Incident WannaCry

Alann HOFFMANN
MEWO

SOMMAIRE

Table des matières

COMMENT L'INCIDENT A DÉMARRÉ

Date de démarrage : 12 mai 2017

L'attaque a commencé en Espagne et au Royaume-Uni avant de se propager à l'échelle mondiale en quelques heures. La première nuit, environ 100 000 systèmes Windows avaient déjà été infectés.

RANSOMWARE (RANÇONGICIEL) *Malware qui chiffre les fichiers d'une victime pour les rendre inaccessibles, puis exige le paiement d'une rançon en cryptomonnaies pour fournir la clé de déchiffrement.*

LES VULNÉRABILITÉS EXPLOITÉES

I. Eternal Blue (vulnérabilité principale)

- **Faille** : Vulnérabilité dans le protocole **SMB (Server Message Block)** de Microsoft Windows
- **Protocole SMB** : Système de partage de fichiers entre ordinateurs sur un réseau
- **Port exploité** : TCP 445
- **Origine** : Découverte originalement par la **NSA** (Agence nationale de sécurité américaine)
- **Caractéristique** : Permettait aux attaquants de :
- Découvrir les ordinateurs vulnérables sur le réseau
- Infecter les systèmes **sans intervention de l'utilisateur** (pas de clic sur lien malveillant nécessaire)
- Se propager latéralement d'un ordinateur à l'autre automatiquement

II. Double Pulsar (porte dérobée secondaire)

- **Type** : Backdoor (porte dérobée) de la NSA
- **Fonction** : Permettait d'installer et d'exécuter du code supplémentaire sur les systèmes déjà compromis
- **Installation** : Via l'exploitation de la vulnérabilité SMB (MS17-010)

CHRONOLOGIE DE LA DIVULGATION

- **Août 2016** : Le groupe **Shadow Brokers** vole les cyberarmes de la NSA, incluant Eternal Blue
- **Mars 2017** : Microsoft publie le correctif MS17-010 pour corriger la vulnérabilité
- **14 avril 2017** : Shadow Brokers rend public l'exploit Eternal Blue sur Internet
- **12 mai 2017** : WannaCry commence son attaque (28 jours après la divulgation publique)

I. POURQUOI L'ATTAQUE A ÉTÉ SI DESTRUCTRICE

- **Systèmes non à jour** : Beaucoup d'ordinateurs n'avaient pas appliqué le correctif de mars 2017
- **Systèmes obsolètes** : Windows XP et autres anciennes versions non supportées étaient particulièrement vulnérables
- **Propagation automatique** : Contrairement aux ransomwares classiques (par email), WannaCry se propageait seul sans action de l'utilisateur
- **Vitesse** : L'exploit Eternal Blue permettait une propagation extrêmement rapide d'un ordinateur à l'autre sur les réseaux d'entreprise
- C'est précisément ce qui en a fait une "**pandémie numérique**" mondiale.

IMPACTS DE L'INCIDENT

I. Impact Économique

L'attaque WannaCry a causé des dommages estimés entre plusieurs centaines de millions et plusieurs milliards de dollars. Ces coûts englobent l'interruption des activités, la remise en état des systèmes informatiques et la restauration des données perdues. Des exemples spécifiques illustrent l'ampleur des pertes : le NHS au Royaume-Uni a subi des pertes de 92 millions de livres sterling, tandis que Renault a perdu 220 millions d'euros de chiffre d'affaires et 80 millions d'euros de résultat d'exploitation.

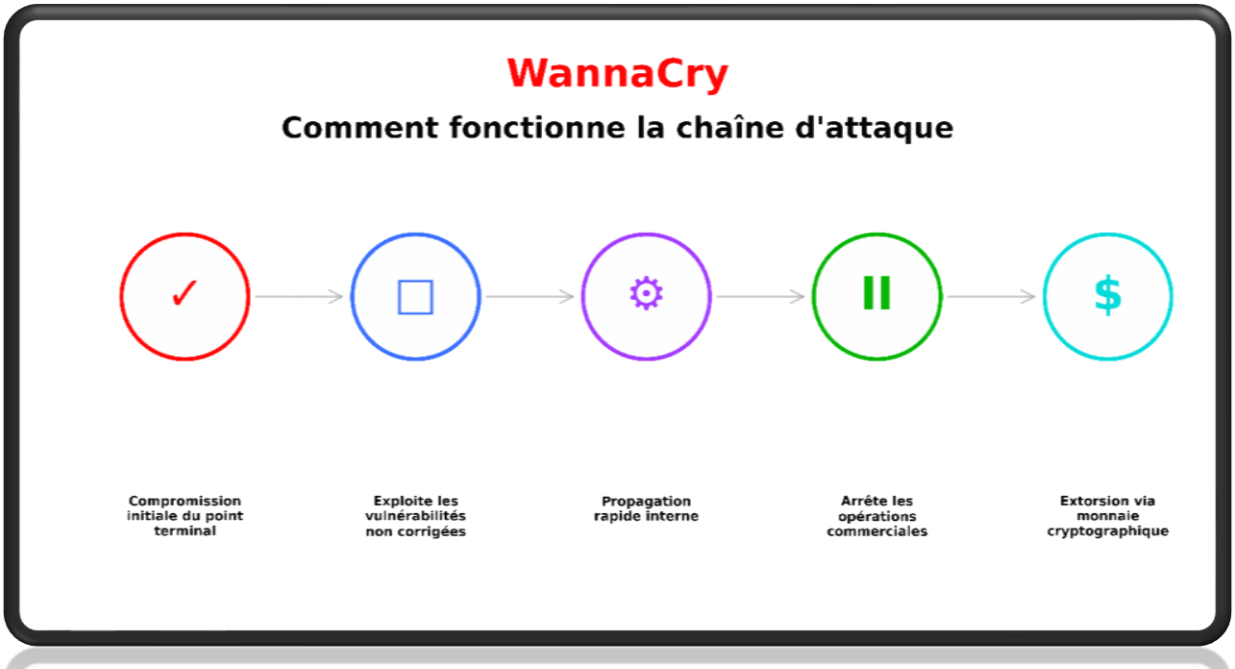
II. Impact Opérationnel et Services Critiques

Le secteur de la santé a été particulièrement touché par cette attaque. Au Royaume-Uni, un tiers des centres hospitaliers du NHS ont été affectés par WannaCry, ce qui a entraîné l'annulation de 19 000 rendez-vous. La situation a été critique au point que des ambulances ont dû être détournées, laissant sans assistance des patients en situation d'urgence. De plus, les médecins se sont retrouvés privés d'accès aux dossiers médicaux de leurs patients.

Au-delà du secteur santé, de nombreux autres secteurs ont subi des perturbations majeures. Les télécommunications ont été affectées, notamment Telefónica en Espagne. Le secteur du transport et de la logistique, avec FedEx et d'autres entreprises, a connu des interruptions significatives. L'industrie automobile a également été durement touchée, avec Renault et Nissan forcées d'arrêter certaines chaînes de production.

III. Ampleur Globale

L'ampleur de cette cyberattaque a été sans précédent à l'échelle mondiale. Entre 200 000 et 300 000 ordinateurs ont été infectés selon les différentes sources. L'attaque s'est propagée dans plus de 150 pays simultanément. En Chine seule, 29 000 organisations ont été touchées, incluant des hôpitaux, des distributeurs automatiques de billets et des sociétés privées. En comparaison, la France a été relativement épargnée avec moins d'une dizaine d'entreprises affectées selon l'ANSSI.

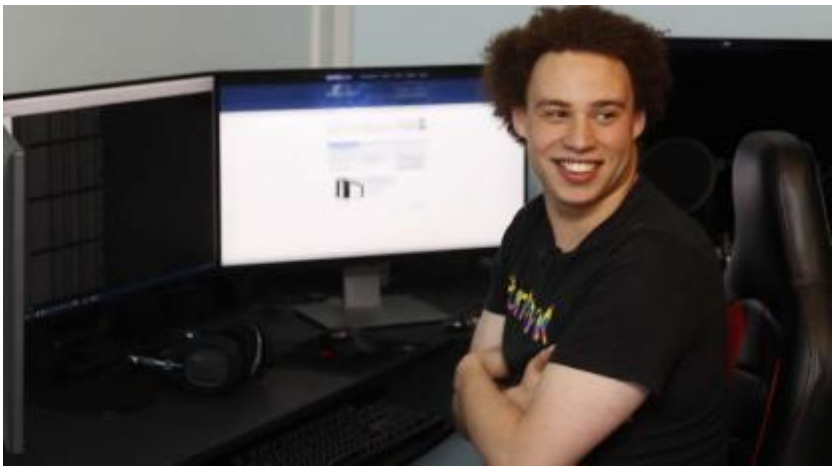


RÉPONSES À L'INCIDENT

I. Réponses Immédiates (Mai 2017)

Microsoft a réagi rapidement en accélérant la publication de correctifs. La société a pris une décision exceptionnelle en fournissant des mises à jour de sécurité pour les versions de son système d'exploitation qui n'étaient plus supportées, notamment Windows XP, Windows 8 et Windows Server 2003.

De son côté, la communauté des chercheurs en sécurité a joué un rôle crucial dans l'arrêt de l'épidémie. Un chercheur en sécurité nommé Marcus Hutchins, connu sous le pseudonyme MalwareTech, a découvert un "kill switch" (interrupteur d'arrêt) intégré au malware. Il a détecté un domaine qui n'avait pas été enregistré par les attaquants et qui était codé dans le malware. En enregistrant ce domaine, il a pu bloquer la propagation de WannaCry. Cet oubli des attaquants, digne de pirates amateurs, s'est avéré décisif pour arrêter l'épidémie mondiale.



Marcus Hutchins, la personne ayant découvert le « kill switch » de WannaCry

II. Enquêtes et Mesures Légales

En France, le Parquet de Paris a ouvert une enquête en flagrance qui a été confiée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Cette enquête portait sur des accusations d'accès frauduleux à des systèmes informatiques, d'entrave au fonctionnement de ces systèmes et d'extorsions.

Au niveau européen, Europol, la police européenne, a lancé sa propre enquête sur l'incident. L'agence a qualifié l'attaque de "niveau sans précédent" et a émis un appel officiel à ne pas payer les rançons demandées par les cybercriminels.

Sur la scène internationale, fin 2017, les États-Unis et le Royaume-Uni ont attribué l'attaque à la Corée du Nord. Cependant, cette attribution reste contestée par certains chercheurs en sécurité.

OFAC anciennement OCLCTIC le changement a eu lieu en décembre 2023

III. Mesures de Sécurité et Prévention

Les organisations ont réagi en augmentant significativement leurs investissements en cybersécurité. Elles ont amélioré leurs politiques de patch management, c'est-à-dire leur système de mise à jour régulière des correctifs de sécurité. La sensibilisation des utilisateurs aux risques numériques a également été renforcée, et nombreuses sont celles qui ont mis en place des sauvegardes régulières de leurs données.

Les gouvernements ont également pris des mesures de fond. Ils ont renforcé leurs politiques de cybersécurité, amélioré la coordination entre les agences de sécurité et développé des protocoles structurés de réponse aux incidents de cybersécurité.

LEÇONS APPRISES

L'incident WannaCry a mis en lumière plusieurs enseignements majeurs pour la sécurité informatique.

- Premièrement, il a démontré l'importance critique de l'application régulière des mises à jour de sécurité. Le correctif pour la vulnérabilité exploitée existait depuis deux mois avant l'attaque, mais n'avait pas été appliqué par de nombreuses organisations.

- Deuxièmement, l'attaque a révélé les risques importants posés par les systèmes informatiques obsolètes, en particulier Windows XP et les anciennes versions de Windows qui étaient particulièrement vulnérables.

- Troisièmement, WannaCry a démontré le danger des Vulnérabilités réseau par rapport aux vecteurs d'attaque traditionnels comme l'email malveillant, car elle pouvait se propager automatiquement sans intervention de l'utilisateur. Quatrièmement, l'attaque a souligné que les systèmes critiques, notamment ceux du secteur santé, doivent bénéficier d'une protection renforcée. Cinquièmement, WannaCry a illustré comment les failles de sécurité découvertes par des agences gouvernementales peuvent devenir des armes lorsqu'elles sont volées et divulguées publiquement. Sixièmement, l'incident a rappelé l'importance cruciale de disposer de sauvegardes régulières, car les données peuvent être restaurées si des copies de secours existent.

EXPLICATION D'UNE ATTAQUE RANSOMWARE : L'EXEMPLE DE WANNACRY

QU'EST-CE QU'UN RANSOMWARE ?

Un ransomware (rançongiciel en français) est un malware qui chiffre (verrouille) les fichiers d'une victime pour les rendre inaccessibles, puis demande le paiement d'une rançon en bitcoins pour fournir la clé de déchiffrement. Ça constitue un crime d'extorsion numérique.

Le champ d'action croissant des ransomwares

Les cybercriminels s'attaquent aux données dont votre entreprise a besoin pour fonctionner. Leur capacité à vous extorquer une rançon dépendra des mesures que vous prenez aujourd'hui pour renforcer votre environnement et améliorer votre réponse en cas d'attaque.

Les menaces liées aux ransomwares ne cessent d'évoluer. Les cibles et les tactiques se développent. Vous devrez bientôt, si ce n'est déjà fait, expliquer comment vous luttez contre les différents moyens utilisés par les cybercriminels pour perturber vos opérations.

	Ransomware 1.0	Ransomware 2.0	Ransomware 3.0
Cible des logiciels malveillants	Données de production	• Données de sauvegarde • Systèmes de sauvegarde • Données de production	• Données de sauvegarde • Systèmes de sauvegarde • Données de production • Données à supprimer illégalement
Mode opératoire	Chiffrement	Chiffrement	Chiffrement et exfiltration
Comment les entreprises luttent contre les attaques	Système de sauvegarde et de récupération	Sauvegardes inaltérables et cyber coffre-fort	Détection précoce et surveillance continue

LES ÉTAPES D'UNE ATTAQUE RANSOMWARE

I. INFECTION INITIALE

L'attaquant doit d'abord accéder à l'ordinateur ou au réseau de la victime. Les méthodes incluent :

- Emails malveillants avec pièces jointes infectées
- Liens de phishing
- Exploiter des vulnérabilités de sécurité

Avec WannaCry : Au lieu des méthodes classiques, WannaCry exploitait directement la vulnérabilité Eternal Blue du protocole SMB de Windows. Aucune action de l'utilisateur n'était nécessaire - le malware se propageait automatiquement sur les réseaux d'entreprise.

II. INSTALLATION ET PROPAGATION

Une fois l'ordinateur initial infecté, le ransomware :

- S'installe sur le système
- Se propage aux autres ordinateurs du réseau
- Utilise les connexions réseau pour accéder à d'autres machines

Avec WannaCry : Le malware utilisait une porte dérobée appelée Double Pulsar pour installer WannaCry sur d'autres systèmes Windows du réseau. Il se propageait latéralement (de machine en machine) sans intervention utilisateur, ce qui était extraordinairement efficace en entreprise.

III. CHIFFREMENT DES DONNÉES

Le ransomware commence alors à :

- Identifier les fichiers importants (.doc, .xls, .pdf, .jpg, etc.)
- Les chiffrer avec un algorithme cryptographique fort
- Rendre ces fichiers complètement inaccessibles

Avec WannaCry : Le malware contenait le composant Wana Decrypt0r 2.0 qui chiffrait tous les fichiers accessibles sur les ordinateurs infectés. Les utilisateurs voyaient soudainement leurs données verrouillées.

IV. AFFICHAGE DE LA RANÇON

Un message s'affiche à l'écran de la victime :

- Une explication de la situation
- Le montant de la rançon demandée
- Les instructions pour payer en bitcoins
- Un délai limite (souvent 3 à 7 jours)
- Une menace d'augmentation du prix ou de suppression des données

Avec WannaCry : Le message de rançon demandait 300 USD (puis 600 USD après 3 jours). Les instructions étaient écrites en 28 langues différentes, indiquant que l'attaque visait une audience mondiale.

V. EXTORSION ET PAIEMENT

Les victimes se retrouvent face à un dilemme :

- Payer la rançon (sans garantie de récupérer les fichiers)
- Perdre définitivement leurs données
- Essayer de restaurer à partir de sauvegardes (si elles existent)

Avec WannaCry : La plupart des organisations infectées n'avaient pas le choix : soit payer, soit perdre leurs données critiques. Les hôpitaux du NHS britannique, par exemple, ne pouvaient pas se permettre de perdre les dossiers médicaux des patients.

POURQUOI WANNACRY A ÉTÉ SI DÉVASTATEUR

I. Propagation automatique

- Contrairement aux ransomwares classiques (par email), WannaCry ne nécessitait pas que l'utilisateur clique sur un lien
- Il exploitait une faille réseau pour se propager d'ordinateur en ordinateur

II. Absence de correctifs appliqués

- Microsoft avait publié un correctif en mars 2017 (2 mois avant)
- De nombreuses organisations n'l'avaient pas appliqué
- Les vieilles versions de Windows (XP) n'étaient pas mises à jour

III. Systèmes vulnérables

- Des millions d'ordinateurs encore sous Windows XP (support arrêté depuis 2014)
- Des systèmes non maintenus par manque de ressources IT

IV. Impact sur les services critiques

- Les hôpitaux britanniques n'avaient pas d'autre choix que d'arrêter les services
- Les chaînes de production automobile ont dû s'arrêter
- Les services gouvernementaux et bancaires ont été perturbés

COMMENT S'EN PROTÉGER

À partir de l'exemple WannaCry, les leçons de protection sont :

1. Appliquer les mises à jour immédiatement - Le correctif existait depuis 2 mois
2. Moderniser les systèmes - Arrêter d'utiliser Windows XP et des systèmes obsolètes
3. Sauvegarder régulièrement - Avoir des copies des données en cas de chiffrement
4. Segmenter le réseau - Isoler les systèmes critiques pour limiter la propagation
5. Former les utilisateurs - Ne pas cliquer sur des liens suspects (pour les ransomwares par email)
6. Surveiller le réseau - Détecter les activités anormales

CONCLUSION

WannaCry de mai 2017 a marqué l'histoire comme la plus grande cyberattaque par ransomware jamais enregistrée, infectant plus de 200 000 ordinateurs dans 150 pays en quelques jours. En exploitant une vulnérabilité divulguée publiquement, ce malware a paralysé des services critiques mondiaux, causant des milliards de dollars de dommages.

L'incident a révélé une vérité simple mais gênante : les organisations n'appliquaient pas les correctifs de sécurité disponibles. Grâce à la détection d'un chercheur en sécurité et aux efforts des autorités, l'attaque a été stoppée, mais les dégâts restaient considérables.

WannaCry a établi des leçons durables pour la cybersécurité : l'importance des mises à jour régulières, la nécessité de moderniser les systèmes obsolètes, la protection renforcée des infrastructures critiques et la valeur des sauvegardes. Sept ans plus tard, cet incident continue d'influencer les politiques de sécurité informatique mondialement et rappelle que la cybersécurité est une question de sécurité nationale.

SOURCE

- ✓ **Wikipédia - WannaCry** https://fr.wikipedia.org/wiki/WannaCry
- ✓ **Cloudflare - Qu'est-ce que l'attaque par rançongiciel WannaCry ?** https://www.cloudflare.com/fr-fr/learning/security/ransomware/wannacry-ransomware/
- ✓ **Kaspersky - Ransomware WannaCry : tout ce que vous devez savoir** https://www.kaspersky.fr/resource-center/threats/ransomware-wannacry
- ✓ **Cisco France Blog - 12 Mai 2017 : Cyberattaque mondiale par le ransomware Wannacry** https://gblogs.cisco.com/fr/securite/12-mai-2017-cyberattaque-mondiale-par-le-ransomware-wannacry/
- ✓ **France 24 - WannaCry : une cyberattaque mondiale qui n'aurait pas dû avoir lieu** https://www.france24.com/fr/20170515-wannacry-virus-informatique-rancongiciel-ransomware-internet-piratage
- ✓ **Arsen.co - WannaCry, le plus grand piratage a rançon de l'histoire** https://arsen.co/blog/wannacry
- ✓ **Proofpoint - Qu'est-ce que le ransomware Wannacry ?** https://www.proofpoint.com/fr/threat-reference/wannacry