Cyber

Site utile :

- Programe BTS
- Hack Academy

Voici une comparaison détaillée entre les malwares **WannaCry** et **Stuxnet**, en tenant compte de plusieurs aspects :

1. Origine et Contexte

- **WannaCry** :
  - **Origine** : WannaCry est un ransomware qui a émergé en mai 2017. Son origine est liée à une vulnérabilité dans les systèmes Microsoft Windows exploitée par le groupe de hackers "Shadow Brokers", qui a volé et divulgué des outils de piratage de la NSA.
  - **Contexte** : WannaCry a exploité la vulnérabilité **EternalBlue**, une faille dans le protocole SMB (Server Message Block). Cette attaque a principalement touché des entreprises, des hôpitaux, des gouvernements, et des particuliers dans le monde entier, affectant des centaines de milliers de machines.
- **Stuxnet** :
  - **Origine** : Stuxnet a été découvert en 2010, mais il a probablement été développé quelques années plus tôt, autour de 2007-2008. Il est largement attribué aux États-Unis et à Israël, dans le cadre d'une opération conjointe visant à saboter le programme nucléaire iranien.
  - **Contexte** : Stuxnet visait spécifiquement des installations industrielles, en particulier les centrifugeuses utilisées par l'Iran pour enrichir de l'uranium. Il est considéré comme un cyberarme, car son objectif n'était pas de voler des données mais de détruire des équipements physiques.

2. Mécanisme de Propagation

- **WannaCry** :
  - **Propagation** : WannaCry se propage principalement via le protocole SMB, exploitant la vulnérabilité **EternalBlue** pour infecter les ordinateurs qui n'avaient pas mis à jour leurs systèmes avec les derniers patchs de sécurité. Une fois dans un réseau, le malware se propage automatiquement à d'autres ordinateurs vulnérables.
  - **Vitesse** : Il s'est propagé rapidement, infectant des centaines de milliers d'ordinateurs dans le monde entier en quelques heures.
- **Stuxnet** :
  - **Propagation** : Stuxnet utilisait plusieurs vecteurs pour se propager, y compris des clés USB infectées, des réseaux locaux (LAN) et des connexions à distance. Cependant, contrairement à WannaCry, Stuxnet n’a pas été conçu pour se propager rapidement à l’échelle mondiale. Il ciblait spécifiquement les systèmes industriels SCADA (Supervisory Control and Data Acquisition).
  - **Vitesse** : Sa propagation était plus ciblée et plus lente, car il avait un objectif très spécifique : détruire des équipements industriels et non causer des dommages à grande échelle.

3. Cible et Impacts

- **WannaCry** :
  - **Cible** : WannaCry a affecté un large éventail d'organisations à l'échelle mondiale, y compris des hôpitaux (comme le NHS au Royaume-Uni), des entreprises, des institutions gouvernementales, etc.
  - **Impacts** : L'attaque a causé des pertes financières massives, perturbé des services essentiels (comme les soins de santé), et laissé de nombreuses organisations incapables d'accéder à leurs fichiers. Le ransom demandé pour déchiffrer les données était payé par certaines victimes, mais il a été en grande partie inefficace car des mesures de désactivation ont été mises en place par des chercheurs en cybersécurité.
- **Stuxnet** :
  - **Cible** : Stuxnet visait spécifiquement les installations industrielles iraniennes, en particulier les centrifugeuses utilisées dans les usines d'enrichissement de l'uranium.
  - **Impacts** : Stuxnet a causé des dommages physiques aux équipements industriels (des centrifugeuses ont été physiquement détruites) et a retardé de manière significative le programme nucléaire de l'Iran. L'attaque a été un sabotage ciblé plutôt qu'un vol de données ou une demande de rançon.

4. Caractéristiques Techniques

- **WannaCry** :
  - **Type** : Ransomware (rançon).
  - **Exploitation de vulnérabilité** : EternalBlue dans SMBv1.
  - **Mécanisme de chiffrement** : Une fois l'ordinateur infecté, il chiffre les fichiers de l'utilisateur et demande une rançon en Bitcoin pour déchiffrer les fichiers.
  - **Propagation** : Utilisation du SMB pour se propager à d'autres machines vulnérables, ainsi qu'un mécanisme de "kill-switch" (un domaine web spécifique qui, une fois enregistré, a stoppé la propagation).
- **Stuxnet** :
  - **Type** : Malware espion et saboteur (cyberarme).
  - **Exploitation de vulnérabilités** : Utilisation de plusieurs vulnérabilités 0-day dans Windows et des failles spécifiques dans les contrôleurs industriels Siemens PLC (Programmable Logic Controllers).
  - **Mécanisme de sabotage** : Modifie les commandes envoyées aux centrifugeuses, les faisant tourner à des vitesses dangereuses, tout en masquant les effets du sabotage pour que les opérateurs ne puissent pas détecter immédiatement les dommages.

5. Réponses et Contre-Mesures

- **WannaCry** :
  - **Réponse** : Après l'attaque, un patch de sécurité a été diffusé par Microsoft pour corriger la vulnérabilité SMB. Des chercheurs en cybersécurité ont rapidement découvert le "kill-switch" qui a permis de stopper la propagation. Les gouvernements et les entreprises ont également renforcé leurs systèmes de sécurité en mettant à jour leurs logiciels et en prenant des mesures contre les ransomwares.
  - **Contre-mesures** : Mise à jour des systèmes, activation des pare-feu, et installation de solutions antivirus. L'éducation des utilisateurs pour éviter le clic sur des liens

malveillants a également joué un rôle crucial.

- **Stuxnet** :
  - **Réponse** : Stuxnet a été une attaque très ciblée et sophistiquée, ce qui a rendu sa détection initiale difficile. Une fois découvert, les autorités et les experts en cybersécurité ont analysé son code et mis en place des mesures pour se protéger contre les exploits utilisés par Stuxnet. Cependant, il n'existait pas de contre-mesures immédiates pour neutraliser son effet spécifique.
  - **Contre-mesures** : Les entreprises ont renforcé la sécurité de leurs systèmes SCADA et ont mis en œuvre des contrôles plus stricts pour les systèmes industriels. L'attaque a également sensibilisé les gouvernements et les entreprises à la sécurité des infrastructures critiques.

Conclusion

- **WannaCry** : Un ransomware à propagation rapide, qui a affecté un large éventail de cibles en exploitant une vulnérabilité connue dans les systèmes Windows. Il a eu un impact financier majeur mais a été relativement simple à stopper une fois le kill-switch découvert.
- **Stuxnet** : Une cyberarme extrêmement sophistiquée et ciblée, utilisée pour des fins géopolitiques spécifiques, visant des installations industrielles critiques. Son objectif était la destruction physique des équipements plutôt que le vol de données ou l'extorsion de fonds.

Ces deux malwares illustrent des approches très différentes du cybercrime et du cyberterrorisme, de l'attaque globale et indiscriminée de WannaCry à la stratégie de sabotage précis et géopolitique de Stuxnet.