Université de
Versailles – Saint-Quentin-en-Yvelines

TER M1

Ransomware

Par :

Youcef El Khodr Metane

Baysan Yenal

Imad Boukedjani

Oscar Cornejo Guillen

Meribout Ahmed Yahia

Supervisé par : Prof. YANN ROTELLA

Sommaire

Chapitre 1

Généralités

1.1 Introduction

Depuis l'avènement d'internet et des réseaux en général, les cyber-attaques n'ont cessé de se multiplier. Parmi les nombreuses menaces qui planent dans le monde numérique, les ransomware sont sans doute l'un des plus dévastateurs.

Dans ce projet, nous nous concentrerons spécifiquement sur cette catégorie d'attaques. Nous explorerons en détail le fonctionnement de ces logiciels malveillants tout en partageant le processus de création de notre propre ransomware.

1.2 Définition d'une cyberattaque

Une cyberattaque est tout effort intentionnel visant à voler, exposer, modifier, désactiver ou détruire des données, des applications ou d'autres actifs via un accès non autorisé à un réseau, un système informatique ou un appareil numérique.
Les cybercriminels s'introduisent généralement dans les réseaux informatiques à la recherche de quelque chose de précis. En voici les exemples les plus courants :

- L'argent,
- Les données financières des entreprises,
- Les listes de clients,
- Les données client, y compris les informations personnelles identifiables (PII) ou d'autres données personnelles sensibles,
- Les adresses e-mail et identifiants de connexion,
- Les formes de propriété intellectuelle, comme les secrets commerciaux ou les conceptions de produits.

1.3 Secteur de la cybersécurité

La cybercriminalité étant un problème majeur, le secteur de la sécurité se positionne comme une industrie massive. Selon les estimations, il serait estimé à 182,86 milliards USD en 2023 et devrait attendre les 314 milliards d'ici 2028. [4]

1.4 Définition d'un malware

Un malware, abréviation de « logiciel malveillant », est tout code logiciel ou programme informatique écrit intentionnellement pour nuire à un système informatique ou à ses utilisateurs. Presque toutes les cyberattaques modernes impliquent un certain type de malware. Ces programmes malveillants peuvent prendre de nombreuses formes, depuis des ransomwares coûteux et très dommageables jusqu'à de simples logiciels publicitaires ennuyeux, selon les intentions des cybercriminels.[1]

- **Vers** sont des programmes malveillants auto-répliquants qui peuvent se propager entre les applications et les appareils sans interaction humaine (contrairement à un virus, qui ne peut se propager que si un utilisateur exécute un programme compromis). Si certains vers ne font que se propager, beaucoup ont des conséquences plus graves. Par exemple, le ransomware WannaCry, qui a causé des dommages estimés à 4 milliards d'USD, était un ver qui a maximisé son impact en se propageant automatiquement entre les appareils connectés.
- **Les cryptojackers** Un cryptojacker est un logiciel malveillant qui prend le contrôle d'un appareil et l'utilise pour miner de la crypto-monnaie, comme le bitcoin, à l'insu de son propriétaire. Les cryptojackers créent essentiellement des botnets de minage de cryptomonnaies.
- **Cheval de Troie** se déguisent en programmes utiles ou se cachent dans des logiciels légitimes pour inciter les utilisateurs à les installer. Un cheval de Troie d'accès à distance ou « RAT » (pour « remote access Trojan ») crée une porte dérobée secrète sur l'appareil infecté. Un autre type de cheval de Troie, appelé « dropper », installe d'autres logiciels malveillants une fois qu'il s'est implanté. Ryuk, l'une des souches récentes de ransomware les plus dévastatrices, a utilisé le cheval de Troie Emotet pour infecter des appareils.

D'autres types de malware sont les virus informatiques, les logiciels malveillants sans fichier, les logiciels malveillants d'accès à distance, etc.

1.5 Définition d'un ransomware

Un ransomware est un type de malware qui verrouille les données ou l'appareil d'une victime et menace de le maintenir verrouillé et qui exigent le paiement d'une rançon pour restaurer l'accès aux données.
Les attaques de ransomware représentaient 17 % de toutes les cyberattaques en 2022. Ces

dernières années, les cyberattaques contre rançon incluent des attaques de double et triple extorsion et actuellement, nous disposons de très peu de temps pour détecter et combattre ces éventuelles attaques. Les attaques de double extorsion ajoutent à la menace de voler les données de la victime et de les divulguer en ligne. Les attaques de triple extorsion menacent en plus d'utiliser les données volées pour attaquer les clients ou les partenaires commerciaux de la victime. Selon le rapport 2022 sur le coût d'une violation de données d'IBM, le coût moyen d'une violation de données causée par une attaque par ransomware, sans compter le paiement de la rançon, s'élevait à 4,54 millions d'USD. Les attaques par ransomware devraient coûter aux victimes environ 30 milliards de dollars en 2023.[2]

1.5.1 Types de ransomware

1. **Crypto ransomware**
   L'objectif des ransomwares Crypto est de chiffrer des données importantes, comme des documents, des photos et des vidéos, mais pas d'interférer avec les fonctions de base de l'ordinateur. Cette action sème la panique car les utilisateurs peuvent voir leurs fichiers, mais ne peuvent pas y accéder. Les concepteurs de ransomwares Crypto ajoutent souvent un compte à rebours à leur demande de rançon : « Si vous ne payez pas la rançon avant la date limite, tous vos fichiers seront supprimés ». Or, étant donné le nombre d'utilisateurs qui ne sont pas conscients de la nécessité d'effectuer des sauvegardes dans le cloud ou sur des appareils de stockage physique externes, les ransomwares Crypto peuvent avoir des effets dévastateurs. Par conséquent, de nombreuses victimes paient la rançon dans le seul but de récupérer leurs fichiers.[3]

2. **Locker ransomware**
   La forme la moins courante de ransomware, appelée ransomware sans chiffrement ou ransomware à verrouillage d'écran, verrouille l'ensemble de l'appareil de la victime, généralement en bloquant l'accès au système d'exploitation, et il peut aussi chiffrer les données. Au lieu de démarrer comme d'habitude, l'appareil affiche un écran qui présente la demande de rançon. Ce type de ransomware ne cible généralement pas des fichiers critiques.

Ces deux types de programmes peuvent être divisés en plusieurs sous-catégories :

— Le leakware/doxware.

— Le ransomware mobile.

— Les wipers ou ransomwares destructeurs.

— Le scareware.

1.5.2 Les étapes d'une attaque par ransomware

Une attaque par ransomware suit généralement les étapes suivantes.

1. **Reconnaissance. -** La phase de reconnaissance constitue le premier pas dans une attaque, impliquant la recherche minutieuse de cibles potentielles avant toute tentative de pénétration. Cette phase englobe l'identification des cibles, la recherche de leurs failles de sécurité, la détection des tiers connectés à ces cibles (et des données auxquelles ils ont accès), ainsi que l'exploration des points d'entrée existants et potentiels. La reconnaissance peut s'effectuer à la fois en ligne et hors ligne.
2. **Accès initial. -** Les vecteurs d'accès les plus courants pour les attaques par ransomware restent l'hameçonnage et l'exploitation de vulnérabilités.
3. **Post-exploitation. -** En fonction du vecteur d'accès initial, cette deuxième étape peut impliquer un outil d'accès à distance intermédiaire ou un logiciel malveillant avant d'établir un accès interactif.
4. **Compréhension et propagation. -** Les attaquants s'efforcent de comprendre le système local et le domaine auxquels ils ont accès et d'accéder à d'autres systèmes et domaines (ce qu'on appelle le déplacement latéral).
5. **Collecte et exfiltration des données. -** À ce stade, les opérateurs de ransomware se concentrent sur l'identification des données de valeur et leur exfiltration (vol), généralement en exportant une copie. Ils se concentrent généralement sur les données particulièrement précieuses (identifiants de connexion, informations personnelles des clients, propriété intellectuelle) qu'ils peuvent utiliser dans le cadre d'une double extorsion.
6. **Déploiement et envoi du message. -** Le crypto ransomware commence à identifier et à chiffrer les fichiers. Certains ransomwares de chiffrement désactivent également les fonctions de restauration du système, ou suppriment ou chiffrent les sauvegardes sur l'ordinateur ou le réseau de la victime, afin d'accroître la pression exercée pour obtenir la clé de déchiffrement. Les ransomwares sans chiffrement verrouillent l'écran de l'appareil, l'inondent de fenêtres pop-up ou empêchent la victime d'utiliser l'appareil d'une autre manière. Une fois les fichiers chiffrés et/ou l'appareil désactivé, le ransomware avertit la victime de l'infection, souvent par le biais d'un fichier .txt déposé sur le bureau de l'ordinateur ou d'une fenêtre pop-up. Le message de rançon contient des instructions sur la manière de la payer, généralement en crypto-monnaie ou par une méthode similaire non traçable, en échange d'une clé de déchiffrement ou d'un retour à la normale.

1.6 Historique des ransomware

Les dernières décennies ont été énormément touchés par ces ransomwares, on pourra citer Wannacry, CryptoLocker ou bien même LockBit. Ces logiciels ont causé d'importants dégâts, ce qui a participé à leur médiatisation. Nous allons voir comment fonctionne ces ransomware et quels sont leurs particularités qui les ont permis d'être les plus devastateurs.

1. **CryptoLocker**
2. **WannaCry**
3. **LockBit**

1.7 Exemples des Vulnérabilités utilisées

- **Microsoft Windows et Office** Il y avait beaucoup de défauts Zero-Day [1] dans les produits Microsoft en 2023, mais l'un des plus importants était CVE-2023-36884 [2], une vulnérabilité d'exécution de code à distance (RCE) dans Windows Search. La faille, qui a été révélée pour la première fois dans Microsoft Juillet Patch Tuesday release, affecte à la fois les logiciels Windows et Office. Deux aspects distinguent CVE-2023-36884 des autres jours zéro de Microsoft l'année dernière. Premièrement, la faille RCE n'avait pas de correctif au moment de la divulgation, bien que Microsoft ait offert des mesures d'atténuation pour empêcher l'exploitation. La vulnérabilité a finalement été corrigée dans la version August Patch Tuesday. Deuxièmement, Microsoft a révélé qu'un groupe cybercriminel russe qu'il suit comme Tempête- 0978 exploité CVE-2023-36884 dans une campagne de phishing axée sur l'espionnage ainsi que des attaques de ransomware motivées financièrement. Selon Rapport de microsoft, La campagne de Storm-0978 a ciblé des organisations de défense et des entités gouvernementales en Amérique du Nord et en Europe. Les e-mails de phishing présentaient des leurres liés à l'OTAN et au Congrès mondial ukrainien, et les attaquants ont exploité CVE-2023-36884 pour contourner la fonctionnalité de sécurité Mark of the Web (MotW) de Microsoft, qui bloque généralement les liens et les pièces jointes malveillants.[5]
- **Ethernal blue** est un exploit développé par la NSA [3]. Il est révélé et publié par le groupe de hackers The Shadow Brokers le 14 avril 2017.

  Cet exploit utilise une faille de sécurité présente dans la première version du protocole SMB (SMBv1) [4]. Bien que cette faille de sécurité ait déjà été résolue par Microsoft par une mise à jour de sécurité publiée le 14 mars 2017 (MS17-010 [archive]), de nombreux utilisateurs de Windows n'avaient toujours pas installé ce correctif de sécurité lorsque, le 12 mai 2017, le ransomware « WannaCry » utilise cette faille de sécurité pour se propager.

  En raison de la gravité de l'attaque de WannaCry, Microsoft prend la mesure inhabituelle de publier une mise à jour de sécurité pour les systèmes d'exploitation qu'il ne maintient plus, comme Windows XP, Windows 8 et Windows Server 2003.

  Cet exploit a également été utilisé pour les cyberattaques Adylkuzz (survenue quelques jours après WannaCry) et NotPetya (survenue le 27 juin 2017). [6]

1. Zero-Day : est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive.
2. CVE : common vulnerabilities and exposures
3. NSA : National Security Agency
4. SMB : Server Message Block

1.8 Conclusion du chapitre

TODO

Bibliographie

[1] IBM. Malware. https://www.ibm.com/fr-fr/topics/malware.

[2] IBM. Ransomware. https://www.ibm.com/es-es/topics/ransomware.

[3] Kaspersky. Reconnaître les ransomwares : quelles sont les différences entre les chevaux de Troie de chiffrement ? https://www.kaspersky.fr/resource-center/threats/ransomware-attacks-and-types.

[4] Mordor Intelligence. Secteur de la cybersécurité. https://www.mordorintelligence.com/fr/industry-reports/cyber-security-market.

[5] Techtarget. Microsoft Windows et Office. https://www.techtarget.com/searchsecurity/feature/10-of-the-biggest-zero-day-attacks-of-2023.

[6] Wikipedia. EternalBlue. https://fr.wikipedia.org/wiki/EternalBlue.