Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 43 – Mai 2018

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°43 Mai 2018

Les logiciels malveillants de minage de cryptomonnaies, un nouveau risque cyber

Les cybercriminels ne cessent d'innover et d'adapter leurs modes opératoires aux tendances technologiques du moment. Après les rançongiciels[1], qui demeurent une cybermenace réelle et sérieuse pour les entreprises, les **logiciels malveillants de minage de cryptomonnaies** deviennent de plus en plus populaires auprès des pirates informatiques.

Un logiciel malveillant de minage de cryptomonnaie va permettre aux cybercriminels d'utiliser la puissance de calcul (CPU) des machines compromises (ordinateur, serveur, smartphone, etc.) pour générer (« miner »), à l'insu des victimes, une cryptomonnaie (ou monnaie virtuelle) - Bitcoin, Monero, Ethereum, etc. Nonobstant la forte volatilité du cours des cryptomonnaies, ces actions frauduleuses peuvent s'avérer très lucratives[2].

Ces logiciels malveillants utilisent plusieurs vecteurs de propagation. Ils peuvent être cachés dans des logiciels publicitaires (« *adware* »), des logiciels piratés ou des extensions Firefox ou Google Chrome. Une autre méthode très utilisée consiste à insérer un code JavaScript sur une page d'un site Internet préalablement compromis (par exemple, à la suite d'une faille de sécurité ou d'une mauvaise configuration). Dans ce dernier cas, le navigateur Internet des victimes est utilisé pour générer des monnaies virtuelles.

Cette technique de minage de monnaies virtuelles (également appelée « *cryptojacking* ») est également utilisée par certains développeurs d'applications mobiles ou éditeurs de sites Internet afin de monétiser leur plateforme. Ce type de technique devient problématique quand elle est mise en oeuvre sans le consentement des utilisateurs et/ou visiteurs de ces plateformes.

Beaucoup moins impactant, sur un plan fonctionnel, que les rançongiciels, ce type d'attaque n'entraîne généralement pas d'interruption de service, même si cette hypothèse n'est pas à exclure. La principale conséquence réside en un ralentissement plus ou moins important des performances des ordinateurs et serveurs compromis.

[1] *Cf. FI N°34 « Les risques cyber liés aux rançongiciels » - Juin 2017.*
[2] *Par exemple, le cours du Bitcoin est passé de moins de 1000 euros début 2017 à plus de 16 000 euros mi-décembre suivant, pour revenir, mi-avril 2018, à environ 6500 euros.*

1er exemple

Un organisme de recherche a constaté des dysfonctionnements récurrents au sein de son réseau informatique, impliquant de forts ralentissements lors de connexions à certaines applications métier.

L'investigation menée par le responsable de la sécurité informatique de l'établissement a permis de déterminer que plusieurs postes de travail avaient été compromis par des cybercriminels exploitant une faille de sécurité non corrigée. Une porte dérobée était installée sur ces machines et permettait aux attaquants de générer des Bitcoins en profitant de la puissance de calcul de l'organisme de recherche.

2ème exemple

En 2017, plusieurs dizaines de milliers de sites Internet, dont certains appartenant à des entreprises ou des administrations françaises, ont été compromis avec des scripts de minage de cryptomonnaies, permettant à des cybercriminels de « miner » des monnaies virtuelles et de gagner des centaines de milliers d'euros depuis les navigateurs des internautes, à leur insu.

Commentaires

Si les logiciels malveillants de minage de cryptomonnaies ne provoquent pas de dommages directs aussi importants pour les entreprises (perte de données, interruption de service, demande de rançon, etc…) que les rançongiciels, **ils exploitent néanmoins des vulnérabilités réelles du système d'information et permettent donc potentiellement aux attaquants de mener d'autres actions malveillantes (sabotage, exfiltration de données, etc.).**

Préconisations de la DGSI

Compte tenu des évolutions et de la recrudescence de ces attaques informatiques, la DGSI émet les préconisations suivantes :

- **Sensibiliser et informer l'ensemble des salariés, notamment ceux appartenant au service informatique, sur ce nouveau type de cyberattaque**, et notamment sur les symptômes (ralentissement général des ordinateurs, etc..) pouvant permettre d'identifier et d'alerter sur la réalisation d'opérations de minage de cryptomonnaies.

- **Installer un bloqueur de publicité ou une extension dédiée au blocage de script sur navigateur Internet.** Des extensions disponibles pour les navigateurs Chrome ou Firefox permettent de bloquer les scripts de minage de cryptomonnaies installés sur des sites Internet légitimes ou compromis (par exemple, Adblock Plus ou NoScript).

- **Mettre à jour régulièrement l'anti-virus (ainsi que les bases de signatures) des postes de travail et des serveurs informatiques.**

- **Vérifier si l'option anti-publiciel** (anti-*adware*) **de l'antivirus est bien activée**.