jour de la constitution. Ce virus a infecté des cibles en Ukraine, y compris les banques, les ministères, les réseaux de métro et même le système de surveillance des radiations à la centrale nucléaire de Tchernobyl.

Toutefois, le virus *NotPetya* s'est propagé à l'échelle mondiale et a touché des sociétés ne présentant aucune affiliation avec l'Ukraine, y compris la société britannique de publicité et de recherche sur les marchés WPP, la compagnie pharmaceutique américaine Merck, le cabinet d'avocats multinational DLA Piper, la société de logistique

---

1 RootCellar Technologies, *Frequently Asked Questions: "WannaCry" and Ransomware* (15 mai 2017).

2 Ce logiciel doit son nom aux satellites qui transportaient les bombes atomiques « Goldeneye » dans le film de James Bond de 1995 portant ce titre.

allemande DHL, le principal port à conteneurs indien JNPT et l'usine de chocolat de Cadbury en Tasmanie. L'hôpital communautaire de Princeton en Virginie occidentale devra désaffecter et remplacer l'ensemble de son système informatique par suite de cette attaque.

Renforcement et blindage

Comment pouvez-vous protéger votre organisation, vos administrateurs et vos dirigeants des risques de cyberattaques contre des rançons?

Renforcement technique – Outre les risques usuels associés aux atteintes à la sécurité des données qui ont proliféré très ouvertement contre bon nombre d'organisations au cours de la dernière décennie, six considérations techniques liées aux logiciels rançonneurs et à leurs variantes viennent changer la donne sur le plan technologique :

- *La valeur des données n'est plus absolue* – Les renseignements sur les cartes de crédit ou les renseignements personnels sur la santé ont une valeur marchande sur le Web opaque (*dark web*), ce qui motive les malfaiteurs à les voler. Toutefois, si les malfaiteurs vous empêchent d'avoir accès à ces données plutôt que de les voler, ils n'ont pas besoin de repérer des renseignements qui ont précisément une grande valeur, mais seulement de repérer des renseignements auxquels VOUS pourriez attribuer une valeur.

- *Aucune nécessité d'exfiltration ou de vente* – Pour tirer un rendement de leurs activités de cybercriminalité, les malfaiteurs doivent généralement trouver un marché opaque convenable pour vendre les renseignements volés, tout en sachant qu'ils peuvent eux-mêmes s'y faire arnaquer. De plus, le processus de transfert des données volées hors du réseau de la victime ciblée (exfiltration) est un autre point où les malfaiteurs risquent d'être repérés par des organisations plus sophistiquées. Par contraste, le logiciel rançonneur ne nécessite aucune exfiltration ni aucune vente de quoi que ce soit pour que les malfaiteurs puissent tirer un bénéfice d'une atteinte fructueuse à la sécurité des données.

- *Les vecteurs d'attaque sont généralement les vulnérabilités communes et/ou l'ingénierie sociale* –Toutes les organisations possèdent des données, dont elles définissent elles-mêmes la

valeur, et constituent ainsi un vaste bassin de cibles pour les logiciels rançonneurs. Celles qui ne se considéraient pas auparavant comme des « cibles » sont désormais très exposées et dans la ligne de mire des malfaiteurs. En effet, ceux-ci ont utilisé avec succès des vulnérabilités communes et de simples stratagèmes de hameçonnage par courriel pour commettre des violations de sécurité au sein d'organisations mal préparées. La propagation fulgurante de l'attaque « *WannaCry* » s'explique par son utilisation d'une vulnérabilité, corrigée depuis peu, de SMBv1[3] dans Windows, ce qui lui a permis de se propager dans un réseau compromis, où elle a opéré un chiffrement dans tous les ordinateurs hôtes vulnérables et les lecteurs réseau connectés auxquels elle a pu avoir accès.

- *L'automatisation entraîne des attaques aveugles* – Comme les techniques fondées sur les vulnérabilités communes et le simple hameçonnage ont été si fructueux, les malfaiteurs ont pu automatiser les processus de reconnaissance et d'infiltration. Ils peuvent ainsi attaquer de vastes groupes d'organisations, sans distinction. Aucune organisation ne peut être considérée comme à l'abri.

- *Le chiffrement de qualité fonctionne bien contre les malfaiteurs aussi* – Le décodage des types de chiffrement maintenant offerts au public, s'ils sont mis en œuvre correctement, est virtuellement impossible. Tant pour les méthodes asynchrones (RSA 2048) que synchrones (AES 256) généralement utilisées, une attaque de force brute contre des millions d'unités centrales et de processeurs graphiques serait impossible.

- *Les logiciels rançonneurs déguisés* – Tout comme un virus biologique peut prendre des formes plus létales, les logiciels rançonneurs peuvent être modifiés pour causer plus de dégâts. Comme l'a montré le virus *NotPetya*, les attaques destructrices déguisées en logiciels rançonneurs peuvent faire d'autres victimes que celle visées initialement.

Lorsqu'un logiciel rançonneur frappe, il est souvent trop tard pour faire quoi que ce soit sur le plan technique pour en atténuer les incidences. En raison de la propagation du maliciel « *WannaCry* », Microsoft a pris une mesure inhabituelle, à savoir de proposer un

[3] https://technet.microsoft.com/library/security/MS17-010.

correctif pour les versions EOL de Windows comme Windows XPiii[4]. Toutefois, un correctif ne peut protéger contre d'éventuelles mutations, variantes et imitations. Il existe une multitude d'exemples outre celui de *NotPetya*.

La plupart des défenses de sécurité traditionnelles (par exemple les pare-feu et les antivirus) n'offrent pratiquement aucune protection contre les attaques par logiciel rançonneur et ne les préviennent pas. Pour le renforcement des défenses contre un logiciel rançonneur, vous devez changer d'approche et mettre de côté l'aspect détection des atteintes qui fonde ce type de produit, pour mettre l'accent sur une gestion plus proactive des risques afin de briser le cycle d'automatisation des malfaiteurs et ce, à un coût raisonnable.

La gestion des risques suppose que l'on s'attaque au risque de façon holistique, dans leurs quatre grandes dimensions suivantes :

- *Risque lié à l'infrastructure clé des TI* – L'infrastructure clé des TI (réseaux, plateformes, systèmes) doit constamment être analysée aux fins de la détection des vulnérabilités. Celles-ci doivent ensuite être classées par ordre de priorité et atténuées, habituellement au moyen de la détection des erreurs de configuration et de la conception d'un correctif. De nombreux logiciels rançonneurs continuent d'exploiter d'anciennes vulnérabilités bien connues.

- *Risque lié aux données et aux applications* – Les applications les plus critiques sont souvent basées sur http, et sont conçues pour transmettre les données au-delà du pare-feu vers une application mobile par le truchement d'une interface de programmation d'application (API). Les malfaiteurs peuvent attaquer ces systèmes directement ou encore obtenir l'accès au réseau par une attaque de hameçonnage, puis se tourner vers les applications internes critiques. Il est donc essentiel que les organisations classent les données clés par ordre de priorité afin que des images instantanées en soient prises plus souvent et de manière plus systématique pour faciliter la sauvegarde et la restauration. Dans bien des cas, la seule restauration possible après l'exécution d'une attaque bien conçue et réussie d'un logiciel rançonneur est celle qui découle d'un programme proactif de gestion du risque lié aux données.

[4] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

- *Risque lié aux processus* – L'examen des processus permet l'analyse de l'exploitabilité des vulnérabilités relatives aux actifs les plus critiques, dans le monde réel. Qu'il s'agisse d'un exercice de pénétration délibérée du réseau par l'équipe de cybersécurité ou de l'instauration d'une authentification multifacteurs pour les ressources les plus exposées et/ou les plus précieuses, l'analyse du risque lié aux processus signifie que l'on exécute régulièrement et de façon proactive des processus choisis conçus pour sonder l'exploitabilité réelle des vulnérabilités en regard des politiques relatives à la sécurité des TI. Puisque les logiciels rançonneurs font appel, dans une certaine mesure, à l'automatisation, de même les défenses d'une organisation doivent être fondées sur les processus et l'automatisation.

- *Risque lié aux personnes (au facteur humain)* – Le risque lié au facteur humain a trait à l'un des maillons les plus faibles qu'exploitent la plupart des logiciels rançonneurs, notamment en trompant les employés afin qu'ils fournissent des renseignements par inadvertance ou permettent l'exécution arbitraire d'un code. Un programme fructueux de gestion du risque lié au facteur humain comprendra notamment des tests de pénétration du réseau par ingénierie sociale, des campagnes anti-hameçonnage et une formation de sensibilisation à la sécurité des TI.

Seule la mise en œuvre d'une stratégie de gestion proactive des risques dans leurs quatre dimensions décrites ci-dessus permettra à votre organisation d'opérer un tel renforcement technique et de prévenir les effets potentiellement dommageables des logiciels rançonneurs.

Blindage juridique – Même s'ils bénéficient d'un certain recul pour évaluer si les administrateurs et les dirigeants se sont acquittés de leurs obligations en matière de gouvernance, les tribunaux n'exigent pas la perfection. Ainsi, lors de leur examen, ils se demandent si les processus et procédures de l'organisation étaient raisonnables et s'ils ont été suivis. Si la réponse est affirmative dans les deux cas, les tribunaux ne contesteront probablement pas la conduite des administrateurs et des dirigeants. Comment les organisations peuvent-elles parvenir à ce résultat?

Les organisations doivent tout d'abord effectuer une évaluation crédible du risque. Dans le cas d'une cyberattaque et d'une attaque

par logiciel rançonneur, les probabilités de matérialisation du risque sont élevées. Par contre, les conséquences qui s'ensuivent, le cas échéant, sont plus difficiles à évaluer.

Voici quelques questions initiales qui méritent d'être analysées :

- Puisque les attaques par logiciel rançonneur supposent un chiffrement non autorisé de données,
  - quelles sont les données les plus sensibles (renseignements personnels des clients et propriété intellectuelle) qui devraient par conséquent faire l'objet d'une attention et d'une protection accrue?
  - À quel endroit les données de l'organisation sont-elles stockées? Quel processus de contrôle diligent ou de surveillance a été mis en place pour la protection des données qui se trouvent en la possession de fournisseurs et de prestataires de services d'impartition? Quelles indemnités et limitations contractuelles ont été mises en place pour la protection de ces données en la possession de tiers?
  - Un protocole de sauvegarde a-t-il été instauré? Est-il solide et sûr?
- L'organisation possède-t-elle un protocole écrit pour la protection ou la restauration de données? Est-il solide? Est-il suivi?
- L'organisation a-t-elle l'expertise interne voulue pour élaborer un plan de protection des données et effectuer un suivi de conformité s'y rapportant?

Étant donné que la menace d'une cyberattaque et d'une attaque par logiciel rançonneur est très élevée et bien connue, une organisation qui omet d'établir une procédure à cet égard expose inutilement ses administrateurs et ses dirigeants à une responsabilité si l'organisation subit une perte majeure. Il est encore plus dangereux pour une organisation d'avoir établi une procédure qui n'est pas suivie.

La plupart des lois sur les sociétés modernes au Canada reconnaissent qu'une activité commerciale comporte des risques et

qu'on ne saurait attendre des administrateurs qu'ils aient toutes les réponses à cet égard. Ces lois prévoient donc des règles d'exonération pour les administrateurs qui s'appuient de bonne foi sur l'avis d'experts. Dans le cas de la *Loi canadienne sur les sociétés par actions*, la disposition pertinente est la suivante :

> …[l'administrateur] … s'est acquitté des devoirs imposés au paragraphe 122(2) [obligation de soin, diligence et compétence], s'il a agi avec le soin, la diligence et la compétence dont ferait preuve, en pareilles circonstances, une personne prudente, **notamment en s'appuyant de bonne foi sur … les rapports des personnes dont la profession permet d'accorder foi à leurs déclarations.**
>
> L'administrateur s'est acquitté des devoirs imposés en vertu du paragraphe 122 (1) [obligation fiduciaire] **s'il s'appuie de bonne foi sur … les rapports des personnes dont la profession permet d'accorder foi à leurs déclarations**[5]. *[mise en relief ajoutée]*

En matière de cybersécurité, les administrateurs et, dans certains cas, les dirigeants peuvent se protéger de diverses façons, dont l'une consiste à faire rédiger les procédures de sécurité par un professionnel compétent ou à les lui soumettre, puis à s'assurer qu'elles sont suivies.

Transfert des risques – Selon le mode de réalisation et l'origine de la cyberattaque, il se peut qu'une autre personne soit tenue responsable des dommages. Par exemple, si la vulnérabilité résulte d'un manquement de la part d'une personne à qui des tâches ont été imparties, la convention d'impartition peut transférer des obligations à cette personne par le truchement d'engagements et/ou d'indemnités. L'organisation aura toutefois du mal à en exiger l'exécution, notamment en raison des dispositions limitatives, des délais de prescription et de la solvabilité de la personne ou de l'entreprise en cause.

---

5 Art. 123 de la LCSA. Les lois d'un grand nombre de territoires renferment des dispositions similaires, notamment 1) l'art. 135 de la *Loi sur les sociétés par actions* (Ontario); 2) l'art. 123 de la *Business Corporations Act* (Alberta); 3) l'art. 157 de *la Business Corporations Act* (Colombie-Britannique); 4) l'art. 118 de la *Loi sur les corporations* (Manitoba); 5) l'art. 121 de la *Loi sur les sociétés par actions* (Québec); 6) l'art. 211 de la *Loi sur les banques*; et 7) l'art. 220 de la *Loi sur les sociétés d'assurances*.

Assurance – Quelle que soit la solidité des processus et procédures d'une organisation en matière de cybersécurité, un certain risque résiduel persistera inévitablement. Même si votre organisation a instauré un ensemble de systèmes et de processus « blindés » qui la protègent contre les attaques de tiers, elle ne pourra vraisemblablement parer pleinement à l'erreur humaine et/ou à la naïveté, à l'égoïsme ou aux caprices politiques éventuels des employés.

On ne saurait trop insister sur la valeur d'une police d'assurance cybersécurité pour protéger votre organisation contre ce risque et l'atténuer. Toutefois, l'assurance cybersécurité n'en est qu'à ses débuts et évolue constamment. En effet, les assureurs ont du mal à évaluer avec précision les incidences d'une cyberattaque sur l'entreprise, la réputation, les biens et d'autres aspects d'organisations de diverses tailles et divers degrés de complexité, dans divers secteurs d'activité. Du coup, les couvertures, les exclusions, les franchises et les primes rattachées aux polices d'assurance cybersécurité continuent d'évoluer.

Bien que la plupart des demandes de règlement présentées à l'heure actuelle proviennent du secteur de la santé, où la protection des renseignements personnels sur la santé est au sommet des préoccupations, le nombre de demandes de règlement provenant de tous les secteurs d'activité augmente sans cesse[6].

Étant donné l'interrelation entre les polices d'assurance des biens, des pertes d'exploitation et de cybersécurité et la complexité relative de ces garanties, votre organisation doit travailler directement avec son courtier et/ou ses conseillers juridiques afin de s'assurer que les polices en place prévoient chaque scénario d'atteinte à la sécurité et couvrent adéquatement une cyberattaque (qui peut avoir un effet de domino ou non).

Un aspect intéressant qui concerne particulièrement les logiciels rançonneurs a trait au choix qu'ils offrent aux organisations entre le paiement d'une rançon (dont le montant est souvent inférieur à la franchise, du moins dans le cas d'une organisation de moyenne ou de grande taille) ou de présenter une demande de règlement aux termes de leur police. Malheureusement, les malfaiteurs ont perfectionné leur

6 Voir, par exemple, Chambre de commerce du Canada, *Cybersécurité au Canada : Solutions pratiques à un problème de taille* (avril 2017).

stratégie sur cet aspect et l'utilisent à leur avantage. Effectivement, la plupart des attaquants par logiciel rançonneurs exigent une somme relativement modeste (généralement de moins de 10 000 $), afin que l'organisation soit plus encline à verser la rançon et à passer à autre chose. Dans le domaine des logiciels rançonneurs, ce n'est pas la grosseur du poisson qui compte, mais plutôt combien de fois le poisson mord à l'hameçon. Quoi qu'il en soit, dans le cas d'attaques comme celle qu'a perpétrée *NotPetya*, l'assurance peut constituer un important secours financier pour l'organisation.

Conclusion

Toutes les organisations doivent connaître les risques liés à la cybersécurité, aux logiciels rançonneurs et aux logiciels malveillants et élaborer des procédures pour se protéger contre ces risques. Les organisations de toute taille et dans tous les pays sont des cibles pour les logiciels rançonneurs. Le logiciel malveillant « *WannaCry* » n'a sûrement pas été le dernier à menacer sans distinction les TI et les actifs de données critiques des organisations. *NotPetya* a porté ces attaques à un niveau nettement plus élevé et dangereux.

Les organisations doivent tenir compte d'un grand nombre de facteurs techniques et juridiques, des besoins de formation et du transfert des risques. Étant donné qu'une approche interdisciplinaire s'impose, le service des TI et de la gestion du risque et les conseillers juridiques devraient participer à l'élaboration des solutions. Ces derniers peuvent non seulement réduire le risque d'une attaque fructueuse, mais encore contribuer à atténuer les risques juridiques si votre organisation est attaquée.

Cet article a été rédigé en collaboration avec Steve McGeown, vice-président principal, Produits et Marketing, RootCellar Technologies, une société hybride de consultation en TI et de sécurité des TI.

par Frank Palmay et Darcy Ammerman, de McMillan, et Steve McGeown, vice-président principal, Produits et Marketing, RootCellar Technologies

Pour obtenir de plus amples renseignements à ce sujet, communiquez avec :

Toronto	Frank Palmay	416.307.4037	frank.palmay@mcmillan.ca
Ottawa	Darcy Ammerman	613.691.6131	darcy.ammerman@mcmillan.ca

mise en garde