APIXIT

L'expertise augmentée

NO MONEY, NO CRIME

Comment réagir face à une expansion de la menace attisée par la rentabilité ?

LIVRE BLANC Juin 2021

SOMMAIRE

APIXIT

Depuis 30 ans, APIXIT éclaire la Cybersécurité, les infrastructures et le Cloud des ETI et Grands Comptes.

Nos missions : réduire la surface d'exposition des SI et rendre les infrastructures agiles et résilientes.

APIXIT associe son offre de services éprouvée aux meilleures technologies du marché pour vous accompagner lors de vos projets.

CONTACTS & CRÉDITS

Service Business Development APIXIT
contact@apixit.fr
Tél : 01 69 93 10 62

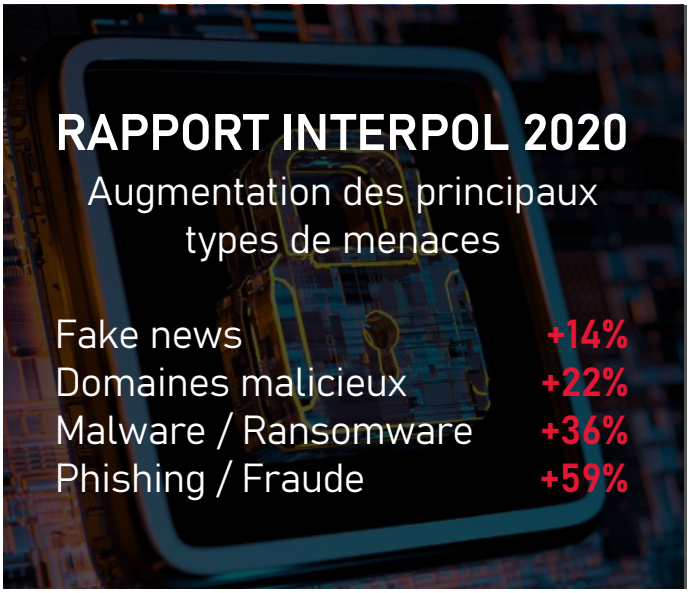
Rédaction du contenu :
Jean-Philippe Guillemin
Consultant cybersécurité

NOUS SOMMES TOUS CIBLÉS

L'emballement des cyberattaques inquiète toutes les entreprises, et pour cause : en 2021 cela concerne toutes les entreprises quelle que soit leur taille ou leur secteur d'activité, et plus seulement les entreprises financières, gouvernementales, ou la grande industrie. De facto, nous le constatons quotidiennement chaque fois que l'un de nos clients de l'agro-alimentaire ou de la distribution, par exemple, déclenche une intervention en réaction à un incident bloquant sa production.

En prenant du recul par rapport à cette situation et en mettant en perspective le niveau de maturité des entreprises en termes de sécurité et de dotation en infrastructures pour faire face aux menaces, on ne peut pas manquer de remarquer un paradoxe : elles n'ont jamais été aussi bien équipées qu'aujourd'hui : firewalls, anti-virus, EDR, IPS, etc... Pourtant, le nombre d'incidents augmente : Interpol le signalait d'ailleurs dans une étude menée fin 2020. On ne peut donc pas attribuer cette augmentation des incidents uniquement à un manque d'équipements des entreprises : un autre facteur entre en jeu.

Ce qui a réellement changé c'est le niveau de sophistication des attaques, et le fait qu'elles sont plus ciblées et plus manuelles. Ainsi l'outillage traditionnel de protection « automatique » se trouve dépassé : on doit le compléter au niveau opérationnel.



DE LA RENTABILITÉ DES ATTAQUES

Il est légitime à ce stade de se poser de nouvelles questions : Qu'est-ce qui peut avoir provoqué ce changement dans la typologie des attaques ? Quel en est le moteur ?

Le moteur est financier, c'est indéniable. Selon Amanda Creak, responsable du risque technologique chez Goldman Sachs, « près de 90% des cyberattaques sont motivées par le gain financier, les attaques par ransomware peuvent atteindre jusqu'à 746% de rentabilité pour un cyberattaquant ».

La rentabilité des attaques étant leur motivation première, intéressons-nous à ce qui rend ces attaques rentables : si elles le sont c'est parce-que le revenu induit est beaucoup plus élevé que le coût de mise en œuvre. Pour lutter contre le phénomène « à la source » : il faut donc en toute logique faire en sorte que d'une part les attaques rapportent moins, et d'autre part que leur réalisation coûte plus cher ou soit plus complexe.

Or le revenu a aujourd'hui deux sources principales :

- La revente de données volées
- L'extorsion selon 2 catégories : l'extorsion à la disponibilité des données (cryptolocker), et l'extorsion à la divulgation de données (exfiltration).

Il va donc falloir nous atteler à faire en sorte que les entreprises soient moins enclines à payer les rançons. Elles devront également mieux protéger les données sensibles, ce qui est très lié si on considère que certaines extorsions reposent sur la divulgation de données.

Le coût de mise en œuvre est réduit par plusieurs facteurs :

- L'augmentation de la surface d'attaque, inhérente à nos modes de fonctionnement hyperconnectés
- La disponibilité des outils d'attaques sous forme de toolkit ou sous forme d'abonnement (malwares as a service)
- Une carence dans la gestion des vulnérabilités techniques
- Un manque de capacité opérationnelle de détection et de réaction

Sur ces 4 facteurs nous allons pouvoir agir sur les deux derniers. Les deux premiers étant pour l'un inhérent à l'évolution de l'IT, et le deuxième relevant d'un écosystème « underground » sur lequel nous avons peu de moyens d'action.

Résumons : la rapide analyse de situation précédente nous conduit à postuler que nous pouvons agir à 4 niveaux :

- Se donner les moyens de ne pas payer les rançons
- Prévenir les vulnérabilités
- Détecter les attaques
- Réagir

SE DONNER LES MOYENS DE NE PAS PAYER LES RANÇONS

Selon une étude IBM réalisée en mars 2020, près de 70% des entreprises auraient tendance à payer une rançon permettant de récupérer leurs données. Pour agir sur le principal moteur des attaques ransomware, le revenu, il faut se donner les moyens de ne pas payer les rançons des tentatives d'extorsion.

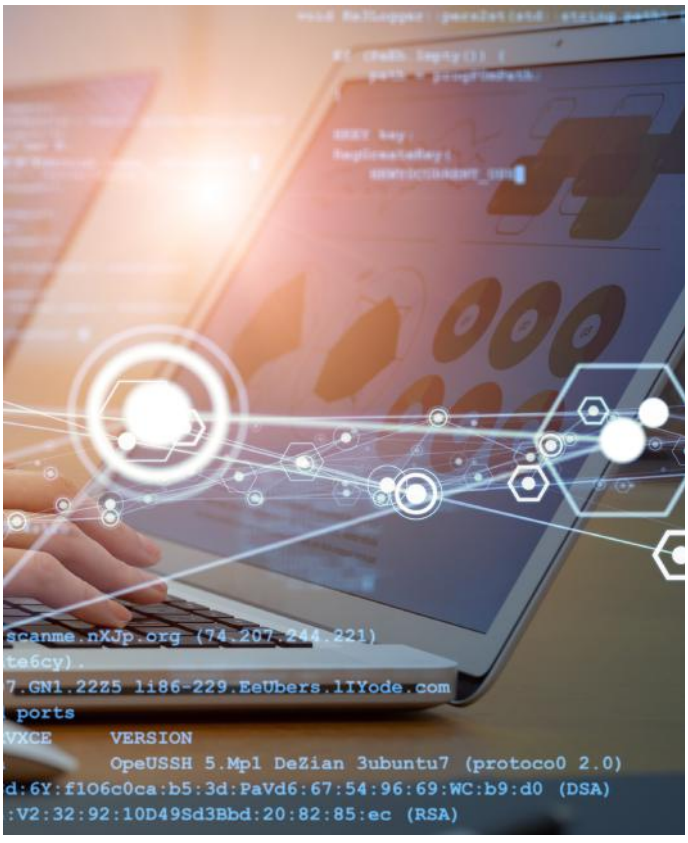
Dans la pratique une attaque persistante commence par l'exfiltration, qui demande du temps et peut passer inaperçue, avant de déclencher la phase de chiffrement qui est, quant à, elle visible et autodestructrice.
Afin d'être en mesure de ne pas payer la rançon, l'entreprise devra donc :

1) Avoir réalisé des sauvegardes hors site, d'une part, afin de réduire l'impact d'un chantage au chiffrement,

2) Avoir chiffré ses données sensibles (ou les avoir détruites si elles sont inutilisées mais toujours sensibles), afin de réduire l'impact d'un chantage à la divulgation.

Plus que jamais on constate la composante opérationnelle de ces mesures : il est question de gouvernance des données : quelles sont les données sensibles, ou sont-elles, qui y a légitimement accès, qui en est responsable, etc …

Pour amorcer cette démarche de gouvernance, dans le cadre d'un Système de Management de la Sécurité de l'Information (SMSI) existant, ou plus généralement, APIXIT propose une cartographie des données basé sur un audit outillé.



PRÉVENIR LES VULNÉRABILITÉS

Augmenter le coût de réalisation des attaques passe par la gestion des vulnérabilités. Il y a deux types de vulnérabilités techniques :

- Les vulnérabilités logicielles (failles de sécurité)
- Les vulnérabilités de configuration ou d'implémentation.

Prévenir les vulnérabilités logicielles consiste à surveiller quotidiennement les bulletins CVE. Le suivi et la gestion des vulnérabilités est l'une des activités de base d'un SOC. Lors de l'initialisation du service APIXIT réalise un inventaire matériel et logiciel du parc concerné. Nous réalisons ainsi une veille quotidienne sur la base de l'inventaire établi et dès lors qu'une vulnérabilité critique est découverte, nous identifions les actions de remédiations à mener et envoyons un rapport d'alerte par mail.

Gérer les vulnérabilités de configuration repose sur l'audit récurrent des composants via un scanner de vulnérabilités externe ou interne. Choisir quels composants auditer n'est pas trivial, car dans l'absolu tous les composants du SI peuvent servir de rebond lors d'une attaque.

Néanmoins on se concentre habituellement en priorité sur les serveurs WEB, qui sont plus exposés sur l'Internet public. La fréquence de scan généralement pratiquée est trimestrielle, ce qui donne le temps aux exploitants d'appliquer les mesures de remédiation moyennement critiques. Une procédure doit toutefois prévoir la correction immédiate des vulnérabilités critiques.

DÉTECTER ET RÉAGIR

En effet, quand il est détecté, l'attaquant ne perd pas son temps : il passe à une autre cible. Depuis qu'ils ont fait leur apparition sur le marché, on a pu juger de l'efficacité des EDR pour détecter les attaques modernes, et le résultat est plutôt positif. Il convient de rappeler qu'un EDR est principalement une sonde distribuée de détection d'attaques, couplée à une capacité d'analyse et de corrélation centralisée (le plus souvent dans le cloud aujourd'hui) : c'est un IDS !

L'EDR est actuellement l'outillage le plus important et la pierre angulaire de la protection contre les ransomware, et plus généralement contre toute forme d'attaque file-less opérée manuellement.

Les attaques basées sur des malwares automatiques sont quant à elles assez bien traitées par les antivirus-sandbox modernes.

Néanmoins, à l'instar d'un IDS, il est illusoire de penser que l'EDR est autonome : ce n'est qu'un outil de détection dont la majorité des alertes doivent faire l'objet d'une levée de doute avant d'envisager un confinement ou l'arrêt d'un processus.

Ainsi on peut dire que l'EDR est paradoxalement à la fois indispensable et insuffisant ! Il doit être adossé à une équipe d'investigation numérique et de réaction pour donner aux entreprises les moyens de stopper les attaques avant qu'elles n'entrent dans leur phase active d'exfiltration ou d'extorsion.

APIXIT

L'expertise augmentée

Ce Livre Blanc est un document d'information.
Il n'a pas vocation à servir de support de prestation de conseil.

SIEGE SOCIAL

Les Conquérants
Immeuble Annapurna
1 avenue de l'Atlantique
91940 LES ULIS

RENNES

Espace Jacques Cartier
CS 96031
35360 MONTAUBAN
DE BRETAGNE

LILLE

Village Créatif
10 rue de la Cense
59650 VILLENEUVE D'ASCQ

QUIMPER

3 allée Emile Le Page
29000 QUIMPER

PARIS

Immeuble AXIUM
22/24 rue du Gouverneur
Général Félix Eboué
92130 ISSY LES MOULINEAUX

NANTES

Les Espaces Océane
4 rue Jack London
44400 REZÉ

REIMS

13 rue Desbureaux
51100 REIMS

TOULOUSE

2 rue des Cosmonautes
31400 TOULOUSE

LYON

Immeuble Woodclub
97, allée Alexandre Borodine
69800 SAINT-PRIEST

www.apixit.fr