LE LIVRE NOIR DU HACKER

Guide de survie pour les entreprises

SOMMAIRE

ÉDITO

Si le Covid-19 a favorisé l'émergence du télétravail et fermé la porte des entreprises aux collaborateurs, il a entrouvert celle de leur Systèmes d'Information aux Cybercriminels. Alors que **le nombre de rançongiciels recensés par l'ANSSI a atteint un très haut niveau ces dernières années**, les PME et ETI font malheureusement partie des organisations les plus attaquées. Pour apprécier l'ampleur du phénomène, il suffit de savoir que les dommages de la cybercriminalité équivalent à **la 3e économie mondiale derrière les Etats-Unis et la Chine** !

Pour les entreprises, les attaques cyber sont parfois lourdes de conséquences. Au-delà des impacts directs (perte d'exploitation, demande de rançon, perte d'activité, etc.), les répercussions indirectes (dégradation de l'image de marque auprès du client final, des partenaires et des fournisseurs, dévalorisation boursière, perte de compétitivité à court terme…) sont aussi très pénalisantes pour les organisations.

Or, face à cette cybermenace omniprésente et dopée par le contexte géopolitique, toutes les entreprises ne sont pas égales : elles n'ont pas la même maturité cyber et l'équipe dirigeante n'a pas forcément pris la pleine mesure des risques. En effet, si 86% des dirigeants se disent sensibilisés aux risques cyber, seulement 44 % des ETI font de la cybersécurité une priorité d'investissement.

Les raisons d'un tel décalage ? La difficulté à passer à l'action ! La principale cause, un excès de confiance, voire de la naïveté : **80% des chefs d'entreprise considèrent leur entreprise bien, voire tout à fait, protégée**… La réalité opérationnelle est plus nuancée !

Dans ce cadre, une meilleure compréhension des motivations des hackers permet de mieux se protéger et de mieux apprécier le degré d'exposition des entreprises. Le secteur d'activité, la taille, les actifs informatiques, la communication externe et le niveau de protection conditionnent en grande partie le déclenchement de cyberattaques. **Quels sont les secteurs les plus ciblés** ? La Finance, l'Assurance, l'Industrie, l'Énergie, le Retail et les Services professionnels.

Comme il existe déjà un certain nombre de livres blancs sur la cybersécurité, nous avons décidé d'innover en vous proposant ce livre noir du hacker. Il vous permettra d'entrer dans la tête d'un cybercriminel, et de comprendre sa démarche, pour mieux le devancer. Bienvenue dans la vie d'un hacker !

L'ORGANISATION CYBERCRIMINELLE

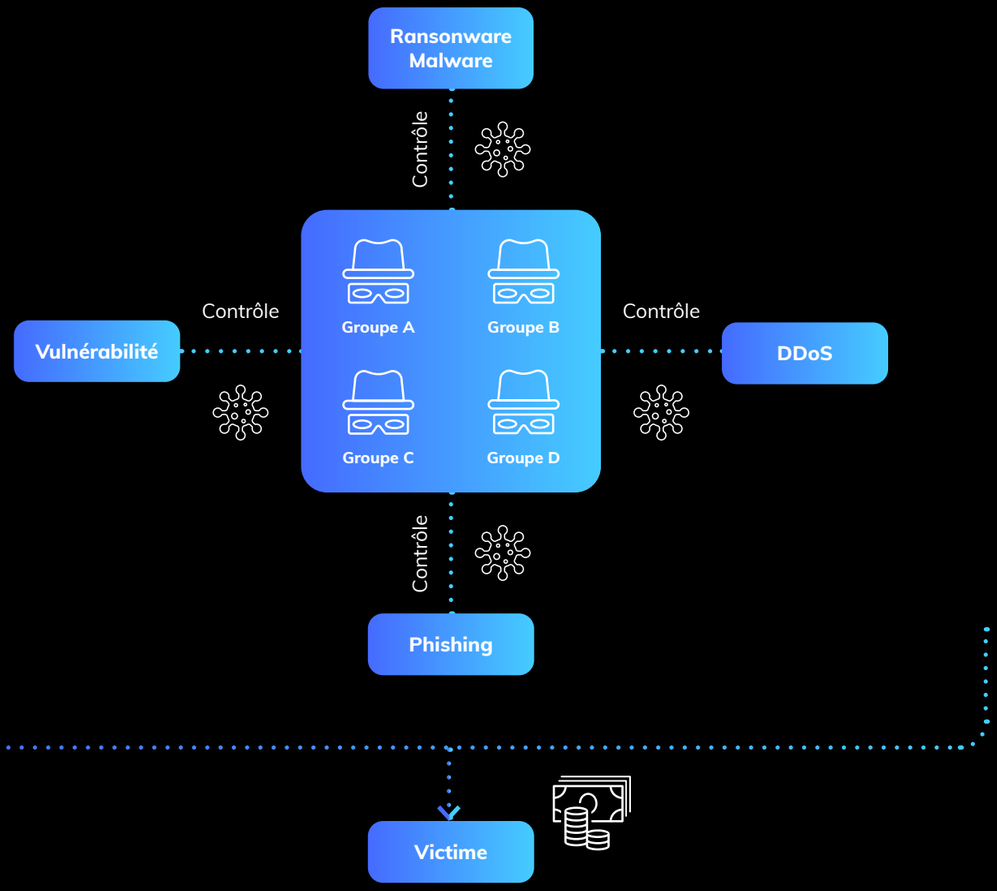
En tant que cybercriminel, je ne travaille pas seul. Au contraire, au même titre que mes cibles, j'appartiens moi aussi à une organisation structurée et hiérarchisée comptant de nombreux « collaborateurs » spécialisés. Au sein de cet écosystème global, chacun a sa mission avec néanmoins un objectif commun : tirer parti de vos informations !

MON ENVIRONNEMENT DE TRAVAIL

Comme dans toute entreprise, au sommet de la pyramide hiérarchique, on retrouve l'équivalent du « comité de direction », mais aussi tout un ensemble de managers et de services divers :

- Un service RH avec des recruteurs et des capacités de recrutement opérant via le dark web mais aussi via les outils traditionnels des employeurs.
- Un service juridique pour prévenir des risques, conseiller l'organisation (dans quels pays ne pas se déplacer…) et impliquer des avocats lorsque nécessaire.
- Un service financier qui gère des budgets pour les salaires, les investissements, les risques (en cas d'arrestation, de saisie des infrastructures), etc.
- Des chercheurs pour notre R&D, c'est-à-dire pour définir de nouveaux débouchés, mettre au point nos démarches et de nouvelles techniques d'attaque.
- Des responsables du blanchiment pour permettre d'exploiter nos gains crapuleux.
- Des équipes DevOps en charge de la conception des logiciels malveillants et de l'évolution de notre Système d'Information.
- Un service commercial, qui garantit la profitabilité de nos services via la vente d'informations dérobées, de codes malicieux, l'achat de vulnérabilités, qui fait de nous une organisation prospère.
- Et bien sûr une équipe de hackers dont je fais partie.

C'est pourquoi on parle aujourd'hui de gang, de cluster ou même de cartel pour désigner les organisations cybercriminelles comme celle à laquelle j'appartiens.



Exemple type d'un cartel cybercriminel (source : **Tehtris**)

Le « télétravail » n'est pas nouveau pour moi, j'y suis habitué depuis bien plus longtemps que la majorité des entreprises, mais il m'arrive aussi de me déplacer dans des bureaux physiques lorsque c'est nécessaire. Et si besoin, je peux aussi travailler en partenariat avec d'autres organisations cybercriminelles. Comme les entreprises traditionnelles, nous avons recours à la sous-traitance lorsque nous n'avons pas toutes les ressources ou les compétences requises pour mener à bien nos attaques.

Grâce à l'organisation industrielle des cybercriminels, une attaque de type ransomware a lieu toutes les 10 secondes. Parmi les clusters les plus importants, celui composé de Wizard Spider, Twisted Spider, Viking Spider et LockBit s'avère particulièrement redoutable.

Source : **CheckPoint**

MA FICHE DE MISSION

En tant que hacker, mon rôle est donc de réussir à pénétrer et à corrompre votre Système d'Information. Mon objectif est généralement de vous demander une rançon pour récupérer vos données, de les revendre à des tiers intéressés ou de détourner directement des fonds. Et pour y parvenir, tous les moyens sont bons.

DU CÔTÉ DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Du côté de l'entreprise, le RSSI fait partie d'une organisation informatique bien structurée et aux rôles bien définis. Qu'il soit interne ou externe, rattaché à la DSI ou à la Direction Générale, il structure puis fait appliquer la démarche cybersécurité de son organisation via :

- **Une Politique de Sécurité du Système d'Information (PSSI)** qui évalue les risques stratégiques puis définit le schéma directeur sécurité.
- **Une charte informatique** qui délimite de manière synthétique les droits et devoirs des utilisateurs vis-à-vis du Système d'Information.
- **Des certifications** telles que CISSP, CISM, NIST, PCI DSS, ISO qui garantissent la compétence des ressources ou la conformité des organisations.
- **Une assurance cyber :** le RSSI qui évalue le risque cyber au regard des enjeux stratégiques d'entreprise peut inviter sa direction à souscrire une assurance cyber pour limiter le risque financier en cas de crise.

Au sein des entreprises, le budget IT représente en moyenne 2,5% du chiffre d'affaires, dont 10% devraient être consacrés à la cybersécurité selon l'ANSSI.

LE CIBLAGE

Comment vais-je m'y prendre pour pénétrer votre Système d'Information ? Tout simplement de la même manière qu'un cambrioleur : en scrutant votre infrastructure pour trouver une porte ouverte ou une fenêtre mal fermée. Et si l'infrastructure est suffisamment robuste pour éviter une compromission directe, je vais alors m'attaquer à votre plus grande faiblesse : vos collaborateurs !

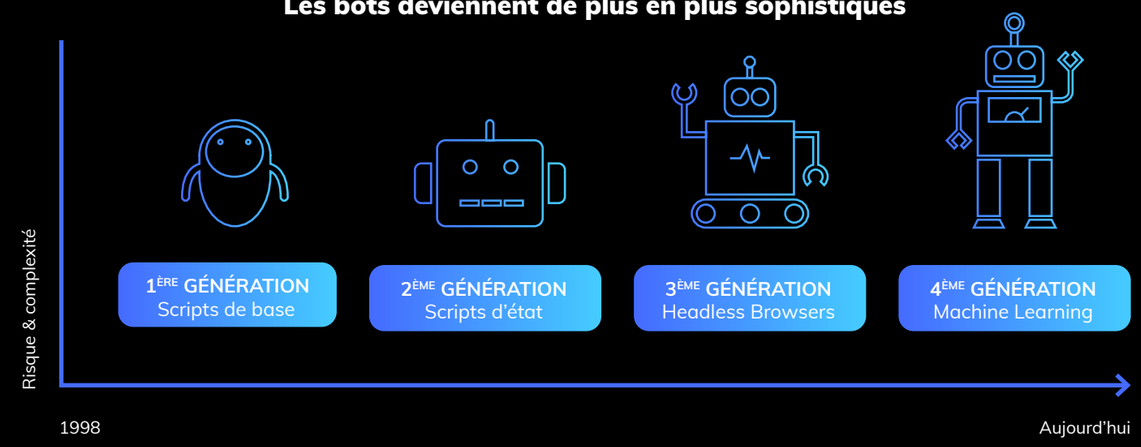
1ère option

LES SCANNERS AUTOMATIQUES POUR DÉCOUVRIR LES VULNÉRABILITÉS DE VOTRE SYSTÈME D'INFORMATION

Pour scanner massivement les entreprises, nous employons des « bots », c'est-à-dire des robots, qui scrutent tout ce qui est visible depuis internet : un site e-commerce, un extranet, des web services, etc. Les faiblesses que nous détectons sont souvent liées à la mauvaise configuration d'un firewall, à une faille logicielle non patchée ou à un code mal développé.

→ **Ces bots sont des programmes de plus en plus sophistiqués exécutés en général depuis des organisations déjà compromises : en listant ces cibles potentielles, ils peuvent ainsi s'apparenter à des « apporteurs d'affaires »... les coûts de commissions en moins.**

Les bots deviennent de plus en plus sophistiqués



Évolution de la sophistication des bots depuis 1998 (source : Barracuda)

66%

des entreprises ont subi des formes d'hameçonnage ciblé et 64% des attaques d'hameçonnage par téléphone.

Source : **Rapport State of the Phish**, Proofpoint

2ème option

L'INGÉNIERIE SOCIALE POUR DÉROBER DES INFORMATIONS CONFIDENTIELLES OU DES IDENTIFIANTS DE CONNEXION

L'idée ici est de mener des campagnes d'attaque par email (phishing), SMS (smishing) ou message vocal (vishing) qui vont permettre de récupérer des informations confidentielles en misant sur la crédulité des utilisateurs. En gros, je lance une attaque sur de nombreuses sociétés, je récupère des données, et je les utilise lorsque je veux déclencher une attaque.

Dans le cadre d'une attaque plus ciblée de type Spearfishing, je vais usurper l'identité d'une personne morale (établissement financier, service public, concurrent…) ou physique (collègue de travail, famille, ami…) connue du destinataire pour mieux lui soutirer des informations. À la différence du phishing, cette attaque est non seulement ciblée, mais également personnalisée car je m'appuie sur des informations crédibles trouvées bien souvent sur les réseaux sociaux. J'utilise cette démarche quand j'ai récolté suffisamment d'informations sur mes cibles.

Enfin, notre meilleur butin est celui qui consiste à dérober les identifiants de « comptes à privilèges » d'administrateurs ou d'utilisateurs clés : pour nous les hackers, ce sont de véritables tapis rouges !

ZOOM SUR L'INGÉNIERIE SOCIALE

Voici quelques-unes de nos techniques pour tenter de vous compromettre via l'ingénierie sociale :

- **Hameçonnage :** courriels (phishing), sites web ou textos trompeurs (smishing) pour voler de l'information.
- **Arnaque au président (CEO fraud) :** escroquerie dans laquelle un criminel se fait passer pour un dirigeant, et réussit à convaincre des collaborateurs de virer une somme d'argent sur un compte bancaire intraçable.
- **Harponnage (spearphishing) :** courriels ciblés visant des personnes ou des entreprises.
- **Appâtage (baiting) :** attaque via l'ingénierie sociale, en ligne et physique, qui promet à la victime une récompense ou un cadeau.
- **Maliciel (malware) :** attaque qui fait croire qu'un maliciel a été installé sur l'ordinateur de la victime en lui offrant de payer pour le supprimer.
- **Faux-semblant (pretexting) :** emploi d'une fausse identité pour tromper les victimes et soutirer de l'information.
- **Quiproquo (quid pro quo) :** démarche utilisant un échange d'information ou de service pour convaincre la victime d'agir.
- **Talonnage (tailgating) :** technique s'appuyant sur la confiance humaine pour donner au criminel l'accès physique à un édifice ou à une zone sécurisée.
- **Attaque par point d'eau (watering hole) :** attaque d'ingénierie sociale sophistiquée qui infecte, par un logiciel malveillant, à la fois un site web et les internautes qui le visitent.

Comme vous pouvez le constater, nous ne sommes jamais à court d'imagination.

85%

des violations de données impliquent un élément humain.

Source : **Verizon Data Breach Investigations Report**

DU CÔTÉ DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Le RSSI et la DSI disposent d'outils équivalents à ceux des hackers : ils savent scruter leur Système d'Information pour découvrir des failles et les corriger. Pour contrer les risques liés à l'ingénierie sociale, ils peuvent alors engager une démarche de cybersensibilisation.

En général, la DSI déclenche trois types de services d'audit de sécurité pour évaluer ses forces et ses faiblesses :

- **Audits méthodologiques :** ils sont le plus souvent réalisés par un auditeur spécialisé sur la base d'un référentiel normé, par exemple l'ISO 27002. Via un questionnaire et l'étude de divers éléments, ils étudient votre organisation, vos processus et vos outils, et fournissent un compte-rendu permettant de mettre en œuvre des plans d'action correctifs.
- **Tests d'intrusion :** ils sont exécutés par des hackers éthiques, officiellement du bon côté de la loi, qui vont tenter de pénétrer votre Système d'Information. Ils mènent cette démarche avec ou sans information de votre part et, vous informent des failles de sécurité découvertes dans votre infrastructure et dans vos codes. Au même titre que les hackers malveillants, ils aiment se faire payer à la faille découverte.
- **Outils d'analyse automatiques :** sur la base de vos adresses IP publiques et privées, ou de vos noms de domaine, ces outils d'analyse de vulnérabilité ou de « cyberscoring » vont scruter régulièrement votre Système d'Information et remonter des rapports de synthèse, des problèmes de configuration et des failles non corrigées.

Ensuite, pour contrer les risques liés à l'ingénierie sociale, le RSSI peut renforcer la cyberrésilience de son organisation via des programmes de formation avec le département RH et de campagnes d'attaques fictives menées auprès des collaborateurs.

Vous souhaitez obtenir plus d'informations sur la cybersensibilisation ?
Téléchargez notre livre blanc dédié ici

Budgets moyens des audits pour une PME/ETI :

Audit méthodologique : 5 à 30K €
Tests d'intrusion : 5 à 15K €
Outils de cyberscoring : 1 à 3K €/an

L'ATTAQUE

Maintenant que j'ai identifié les failles de votre Système d'Information ou des utilisateurs compromis, je vais pouvoir déclencher mon attaque.

1ère démarche

EXPLOITER LES FAILLES

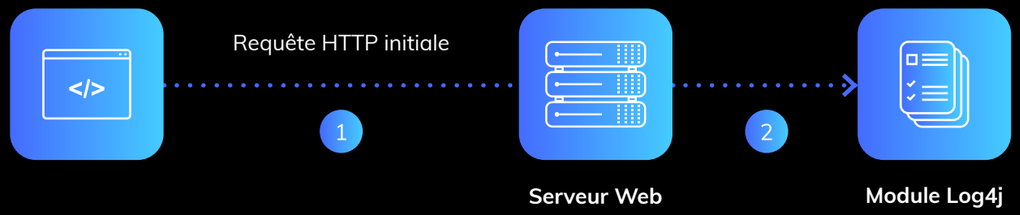
Votre Système d'Information évolue sans cesse et doit rester ouvert pour communiquer avec vos partenaires, vos télétravailleurs et vos collaborateurs nomades. Ce contexte favorable permet à mes « confrères » hackers et à moi-même d'exploiter chaque jour de nouvelles failles de sécurité : plus récentes sont les vulnérabilités, moins elles sont corrigées et, par conséquent, moins vous êtes protégés, plus notre travail est facilité.

Deux cas de figure se présentent alors :

- Soit nos bots automatiques ont identifié des failles non corrigées.
- Soit nous menons une analyse ciblée manuelle pour un « compte stratégique » financièrement intéressant ou visé par un commanditaire (car, je vous l'expliquerai plus tard, nous pouvons travailler pour nous-mêmes ou pour le compte d'un « client »).

Une fois qu'une faille de sécurité est découverte, je peux alors lancer mon attaque. Et ensuite ? Je prends tout simplement pied dans votre Système d'Information pour espionner, voler vos données ou corrompre votre système via un ransomware.

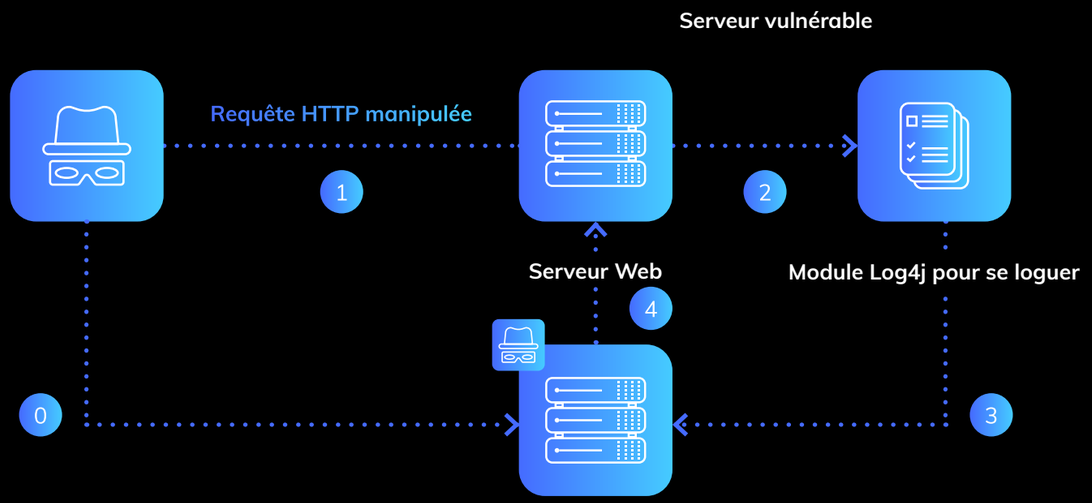
Prenons l'exemple d'une démarche d'attaque basée sur la vulnérabilité LOG4J :



1 Le requête qui comprend les informations détaillées de l'en-tête est envoyée au serveur Web

2 La charge utile malveillante est transmise au Log4j pour se loguer

Figure 2 : Requête HTTP classique vers un serveur Web



0 Un acteur malveillant se prépare à injecter un code malicieux dans une carte Java.

1 Un acteur malveillant envoie une charge utile malveillante qui sera vraisemblablement activée par l'application.

2 Une charge utile malveillante est transmise au Log4j pour se loguer.

3 Le Log4j décompose la charge utile malveillante et lance une requête vers le serveur LDAP malicieux.

4 Le serveur LDAP répond en envoyant du contenu infecté avec la carte Java.

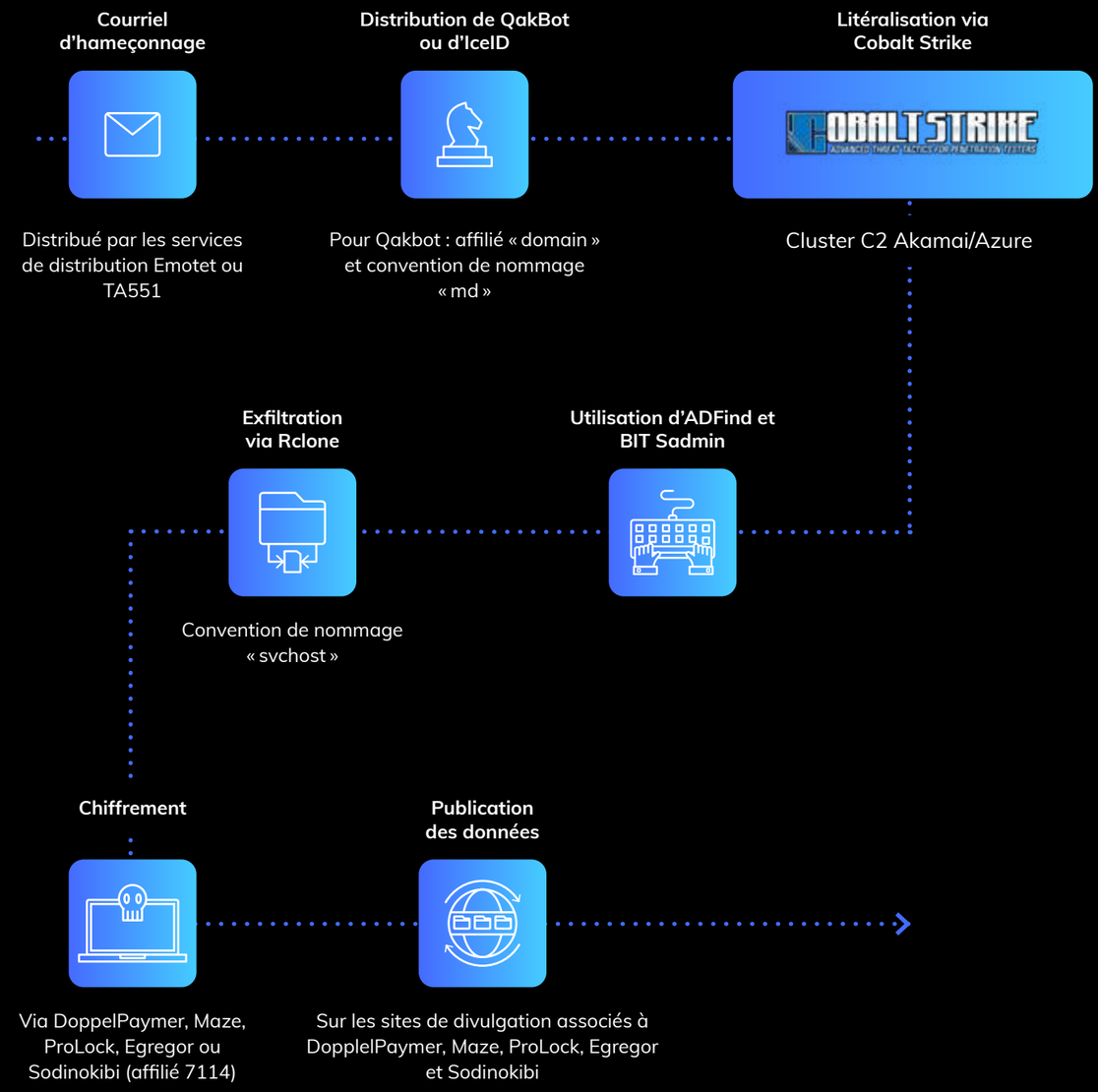
Attaque basée sur la vulnérabilité LOG4J (source : **Cyberint**)

2ème démarche

EXPLOITER LES COMPTES UTILISATEURS COMPROMIS

Comme je vous l'ai expliqué plus haut, nos techniques d'ingénierie sociale me permettent de vous soutirer des informations sensibles, jusqu'à obtenir le contrôle de votre machine ou disposer de vos identifiants de connexion. Une fois en place, je lance alors des démarches très outillées et industrielles pour élever mes privilèges, et m'implanter à différents endroits de votre Système d'Information.
Next step : exécuter mon attaque.

Exemple de démarche pour encrypter et exfiltrer vos si précieuses données :



Panorama des menaces informatiques (source : **ANSSI**)

En moyenne, les organisations découvrent leurs failles de sécurité 207 jours après l'intrusion.

Source : **Cost of a Data Breach report**, IBM Security

DU CÔTÉ DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Face à ces attaques, le RSSI et la DSI disposent de parades efficaces :

- Concernant les failles de sécurité, la DSI peut mettre en œuvre des outils **d'analyse des vulnérabilités** et des outils **d'application de correctifs**. Ils permettent d'évaluer la sécurité des systèmes au quotidien et de corriger les failles très rapidement. Bien évidemment, ces outils restent inopérants face aux failles « Zero day » tout juste découvertes qui se monnayent très cher dans l'univers de la cybercriminalité.

- Ensuite, la DSI peut mettre en œuvre de nombreux outils pour contrer les attaques : des solutions d'antivirus modernes **appelées EPP (EnPoint Protection), EDR (Endpoint Protection & Response) ou XDR (plateforme intégrée de sécurité)** qui détectent les démarches des hackers, bloquent les attaques, et réparent ou isolent les postes touchés.

- Enfin, la DSI ou leur organe spécialisé appelé SOC (Security Operation Center) exploite de plus en plus les solutions SIEM (Security Information & Event Management). Elles permettent d'agréger les logs de l'ensemble des actifs IT, de détecter les risques, et de déclencher des alertes de manière ciblée et proactive.

Pour une entreprise, le budget pour :

Une solution d'antivirus EPP/EDR est de 50€ par utilisateur.

Une solution d'évaluation de vulnérabilité et de gestion de correctifs s'élève à environ 15K€ pour 100 serveurs.

LA COMPROMISSION

Ça y est ! Je suis confortablement installé dans votre système et maintenant, je vais pouvoir tirer parti de mes efforts : voler ou encrypter vos données et systèmes, détourner des fonds, influencer, passer des messages… J'ai l'embarras du choix !

En réalité, tout dépend de mon objectif initial et du profil de l'organisation cybercriminelle pour laquelle je travaille. Selon les raisons qui m'ont poussé à agir, mon plan d'action va différer. Très bien, mais quelles sont mes principales motivations ?

#A – LE CYBERCRIME

Ici, ma motivation repose essentiellement sur le gain financier que je vais pouvoir obtenir. Là encore, il y a plusieurs façons de procéder :

- Soit je détourne des fonds en m'immisçant dans vos systèmes financiers.

- Soit je revends vos informations sensibles ou personnelles au plus offrant sur le dark web. Ne vous inquiétez pas, je trouve toujours preneur.

- Soit j'ai déposé un rançongiciel dans votre système et j'exige une rançon pour vous fournir la clé de déchiffrement.

Autres possibilités : multiplier les gains et réclamer une rançon tout en revendant les informations sur le dark web, puis relancer une attaque quelques mois plus tard. En résumé, comme je suis malin, je pérennise mon investissement.

Plus de 40 milliards de données diverses sont piratées ou perdues chaque année.

Source : **Threat Landscape Retrospective**, Tenable

#B – L'ESPIONNAGE

La dure loi du marché ! Vos concurrents peuvent aussi être les commanditaires de cyberattaques pour vous déstabiliser ou dérober vos informations sensibles et vos savoir-faire. Je peux par exemple dérober le plan de votre dernière offre révolutionnaire, vos contrats fournisseurs, vos prix de revient, les prix auxquels vous vendez vos produits et services, etc.

#C – L'INFLUENCE OU LA VENGEANCE

Cela ne vous surprendra peut-être pas mais certains de mes commanditaires sont parfois des particuliers, des organisations ou carrément des États. Ces derniers cherchent à désinformer, à influencer une élection, à espionner leurs adversaires, voire à publier certaines informations qui pourraient compromettre les parties adverses.

Dans le même genre, des activistes peuvent employer mes services pour faire passer leurs messages et leurs revendications : diffusion de fake news ou action de « defacing » de site. Enfin, je peux également chercher à venger mon commanditaire d'une personne ou d'une société avec laquelle il est en délicatesse en divulguant notamment des données compromettantes.

Le cas Cambridge Analytica, un cas d'école : à partir de 2014, cette entreprise spécialisée dans la communication stratégique a utilisé, sans leur consentement, des données personnelles de millions d'utilisateurs de Facebook afin de cerner leur « personnalité ».

Objectif : leur pousser ensuite des messages ciblés et les inciter à voter pour le candidat désigné par le commanditaire de l'opération. C'est ce qu'on appelle le microciblage comportemental.

DU CÔTÉ DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Le RSSI et la DSI ont à leur disposition toute une panoplie d'outils et de moyens afin de protéger leur Système d'Information :

- **Sécurité des utilisateurs, des terminaux et des systèmes :** en complément des produits de sécurité évoqués plus haut, les organisations s'appuient sur le MFA (MultiFactor Authentication) pour garantir l'identité de leurs utilisateurs, sur le Mobile Device Management (MDM) pour configurer leurs terminaux.
- **Sécurité périmétrique :** les pare feux (Firewall), les boîtiers SSL, les WAF (Web Application Firewall), les solutions NAC (Network Access Control), les démarches de cloisonnement des réseaux et les passerelles de filtrage de messagerie.
- **Classification et protection des données :** ces solutions permettent de classifier vos données, d'appliquer une politique de sécurité et de réaliser des audits de contrôle. De même, pour garantir la protection de vos données et systèmes, les systèmes de sauvegarde et de Plan de Reprise d'Activité (PRA) doivent être correctement implémentés, configurés et testés régulièrement.
- Enfin, nous devons imposer à notre DSI et à nos partenaires IT le respect des **best practices sécurité « Security by Design » et « Security by default »**, en particulier dans les phases de conception, de mise en œuvre et d'évolution du Système d'Information.

Pour une organisation, les coûts moyens s'établissent à :

20 € par utilisateur pour une solution de MFA ;
10K € pour un firewall et 5K € pour une solution WAF.

L'EXTORSION

Enfin ! C'est l'heure de passer à la caisse. Moi aussi, j'aspire à bien gagner ma vie… mais sans passer par la case prison.

J'ai donc préparé mon plan de communication et mes outils afin de collecter les fonds sans que mon identité ne soit compromise.

LA 1ÈRE RÈGLE DU HACKER : ÊTRE INTRAÇABLE

Durant l'attaque, la phase de négociation ou lors de la récupération des fonds, ni mon identité, ni celle de mon organisation criminelle ne doivent être compromises.

LA 2ÈME RÈGLE DU HACKER : ÊTRE PAYÉ

Je dois évidemment prendre soin que l'argent extorqué ne puisse pas être tracé. La plupart du temps, je me fais donc payer en cryptomonnaie sur le dark web : c'est anonyme, rapide et facile à utiliser. Pour la police, ces mouvements de fond sont quasiment impossibles à suivre et les quelques traces laissées ne sont que temporaires.

Ma monnaie préférée ? Le Bitcoin, bien sûr ! Les paiements en Bitcoins représentent d'ailleurs près de 98 % des paiements dans les cas d'extorsion par rançongiciel (selon **Marsh**). Le plus drôle, c'est que nous n'hésitons pas à pirater des sites de cryptomonnaies. Un collègue a ainsi réussi à s'introduire dans la plateforme crypto.com et à dérober plus de 34 millions de dollars en Ethereums et en Bitcoins : il fait la fierté de toute notre communauté !

LA 3ÈME RÈGLE DU HACKER : CONSERVER UNE « BACK DOOR » DANS VOTRE SYSTÈME D'INFORMATION

Pour autant, ne pensez pas en avoir fini avec moi. Même après l'attaque, je dispose toujours de portes d'entrée cachées que j'ai placées dans votre Système d'Information, au cas où j'aurais envie de revenir vous faire une petite visite d'ici quelque temps.

Votre Système d'Information est très accueillant, on y entre comme on veut, quand on veut. Bref, on s'y sent comme chez soi. Tant qu'il y a de l'argent facile, je suis un hacker fidèle, alors à très bientôt !

En un an, le groupe criminel Revil a fait un profit de 123M $ et volé 21,6 To de données.

Source : **X-Force Threat Intelligence**, IBM

DU CÔTÉ DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Pour la DSI, la priorité est de comprendre l'origine et de conserver les preuves de l'attaque, de corriger les vulnérabilités détectées, puis de garantir la reprise de l'activité dans les meilleurs délais. Mais avant toute chose, il faut rappeler qu'une crise cyber déclenche généralement la mobilisation d'un comité de crise qui coordonne les actions de tous les départements de l'organisation attaquée : direction, communication, RH, juridique, métiers, etc.

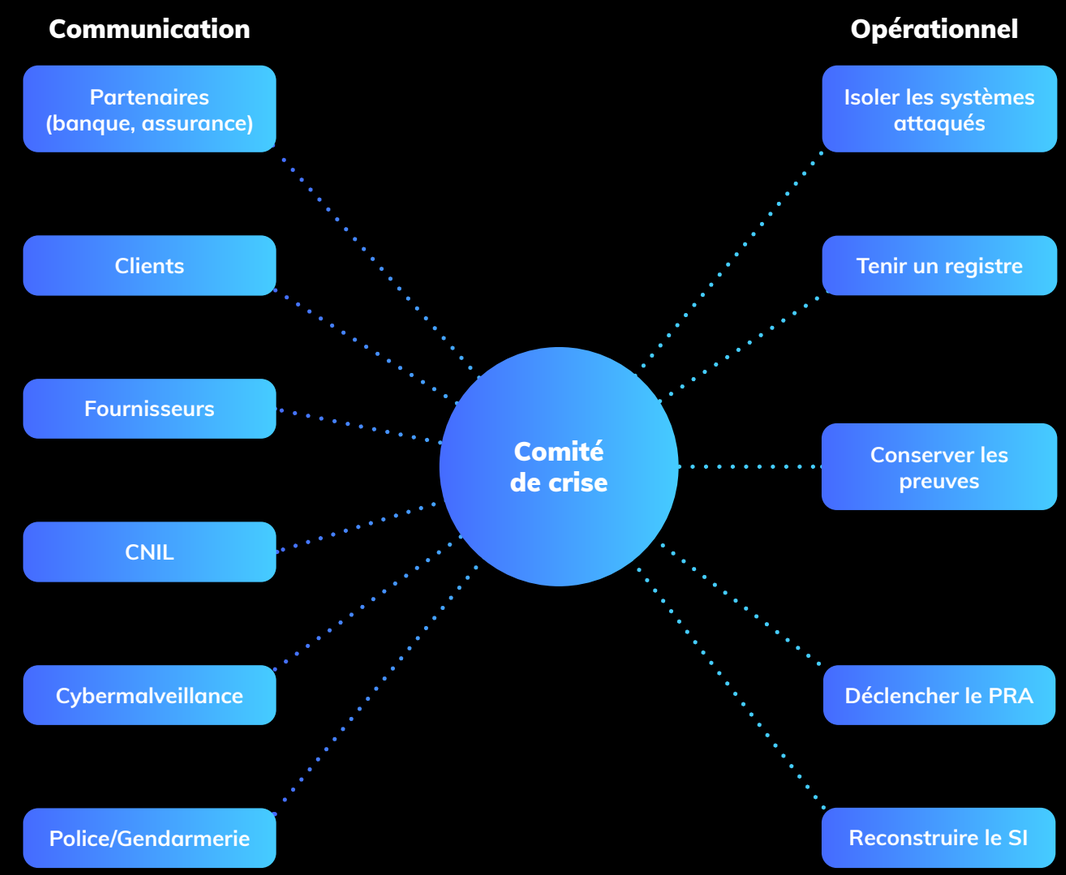
Pour gérer les incidents de sécurité ou une crise cyber, la DSI fait souvent appel à des partenaires extérieurs :

- **Des sous-traitants CERT** (Computer Emergency Response Team) : ils mobilisent rapidement des ressources qui vont assister le client dans toutes les dimensions de gestion de sa crise. Ils vont ainsi monter un comité de crise, gérer la communication interne et externe, retrouver le « patient 0 », sauvegarder les preuves du piratage puis élaborer un plan d'action pour redémarrer.

- **Des experts et des consultants :** pour restaurer le Système d'Information depuis les sauvegardes ou le réinstaller totalement dans une « green zone » si ce dernier est trop corrompu.

- **Des partenaires juridiques et / ou psychologiques :** pour gérer les conséquences de la crise auprès des clients, des fournisseurs, des autorités ainsi que la fragilisation psychologique des collaborateurs.

- **Des assureurs :** l'assurance de l'entreprise, de l'institution ou de l'organisation attaquée peut impliquer une société de cybersécurité spécialisée pour assister le client et couvrir une partie des risques financiers.



Dispositif de gestion de crise Cyber

Seulement 8 % des ETI et moins d'1 % des PME avaient souscrit une assurance cyber.

Source : selon **AMRAE**

Pour une organisation, une assurance cyber coûte en moyenne 3% du montant couvert.

CONCLUSION

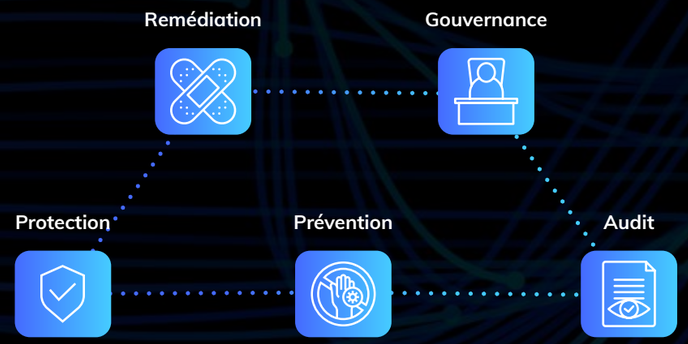
Dans ce livre noir, vous aurez compris que le cybercriminel n'est finalement pas si différent de vous. Il travaille lui aussi dans une organisation structurée soumise à des réalités économiques, et évolue dans un monde concurrentiel dans lequel il faut sans cesse se réinventer pour pirater des clients plus ou moins bien protégés.

La démarche du cybercriminel que nous venons de relater est malheureusement très fidèle à la réalité : les hackers exploitent facilement vos failles de sécurité ou manipulent aisément vos utilisateurs.

Les risques étant bien réels et en constante évolution, la cybersécurité doit donc être prise très au sérieux par la DSI mais aussi par la Direction Générale. Cette dernière doit désigner un RSSI interne ou externe, et mobiliser les moyens suffisants, y compris dans la durée. Pour rappel, **l'ANSSI préconise de consacrer entre 5 et 10 % du budget** de la DSI à la cybersécurité.

Chacun des projets informatiques entrepris doit considérer le risque cyber et la sécurité informatique comme des priorités essentielles, à l'instar de ce qui est déjà fait sur les données personnelles avec le règlement européen RGPD.

Face à ces enjeux particulièrement complexes, il est recommandé de recourir à des expertises extérieures et à des solutions spécialisées pour prendre en compte, de manière proactive et coordonnée, les 5 dimensions clés du domaine cyber :



Les dimensions clés de la cybersécurité

Nous proposons **un large catalogue de services et de solutions** pour accompagner les PME et ETI en matière de cybersécurité : services d'audits, solutions de protection, services de cybersensibilisation et, naturellement, un support spécialisé : le Security Operation Center, pour contenir en permanence les menaces cyber. Vous pouvez ainsi vous consacrer sereinement à vos clients et à votre business !

QUIZ : AUTO-ÉVALUEZ VOTRE CYBERSÉCURITÉ

Êtes-vous prêt(e) à faire face aux hackers ? Pour le savoir, les critères ci-dessous permettent de réaliser **une première évaluation de la cybersécurité dans votre entreprise** :

- **Une campagne de cyber-sensibilisation est-elle conduite auprès des utilisateurs ?**
- **Mes données sensibles sont sauvegardées sur plusieurs médias et sites, y compris de manière immuable ?**
- **L'identité de mes utilisateurs est garantie par un mécanisme d'authentification forte ?**
- **Les terminaux des utilisateurs sont systématiquement protégés par un EDR et gérés au travers d'un MDM ?**
- **Je déclenche régulièrement des tests de pénétration sur mon Système d'Information ?**
- **Je teste régulièrement l'efficacité de mes sauvegardes et de mon Plan de Reprise d'Activité ?**
- **J'ai nommé un RSSI dans mon organisation ?**

Vous avez répondu « Oui » à toutes les questions ? Bravo, vous êtes bien avancé(e) ! Dans le cas contraire, votre politique en matière de cybersécurité n'est pas encore totalement au point. Pas d'inquiétude, nous pouvons vous accompagner.

POURQUOI PRODWARE ?

Une approche cyber 360° :

Organisation & gouvernance

- RSSI interne ou externe
- Conseil en organisation Sécurité IT
- Démarche de certification ISO, CISSP, CISM, etc.

Audit

- Services d'audit méthodologiques, tests d'intrusion, scans automatiques
- Contrôle du Plan de Reprise d'Activité
- Recherche de compromission

Prévention

- Cyber-sensibilisation des employés
- Simulation d'attaques et de crises
- Service SOC pour prévenir, détecter et répondre aux menaces Cyber

Protection

- Sécurité des utilisateurs et des terminaux
- Sécurité périmétrique
- Sécurité des données et des systèmes

Remédiation

- Gestion d'incidents de sécurité et de crise Cyber via un CERT/CSIRT
- Analyse forensique
- Redémarrage du SI et Green zone
- Assurances, assistances juridique et psychologique

CONTACTEZ NOS EXPERTS CYBER

PRODWARE
45, quai de la Seine, 75019 Paris
+33 (0) 979 999 799
infos@prodware.fr