le cnam

SEC102 - TP01

Motivations et objectifs derrière les nuisances

Date	Version	Description	Auteurs
18/02/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire :

Contexte

Les menaces informatiques sont aussi vieilles que l'informatique elle-même. Qu'il s'agisse par exemple des exploits de Alain Turing pour décoder Enigma, des premières portes dérobées implantées dans les machines de Crypto AG dès les années 1950; ou encore des chevaux de trois utilisés dès les années 1980 pour saboter des gazoducs soviétiques. Aujourd'hui, les menaces informatiques ne sont plus qu'exclusivement développées par états contre d'autres états; elles sont aussi développées par des mafieux contre des citoyens et des entreprises. Les menaces informatiques évoluent au même titre que l'informatique elle-même. Ainsi en cette année 2023, les Ransomware utilisent désormais des cryptomonnaies pour garantir l'anonymat des attaquants et les récentes avancées en matière de modèle de langage permettent déjà aux attaquants de faire évoluer les campagnes d' hameçonnage et les faux postes sur les réseaux sociaux.
Cette étude porte sur l'analyse de nuisances informatiques contemporaines.

Nuisances informatiques :

Bad Rabbit :

Bad Rabbit était un logiciel malveillant de type ransomware.

Type de nuisance : Bad Rabbit était un logiciel malveillant de type ransomware, ce qui signifie qu'il chiffrait les fichiers du système de la victime et demandait une rançon en échange de la clé de déchiffrement. Les utilisateurs touchés étaient incapables d'accéder à leurs fichiers sans payer la rançon demandée.

Motivations : Les motivations des auteurs de Bad Rabbit ne sont pas connues avec certitude, mais comme c'est souvent le cas pour les logiciels malveillants de type ransomware, il est probable que l'objectif était de gagner de l'argent en extorquant des victimes.

Vecteur : Bad Rabbit se propageait par le biais de sites web compromis qui diffusaient de fausses mises à jour d'Adobe Flash Player. Les utilisateurs qui visitaient ces sites étaient invités à télécharger une mise à jour de Flash Player, qui était en réalité un fichier exécutable malveillant déguisé en mise à jour. Une fois que le fichier était exécuté, Bad Rabbit chiffrerait les fichiers du système de la victime.

Profits estimés : Le montant total des profits gagnés par les auteurs de Bad Rabbit n'est pas connu avec certitude, mais les auteurs ont exigé un paiement en Bitcoin pour débloquer les fichiers chiffrés.

Coûts des dégâts estimés : Le coût total des dégâts causés par Bad Rabbit n'est pas connu avec précision, mais il a été signalé que plusieurs entreprises en Russie et en

Ukraine ont été infectées avant que le logiciel malveillant ne se propage à d'autres pays. Les coûts des dégâts incluraient les pertes de données, les perturbations des activités commerciales et les coûts de récupération des données.

Sources :

- https://www.proofpoint.com/fr/threat-reference/bad-rabbit
- https://www.varonis.com/blog/bad-rabbit-ransomware
- https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887

LockBit

LockBit est un ransomware, un type de malware qui chiffre les fichiers sur un système informatique et exige un paiement de rançon pour fournir une clé de déchiffrement permettant de récupérer les fichiers.

Type de nuisance : LockBit a pour effet de chiffrer les fichiers sur les systèmes informatiques infectés, les rendant inaccessibles aux utilisateurs légitimes. Cela peut entraîner des pertes de données importantes pour les organisations touchées, des perturbations des activités commerciales et des coûts élevés de récupération des données.

Motivations : Les motivations des auteurs de LockBit sont purement financières. Ils cherchent à obtenir des paiements de rançon de la part des victimes pour fournir une clé de déchiffrement permettant de récupérer les fichiers chiffrés.

Vecteur : LockBit se propage généralement par le biais de campagnes d’hameçonnage par e-mail, où les utilisateurs sont incités à ouvrir une pièce jointe ou à cliquer sur un lien malveillant. Une fois qu'il infecte un système, il utilise des techniques d'escalade de privilèges pour se propager à travers le réseau de l'organisation.

Profits estimés : Le montant des profits générés par LockBit n'est pas connu avec certitude. Cependant, les cybercriminels peuvent exiger des sommes importantes en rançon, qui peuvent aller jusqu'à plusieurs millions de dollars pour les grandes organisations.

Coûts des dégâts estimés : Les coûts des dégâts causés par LockBit peuvent être considérables, notamment les coûts liés à la récupération des données, les perturbations des activités commerciales, les coûts de restauration des systèmes infectés et les coûts de réputation pour l'organisation touchée. Les estimations de ces coûts varient en fonction de la taille et de la nature de l'organisation touchée.

Sources :

- https://www.kaspersky.fr/resource-center/threats/lockbit-ransomware
- https://fr.wikipedia.org/wiki/LockBit
- https://www.theguardian.com/business/2023/jan/13/what-is-lockbit-ransomware-and-how-does-it-operate-malware-royal-mail

Code Red

Type de nuisance : Code Red était un ver informatique qui a infecté des milliers de serveurs Web à travers le monde en juillet 2001. Il exploitait une vulnérabilité dans le logiciel Microsoft Internet Information Services (IIS) pour infecter les serveurs Web. Une fois infecté, le ver lançait une attaque de déni de service distribué (DDoS) contre le site web de la Maison Blanche.

Motivations : Les motivations des auteurs de Code Red ne sont pas connues avec certitude. Cependant, certains experts estiment que l'attaque avait pour objectif de perturber l'infrastructure de l'Internet et de causer des dommages économiques importants.

Vecteur : Code Red se propageait via Internet en exploitant une vulnérabilité dans le logiciel Microsoft IIS. Il utilisait une méthode de propagation de ver communément appelée "ver à cheval de Troie", dans laquelle le ver exploitait une vulnérabilité pour infecter un serveur et utiliser ce serveur comme point de départ pour infecter d'autres serveurs.

Profits estimés : Il n'y avait pas de profits directs liés à l'attaque de Code Red, mais certains experts estiment que les auteurs cherchaient à perturber l'infrastructure de l'Internet et à causer des dommages économiques importants.

Coûts des dégâts estimés : Les coûts des dégâts causés par Code Red ont été estimés à des centaines de millions de dollars. Les dommages incluaient les pertes de données, les perturbations des activités commerciales, la perte de confiance des clients, les coûts de récupération des données et les coûts de réparation des systèmes

infectés. En outre, l'attaque a également eu un impact sur la réputation de Microsoft et a conduit à une augmentation de la sensibilisation à la sécurité informatique.

Sources :

- https://en.wikipedia.org/wiki/Code_Red_(computer_worm)
- https://www.cybereason.com/blog/what-is-code-red-worm
- https://www.kaspersky.com/blog/history-lessons-code-red/45082/

Ardamax Keylogger

Type de nuisance : Ardamax est un logiciel espion (ou spyware) qui permet à un utilisateur non autorisé d'enregistrer les frappes de clavier, de prendre des captures d'écran et d'écouter les conversations sur un ordinateur infecté à l'insu de l'utilisateur. Il peut être utilisé pour voler des informations sensibles telles que les mots de passe, les numéros de carte de crédit, les informations personnelles et les données Je professionnelles.

Motivations : Les motivations de l'utilisateur qui utilise Ardamax peuvent varier. Dans certains cas, il peut être utilisé par des cybercriminels pour voler des informations sensibles ou pour accéder à des systèmes informatiques à des fins malveillantes. Dans d'autres cas, il peut être utilisé par des entreprises ou des organisations pour surveiller l'utilisation de l'ordinateur par leurs employés ou pour protéger leurs données sensibles.

Vecteur : Ardamax peut être installé à l'insu de l'utilisateur par le biais de programmes malveillants téléchargés à partir de sites web infectés, ou il peut être installé par des utilisateurs malveillants qui ont un accès physique à l'ordinateur cible. Il peut également être installé à distance à l'aide d'une

Profits estimés : Les profits que les auteurs d'Ardamax peuvent tirer dépendent de leur motivation. Dans le cas des cybercriminels, il peut être utilisé pour voler des informations sensibles telles que les mots de passe, les informations bancaires, les informations personnelles, qui peuvent être revendues sur le marché noir. Dans le cas des entreprises ou des organisations, le coût de la surveillance de l'activité des employés peut être économique.

Coûts des dégâts estimés : Le coût total des dégâts causés par Ardamax dépend de l'étendue de l'infection et des données volées. Les coûts des dégâts incluraient les pertes de données, les perturbations des activités commerciales, la perte de confiance des clients et les coûts de récupération des données.

Sources :

- https://www.malwarebytes.com/blog/detections/pup-optional-ardamaxkeylogger
- Deloitte.com

Bazar Loader

Type de nuisance : Bazar Loader est un malware qui peut être utilisé pour installer des logiciels malveillants supplémentaires sur les ordinateurs infectés, tels que des ransomwares ou des logiciels espions. Il peut également être utilisé pour voler des données sensibles stockées sur les ordinateurs infectés.

Motivations : Les motivations des auteurs de Bazar Loader peuvent varier. Dans certains cas, il peut être utilisé par des cybercriminels pour infecter des ordinateurs et voler des données sensibles, telles que des informations de carte de crédit ou des informations d'identification de connexion. Dans d'autres cas, il peut être utilisé pour installer des ransomwares sur les ordinateurs infectés et exiger des paiements en échange de la récupération des fichiers cryptés.

Vecteur : Bazar Loader peut être distribué via des campagnes de spam par e-mail ou des liens malveillants sur des sites web infectés. Il peut également être distribué via des kits d'exploitation (ou exploit kits) qui exploitent des vulnérabilités dans des logiciels installés sur les ordinateurs des victimes. Les auteurs de Bazar Loader utilisent souvent des techniques d'ingénierie sociale pour inciter les utilisateurs à télécharger et installer des fichiers malveillants.

Profits estimés : Les profits que les auteurs de Bazar Loader peuvent tirer dépendent de leur motivation. Dans le cas des cybercriminels, il peut être utilisé pour voler des informations sensibles telles que les informations bancaires, les informations personnelles, qui peuvent être revendues sur le marché noir. Dans le cas des ransomwares, les paiements exigés peuvent varier, mais ils peuvent être importants, allant de quelques centaines à plusieurs milliers de dollars.

Coûts des dégâts estimés : Le coût total des dégâts causés par Bazar Loader dépend de l'étendue de l'infection et des données volées. Les coûts des dégâts incluraient les pertes de données, les perturbations des activités commerciales, la perte de confiance des clients et les coûts de récupération des données. Le coût des paiements de rançon peut également être important pour les victimes de ransomware.

Sources :

- https://www.datto.com/blog/bazar-loader-attack-what-is-it-and-how-to-prepare
- Zscaler.fr
- Wikipedia

Conclusion

Il est évident que les menaces informatiques ont évolué au fil du temps pour devenir une préoccupation majeure dans notre monde numérique actuel. Les attaquants utilisent des techniques de plus en plus sophistiquées pour compromettre les systèmes informatiques et les données sensibles. Malgré les mesures de sécurité en place, les cyberattaques restent un défi important pour les gouvernements, les entreprises et les citoyens. Il est donc crucial de rester vigilant et de prendre les mesures nécessaires pour se protéger contre ces menaces en constante évolution. La sauvegarde; la veille; la prévention et les mises à jour sont les meilleurs outils pour se protéger des nuisances informatiques évoquées.

Glossaire

Exploits : il s'agit d'un code informatique ou d'une méthode qui exploite une faille de sécurité dans un système informatique pour en prendre le contrôle ou y accéder illégalement.

Portes dérobées : il s'agit d'une méthode pour accéder à un système informatique en utilisant une méthode secrète qui n'est pas connue de l'utilisateur légitime du système.

Cheval de Troie : il s'agit d'un type de programme malveillant qui semble inoffensif, mais qui contient en réalité un code malveillant qui permet à l'attaquant de prendre le contrôle du système infecté.

Ransomware : il s'agit d'un type de logiciel malveillant qui chiffre les fichiers du système de la victime et demande une rançon en échange de la clé de déchiffrement. Les utilisateurs touchés sont incapables d'accéder à leurs fichiers sans payer la rançon demandée.

Cryptomonnaies : il s'agit d'une monnaie virtuelle qui utilise des techniques de cryptographie pour sécuriser et vérifier les transactions, ainsi que pour contrôler la création de nouvelles unités de la monnaie.

Modèle de langage : il s'agit d'un modèle statistique qui est utilisé pour prédire la probabilité de la prochaine séquence de mots dans un texte donné. Les modèles de langage sont utilisés dans le traitement automatique du langage naturel pour diverses tâches, telles que la génération de texte et la traduction automatique.

Vecteur : il s'agit d'une méthode utilisée par les attaquants pour propager un logiciel malveillant ou une menace informatique.

Campagnes d'hameçonnage : il s'agit d'une technique d'ingénierie sociale utilisée par les attaquants pour obtenir des informations sensibles ou pour tromper les utilisateurs

en leur faisant croire qu'ils sont en train de communiquer avec une source légitime. Les campagnes d'hameçonnage peuvent inclure des courriels, des messages texte, des appels téléphoniques ou des messages sur les réseaux sociaux.

Ver informatique : il s'agit d'un type de programme malveillant qui se propage en infectant d'autres systèmes informatiques. Les vers informatiques sont capables de se répliquer et de se propager rapidement, ce qui peut causer des perturbations importantes dans les réseaux informatiques.

Vulnérabilité : il s'agit d'une faille ou d'une faiblesse dans un système informatique qui peut être exploitée par un attaquant pour compromettre la sécurité du système.

Microsoft IIS : il s'agit d'un serveur Web développé par Microsoft pour les systèmes d'exploitation Windows.