CAILLET Evan | DANDRE Alexis | BLOIS Arthur

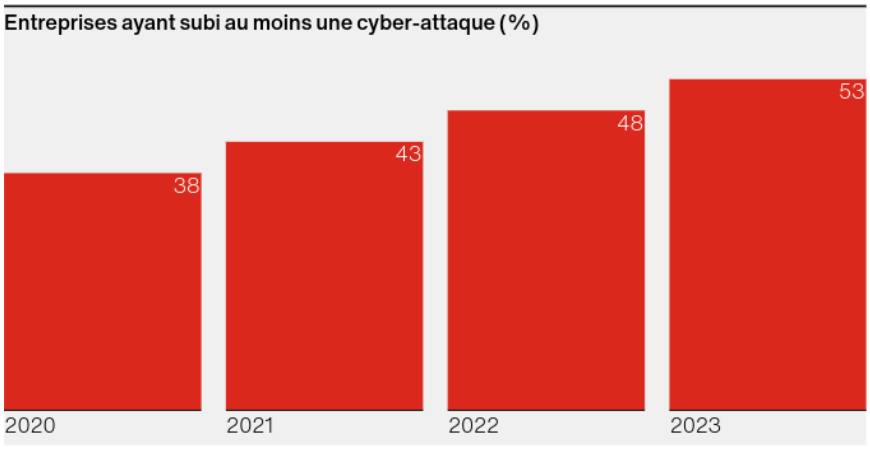
SAE 1.01 : Méthodologie d'une attaque

Introduction :

53% des entreprises ont subi une attaque en 2023, comparativement à 48% l'année précédente selon le rapport des cyber-risque Hiscox 2023. Cette hausse de 5 points en un an montre l'évolution alarmante des attaques informatiques. Mais dans 8 cas sur 10, le facteur humain est à l'origine de ces attaques. Il est donc essentiel de sensibiliser de plus en plus les utilisateurs sur le comportement à avoir.

Ici, nous voulons sensibiliser les utilisateurs sur la façon dont les attaquants procèdent. Plus particulièrement dans le cas d'un rançongiciel (ou "ransomware"), considérés comme les plus fréquentes et les plus coûteuses. Une attaque par rançongiciel consiste à voler et/ou chiffrer les données d'un système. Les attaquants vont ensuite demander une rançon contre laquelle ils ne diffuseront pas les données. Quels sont les moyens employés par les attaquants lors d'une cyberattaque, notamment de type rançongiciel et comment s'en protéger ?

Dans un premier temps, nous verrons la première étape d'une attaque qui est la reconnaissance dans un réseau informatique. Ensuite, nous verrons l'infiltration d'un attaquant et les techniques employées pour persister. Enfin, nous présenterons la propagation dans le système et la récupération des données souhaitées. Tout le long de notre présentation, nous développerons en parallèle le cas d'une attaque par rançongiciel.

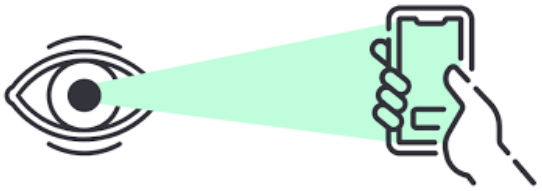


Source : Rapport Hiscox sur les cybers risques

I. La reconnaissance :

I.I. Identifier les cibles potentielles

La reconnaissance est la première étape d'un piratage. Elle consiste à collecter des informations sur la cible pour découvrir des vulnérabilités. Il existe deux types de reconnaissances : la reconnaissance passive et la reconnaissance active.



Source : Site Web : I Love PDF

La reconnaissance passive consiste à se renseigner sur la cible sans interagir directement avec lui. Les informations peuvent être collectés via différentes sources comme des réseaux sociaux ou des moteurs de recherche.

La reconnaissance active, contrairement à la reconnaissance passive, interagit directement avec la cible. C'est-à-dire que l'attaquant va s'engager directement dans un système pour trouver des faiblesses. Cela implique l'analyse de données et de sonder plus en détail le système, généralement introduit par un processus de "hameçonnage" ou "phishing". Ce type de reconnaissance est plus détectable qu'une reconnaissance passive.

Les attaquants adeptes d'une reconnaissance passive vont utiliser des outils spécifiques pour trouver des informations voire des vulnérabilités. Il existe des outils dans les moteurs de recherche, comme Google Hacking qui permet d'utiliser les requêtes natives d'un moteur de recherche pour accéder à des pages privés et donc des données sensibles. Toujours dans un moteur de recherche, nous avons des outils pour rechercher des noms de sous-domaine d'un organisme. Ils peuvent nous donner un aperçu des différents départements ou unités de travail de l'organisme. Ensuite, un attaquant peut se renseigner sur les acteurs d'un organisme via leurs réseaux sociaux.

En effet, certains utilisateurs publient des informations sur leurs activités et sur l'activité de leurs collègues.

Dans d'autres cas, les attaquants peuvent faire appel à des courtiers en accès initial. Ces cybercriminels obtiennent des accès non autorisés à un réseau. Ils vont généralement vendre leurs accès aux attaquants, ce qui leur permettra de passer l'étape de la reconnaissance. Les attaquants de type ransomware peuvent utilisés ces accès non autorisés, ce qui leur fait gagner énormément de temps (la phase de reconnaissance peut durer plusieurs semaines).

Pour résumer, la phase de reconnaissance permet de concentrer toutes les informations afin de définir un point d'attaque et de se concentrer sur celui-là.

I.II. Comment s'en protéger

Les risques liés au processus de reconnaissance par un attaquant dépendent des caractéristiques de l'organisme. En effet, les risques seront différents selon la nature de l'organisme, par exemple s'il s'agit d'un hôpital contenant des données médicales sensibles. En revanche, il y a trois risques majeurs que l'on retrouve dans chaque système :

La confidentialité : Vérifier les permissions d'accès aux données de l'organisme grâce à une hiérarchie et une base de données avec accès différents pour éviter des accès non autorisés aux données sensibles.

L'intégrité : Faire en sorte que les données ne soient pas modifiées sans autorisation par un tiers notamment lors d'un transfert. Utiliser une clé cryptographique unique pour vérifier que le fichier est authentique.

La disponibilité : Surveiller les données et l'accès aux données, contrôler les permissions pour éviter un vol ou un chiffrement lors d'une attaque par rançongiciel.

Il existe plusieurs moyens pour contrer cette phase de reconnaissance. Dans le cas d'une reconnaissance passive, il est essentiel de bien connaître les utilisateurs et prestataires qui utilisent le système informatique car les vulnérabilités les plus courantes sont des erreurs humaines. De plus, il faut être vigilant lors de l'utilisation de sa messagerie et ne pas communiquer des données sensibles sous peine d'être écouté par un attaquant (attaque passive "Man In the Middle"). Enfin, les utilisateurs doivent séparer leurs usages personnels et professionnels, notamment lors de la diffusion sur les réseaux sociaux de leur train de vie dans l'organisme. Ce genre de

choses permettrait à un attaquant, par exemple, de connaître le moment le moins protégé pour infiltrer le réseau. Il est donc important de préserver son identité numérique.

De l'autre côté, nous avons les reconnaissances actives. Pour cela, les administrateurs se doivent de mettre à jour les systèmes et logiciels puis sauvegarder régulièrement sur un serveur à part entière. De plus, il est essentiel de vérifier fréquemment l'accès à internet pour éviter une intrusion lorsque l'attaquant va tenter de balayer les ports du routeur pour trouver une entrée.

II. Intrusion et Persistance

II.I. Pénétrer dans le système de la victime

L'intrusion dans un système cible commence généralement par l'exploitation de vulnérabilités dans les dispositifs de sécurité, comme les failles dans les logiciels, les configurations réseau mal protégées ou les mots de passe faibles. Les attaquants peuvent utiliser des techniques telles que le phishing (mail se faisant passer pour notre banque ou autre), l'exploitation de failles Zero Day (failles que l'on ne connaissait pas encore et dont nous avons aucun correctif) ou encore l'ingénierie sociale (manipulation psychologique utilisé inciter une personne à divulguer des info perso/ effectuer une action compromettant le sécurité) pour obtenir un accès initial. Une fois à l'intérieur du réseau, ils cherchent à élever leurs privilèges pour avoir un contrôle plus étendu sur le système.

II.II. S'implanter durablement dans le système

Après avoir pénétré dans le système, les cybercriminels mettent en place des méthodes pour maintenir un accès persistant. Ils peuvent installer des malwares (logiciel malveillant) pour contrôler et surveiller les activités sur le système infecté ou des backdoors (Créer des comptes d'utilisateurs supplémentaires pour faciliter l'accès ultérieur au système) qui leur permettent de revenir dans le système sans être détectés, même après des redémarrages ou des mises à jour de sécurité. D'autres techniques incluent la modification de fichiers critiques ou l'insertion de scripts malveillants dans des processus légitimes, rendant l'attaque plus difficile à déceler. De plus, les

cybercriminels peuvent modifier les paramètres de sécurité du système ou encore désactiver les logiciels de protections tel qu'un antivirus. Toute cette phase d'action a pour but d'être détectable moins facilement par l'utilisateur infecté tout en prenant une place importante dans le système.

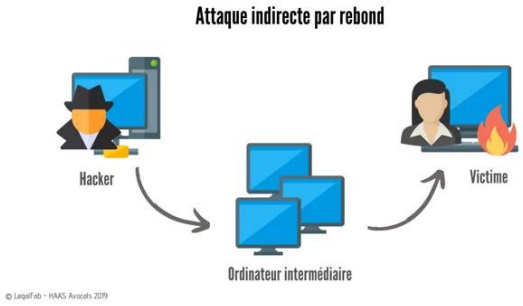
II.III. Comment s'en protéger

Pour se défendre contre ces attaques, il est crucial d'adopter une approche multicouche de la sécurité. Cela inclut l'utilisation de pare-feu et d'antivirus robustes, la mise en place de politiques de sécurité strictes et la sensibilisation des utilisateurs aux risques de phishing et d'ingénierie sociale. Les mises à jour régulières des logiciels et la surveillance active des systèmes peuvent également aider à identifier les comportements suspects et à bloquer les tentatives d'intrusion.

III. **Elévations de privilège et Actions**

III.I. Explorer et compromettre d'autres systèmes

Après s'être implanté dans le système, l'objectif suivant du malware va être de contaminer d'autres réseaux grâce notamment aux identifiants volés. Grâce à ces identifiants, le malware se connecte à d'autres machines pour les infecter également dans le but de trouver une machine administrateur et avoir plus d'emprise sur le réseau. On appelle cela une attaque indirecte par rebond.



Celui-ci peut également rechercher d'autres vulnérabilités ou utiliser différentes techniques « de persistance et d'évasion » afin d'éviter la détection et de contrôler davantage de ressources informatiques, toujours dans le but de contaminer d'autres machines du réseau. Toute cette phase d'action est appelée le mouvement latéral.

III.II. Voler et exploiter les informations sensibles

Une fois dans le réseau d'une entreprise, le cybercriminel peut dévoiler des informations récupérées sur les ordinateurs de l'entreprise. Cela a pour but de faire baisser la notoriété de cette entreprise et donc diminuer la confiance de ces clients. De plus, ils

peuvent chiffrer les données déposées sur les serveurs afin de demander une rançon tout en bloquant les activités de l'entreprise voir obtenir l'accès à des systèmes critiques pour causer des perturbations ou des dommages. Dans le cas d'un ransomware, le logiciel va crypter vos données pour ensuite demander une rançon. Si vous ne la payez pas, le cybercriminel peut détruire ou divulguer les données personnelles de votre ordinateur.

III.III. Comment s'en protéger

Pour s'en protéger, on peut tout d'abord effectuer des analyses récurrentes des différentes machines grâce à un antivirus. S'il s'avère qu'une des machines est infectée par un virus, il faut alors l'isolée du reste du réseau, c'est-à-dire, la déconnecter du réseau internet (wifi + Ethernet). Il ne faut surtout pas éteindre l'appareil car certains fichiers temporaires peuvent être la preuve d'une attaque ou contenir des informations utiles afin de comprendre d'où provient cette attaque. En éteignant l'ordinateur, ces fichiers disparaitront et il sera difficile de contrer l'attaque. Il faut ensuite contacter au plus vite le support informatique et prévenir le reste du personnel de ne plus utiliser la machine infectée. Dans le cas du ransomware, il ne faut surtout pas payer la rançon demandée car vous n'êtes pas sûr de récupérer l'accès à vos données.

Conclusion :

Pour conclure, nous avons vu qu'une cyberattaque se fait en cinq temps, la reconnaissance, l'intrusion, la présence, le mouvement latéral et enfin l'Acquisition. De nombreuses façons de s'en protéger existent mais les plus évidentes sont la sécurisation des postes et du réseau via des antivirus et des pares-feux. De plus la prévention auprès des employés d'une entreprise peut également jouer un rôle crucial dans la protection de l'entreprise.