

ATTAQUES ET VULNÉRABILITÉS

MALWARES ET AUTRES SCHÉMAS D'ATTAQUE

INDICATEURS DE COMPROMISSION

- Quelque chose qui indique (avec un haut degré de confiance) une intrusion informatique
 - trafic réseau sortant élevé
 - anomalies dans les requêtes DNS
 - port d'application non conformes
 - activité anormale d'un compte administrateur...

MALWARES

- **Malware** = *Malicious Software* (logiciel malveillant)
- Exploite toujours une/des vulnérabilité(s) (notamment logicielles mais pas uniquement)
- Objectifs:
 - amusement, hacktivisme, destruction, **profit**
- Quelques types de malwares: virus, ver, rootkit, ransomware, keylogger, adware, cheval de Troie, spyware...

PRÉVENTION FONDAMENTALE

1. Mises à jour logicielles
2. Antivirus à jour
3. Ne pas télécharger/exécuter des fichiers de nature incertaine
 - **notamment les liens et les pièces jointes dans les emails**
 - inciter les utilisateurs à demander assistance en cas de doute

VIRUS

- Code malicieux qui requiert une interaction utilisateur pour s'installer
- Comme un virus biologique, le virus informatique tente de **se dupliquer** dès qu'il le peut (infecte d'autres programmes lancés, y compris depuis le réseau)
 - *MyDoom* (2004): 2 millions PCs infectés, 30 milliards € de dommages
 - *Conficker* (2009): 3,5 millions PCs infectés, 8 milliards € de dommages
- Les plus virulents mettent entre 10 minutes et 96 heures pour se répandre (moyenne 24 h)

VER (WORM)

- Un peu comme un virus, sauf qu'il ne requiert pas en général d'interaction utilisateur (il s'auto-propage)
- **Ver réseau**
 - exploite des vulnérabilités réseau pour se propager
- **Ver email**
 - distribue des copies de lui-même dans un exécutable infecté attaché à des emails

PUP

- PUP = *Potentially Unwanted Program* (programme potentiellement indésiré)
 - *adware, spyware*, barre de recherche de navigateur...
- Est typiquement inclus dans un programme utilitaire
 - lors de l'installation, le programme vous incite à installer ces PUP en supplément

CHEVAL DE TROIE (TROJAN HORSE)

- Logiciel apparemment anodin qui contient un autre logiciel, quant à lui malveillant (charge utile ou *payload*)
- L'application de base semble fonctionner de manière normale, ce qui contribue à ne pas alerter la victime
- Parfois le *trojan* télécharge la charge utile depuis internet
 - ex.: RAT (*Remote Access Tool*), permettra à l'attaquant, à distance, de télécharger/téléverser des fichiers, allumer et consulter la caméra, lancer un *keylogger*, etc.

BOTNET

- **Botnet** = réseau d'ordinateurs « zombies »
 - ordinateurs infectés par un malware (quel que soit le moyen d'infection)
 - le malware permet à l'attaquant de prendre le contrôle des ressources à distance
 - le contrôle se fait par l'intermédiaire d'un serveur dit *Command & Control* (C&C)
 - le C&C peut contrôler des milliers de *bots zombies* en même temps
- Objectif: utiliser cette énorme puissance pour lancer une attaque de grande ampleur, à la demande, sur une cible spécifique

BOMBE LOGIQUE

- Code malicieux qui se déclenche seulement après un certain temps
 - à une date prédéfinie
 - ou lorsqu'il détecte une activité spécifique
- Le code en question peut déclencher des actions de tout type
 - dysfonctionnement du système
 - communication avec un serveur
 - chiffrement
 - exfiltration de données...

KEYLOGGER

- Logiciel malveillant qui capture toutes les entrées clavier de la machine cible
 - identifiants de connexion
 - numéros de CB
 - données et conversations personnelles ou professionnelles
 - toute information sensible...
- Les fichiers de retranscription sont ensuite:
 - envoyés à un serveur externe (par email ou *upload*)
 - ou stockés localement pour récupération ultérieure

LOGICIEL ESPION (SPYWARE)

- Logiciel qui capture l'**activité de l'utilisateur** et transmet à l'attaquant
 - capture clavier (*keylogger*)
 - historique de navigation
 - autres données...
- Souvent injecté lors de l'installation d'un logiciel quelconque

ROOTKITS

- Code malveillant qui s'installe au niveau de l'OS ou du noyau pour maintenir un accès **caché et privilégié**
 - en gros, le code est activé avant le système
 - ça lui permet d'éviter la détection par anti-malware en désactivant tout ou partie de ce qui permet de les trouver
- Contre-mesure: des logiciels spécifiques comme TDSSKiller (*rootkit removing tool* de Kaspersky) vont:
 - scanner services et pilotes
 - et également le secteur de boot de la machine

PORTE DÉROBÉE (BACKDOOR)

- Logiciel installé dans le but d'ouvrir des accès depuis l'extérieur
 - l'attaquant peut ensuite agir sur le système comme s'il s'y était connecté
- Lors d'une attaque de pénétration réussie, un attaquant va souvent tenter d'installer une *backdoor* pour pouvoir se réintroduire discrètement dans le système sans avoir à relancer à nouveau le (potentiellement long et difficile) processus de l'attaque originale

SPRAYING

- Principe:
 - on a récupéré (fuite, achat...) un grand nombre d'identifiants/pseudos
 - mais on ne connaît ni les sites ni les mots de passe associés
 - on va utiliser un programme qui va tester chacun de ces identifiants sur une cible donnée (site, programme, tout accès qui requiert de s'authentifier par mot de passe)
 - tout en essayant de casser le mot de passe
- Exemple de contre-mesure: 2FA

ATTAQUE PAR RÉTROGADATION (DOWNGRADE ATTACK)

- Force un système à passer à un mode de communication de sécurité inférieure
 - le pirate configure sa version ancienne (protocoles de sécurité obsolètes)
 - il l'utilise pour contacter un service capable de communiquer à la pointe de la sécurité
 - mais ce service est également configuré pour accepter les communications avec les clients anciens, en **ajustant (diminuant) son propre niveau de sécurité**
 - il ne reste plus au pirate qu'à utiliser une faille connue sur cette ancienne version pour effectuer son attaque

ATTAQUES PAR PÉRIPHÉRIQUE EXTERNE

- Une simple clé USB peut être un vecteur d'attaque physique très efficace
 - contient des malwares plantés dans les fichiers
 - aucune action utilisateur requise si *auto-load* activé sur le système
 - USB Killer
 - ...
- *Juice Jacking*: ports USB de recharge malveillants

ATTAQUE DE LA CHAÎNE LOGISTIQUE (SUPPLY CHAIN ATTACK)

- L'attaque vise un élément moins sécurisé de la chaîne
 - l'élément infecté « remonte » la chaîne pour finalement pénétrer le coeur de l'organisation
- Exemples:
 - équipement quelconque infecté avant d'être livré à l'organisation
 - fonctionne aussi avec des programmes : des composants logiciels développés ailleurs peuvent avoir été modifiés avant d'être rapatriés et utilisés en interne dans l'organisation

CLOUD VS « SUR SITE »

- Qu'est-ce qui est plus sécurisé?
 - installer et maintenir toute son infrastructure **sur site** (*on-premises*)?
 - ou utiliser des services **cloud** pour remplacer l'infrastructure sur site?
- Réponse: ça dépend!
 - législation / conformité, activités de l'organisation, expertise en place
 - coûts d'abonnement vs coûts de maintien et de renouvellement
 - fréquence et volume d'accès aux données
 - mobilité des données (changer de fournisseur cloud?)

ATTAQUE DE MOTS DE PASSE

- Deux grandes techniques:
 - **force brute**
 - *rainbow tables*

Mais d'abord, c'est quoi une attaque de mot de passe ?

TRANSFERT ET STOCKAGE DE MOT DE PASSE SUR SERVEUR

- Un mot de passe ne doit **jamais** transiter « en clair »
- Il doit être d'abord **haché** et le serveur ne doit connaître et stocker que la version hachée

ATTAQUE PAR FORCE BRUTE

- **Principe:** tentative systématique de toutes les possibilités
 - trouvera tous les mots de passe courts car teste toutes les combinaisons
- **Contre-mesures:**
 - accès qui bloque après X tentatives infructueuses
 - temps de cassage augmente exponentiellement avec la taille du mot de passe

FORCE BRUTE - DICTIONNAIRE

- **Principe**: on dispose d'un grand ensemble de mots qui ont des chances d'être utilisés comme mot de passe
 - c'est le **dictionnaire**
 - plutôt que d'essayer *toutes* les combinaisons, **on va se contenter d'essayer tous les mots du dictionnaire**
- Très efficace:
 - mots que les gens utilisent car faciles à retenir
 - souvent issus de bases de mots de passe réels qui ont fuités
 - et ça rend les mots de passe longs non aléatoires beaucoup plus fragiles

FORCE BRUTE - ATTAQUE HYBRIDE

- On va combiner dictionnaire et techniques de force brute pure
- À partir d'un mot du dictionnaire, on construit des variations
- Ex: le dictionnaire contient *jeanmichel*
 - *Jeanmichel*
 - *JEANMICHEL*
 - *jeanmichel123*
 - *Jeanmichel!*
 - *J34NM1CH31 (leetspeak)*

RAINBOW TABLES

- Liste précalculée de mots de passe hachés
 - réduit **grandement** le temps de cassage (on doit juste comparer les *hashes*)
 - mais augmente **drastiquement** la taille de stockage nécessaire (Tb)
 - d'autant qu'il faut une *rainbow table* pour chaque type de hachage
- Contre-mesure: **salage**

SÉCURITÉ DES MOTS DE PASSE

- Taille = élément le plus important
 - min 12, 16 recommandé
- Casse + nombres + cars spéciaux bienvenus, mais *moins primordiaux qu'on ne le pense*
- Éviter mots du dictionnaire
 - y compris variations ((H@CK3R\$...))
 - et les patterns usuels (Monsupermotdepasse123!)
 - sauf si passphrase!

SÉCURITÉ DES MOTS DE PASSE (2)

- Éviter éléments personnels (dates de naissance, prénoms...)
- **Utiliser mots de passe uniques pour différents comptes**
 - *Credential Stuffing*
- Dans tous les cas, le mot de passe n'a-t-il pas déjà été compromis?
 - haveibeenpwned.com/passwords

BONNE PRATIQUE : GESTIONNAIRE DE MOTS DE PASSE

- Garantit **unicité** et **force** des mots de passe (si correctement configuré)
- Lastpass, 1password, **Keepass...**

RANÇONGICIEL

- Chiffre les données sur le PC infecté (et les données auxquelles il peut avoir accès sur le réseau)
 - accès aux données rendu impossible
- Propose le paiement d'une rançon pour récupérer les données
- Paiement en Bitcoin ou autre crypto-monnaie (intraçable)
 - 100-500€ pour utilisateur isolé ou TPE
 - et bien plus en fonction de la taille de l'entreprise
- *WannaCry, NotPetya*