le cnam

SEC 102 - TP08
Analyse de WannaCry

Date	Version	Description	Auteurs
04/05/2023	1	Première version	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire

A. Introduction **3**
B. Analyse de Wannacry **4**
C. Conclusion **6**

A. Introduction

WannaCry est un ransomware qui a causé d'importants dégâts à travers le monde en infectant des milliers de systèmes informatiques. Ce logiciel malveillant est conçu pour crypter les fichiers de l'utilisateur et exiger une rançon en Bitcoin pour les déchiffrer. Nous allons analyser les différentes techniques utilisées par WannaCry pour prospecter, pénétrer, pérenniser, propager et paralyser les systèmes ciblés.

B. Analyse de Wannacry

Prospecter :
T1018: WannaCry scanne son segment de réseau local à la recherche de systèmes distants à exploiter et infecter.

Pénétrer :
T1210: WannaCry utilise une faille dans SMBv1 pour se propager sur d'autres systèmes distants dans un réseau

Pérenniser :
T1543.003 : WannaCry crée le service ‘mssecsvc2.0’ avec le nom d'affichage ‘Microsoft Security Center (2.0)’ afin de rester incognito.

T1222.001 : WannaCry modifie les permissions d’accès et de visibilités des dossiers et fichiers pour les rendres inutilisables par les autres utilisateurs

T1564.001 : Hidden Files and Directories: WannaCry utilise attrib +h pour rendre certains de ses fichiers cachés.

Propager :
T1570 : WannaCry a initialement infecté les réseaux informatiques, mais s'est propagé aux réseaux industriels grâce à une exploitation (en particulier la vulnérabilité MS17-010 ciblant SMBv1).

Paralyser :

T1486 : WannaCry chiffre les fichiers des utilisateurs et exige qu'une rançon soit payée en Bitcoin pour déchiffrer ces fichiers

T1490 : WannaCry inhibe la récupération du système en supprimant et désactivant les fonctionnalités de récupération du système d'exploitation avec des outils tels que vssadmin, wbadmin, bcdedit et wmic.

T1489 : WannaCry tente d'arrêter les processus associés à Exchange, Microsoft SQL Server et MySQL pour permettre le chiffrement de leurs bases de données

C. Conclusion

WannaCry est un ransomware sophistiqué qui a causé d'énormes perturbations dans de nombreux secteurs à travers le monde. Il utilise une série de techniques pour prospecter, pénétrer, pérenniser, propager et paralyser les systèmes informatiques ciblés. La compréhension de ces techniques est essentielle pour les entreprises et les organisations afin de renforcer leurs défenses et de mieux se protéger contre de telles menaces à l'avenir.