Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question : Comment des objets connectés non sécurisés peuvent-ils être une menace pour d'autres personnes, sans que les propriétaires de l'objet n'en soient conscients ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Expliquer ce qu'est une attaque par déni de service.
2. Pourquoi ce genre d'attaque ne peut pas être effectué depuis un seul ordinateur ?
3. Expliquer comment les hackers ont réussi à prendre le contrôle de tous ces objets connectés sans que les utilisateurs ne s'en rendent compte ?
4. Donner les avantages et inconvénients (pour le constructeur et pour les utilisateurs et utilisatrices) de laisser des mots de passe simple pour les objets connectés.

Barème

⚠️ **Avertissements** ⚠️ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation	**(... / 4)**
Titre Vous avez proposé un titre, court, clair, et percutant.	
Forme Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe.	
Fond Elle présente correctement le podcast, pour donner envie de l'écouter.	
Bibliographie Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	

Prestation	**(... / 6)**
Pertinence Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse.	
Vulgarisation Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne.	
Plan Le contenu est structuré.	
Bibliographie Vous citez le ou les documents présentés.	
Crédits Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.	

SNT > INFORMATIQUE EMBARQUÉE > ENJEUX VIRUS

Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question : Comment des objets connectés non sécurisés peuvent-ils être une menace pour d'autres personnes, sans que les propriétaires de l'objet n'en soient conscients ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Expliquer ce qu'est une attaque par déni de service.
2. Pourquoi ce genre d'attaque ne peut pas être effectué depuis un seul ordinateur ?
3. Expliquer comment les hackers ont réussi à prendre le contrôle de tous ces objets connectés sans que les utilisateurs ne s'en rendent compte ?
4. Donner les avantages et inconvénients (pour le constructeur et pour les utilisateurs et utilisatrices) de laisser des mots de passe simple pour les objets connectés.

Barème

⚠️ **Avertissements** ⚠️ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation	**(... / 4)**
Titre Vous avez proposé un titre, court, clair, et percutant.	
Forme Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe.	
Fond Elle présente correctement le podcast, pour donner envie de l'écouter.	
Bibliographie Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	

Prestation	**(... / 6)**
Pertinence Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse.	
Vulgarisation Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne.	
Plan Le contenu est structuré.	
Bibliographie Vous citez le ou les documents présentés.	
Crédits Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.	

Douglas Bonderud, SecurityIntelligence.com, *Leaked Mirai Malware Boosts IoT Insecurity Threat Level* (traduit par Louis Paternault), 4 octobre 2016.

https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level

Les mots marqués d'une astérisque sont définis dans le second document.*

Comme expliqué par le magazine Infosecurity, Mirai* est conçu pour tirer profit de l'IoT* en parcourant le web à la recherche d'appareils protégés par des mots de passe par défaut, ou par des identifiants codés en dur, les rendant facile à compromettre et à infecter. Une fois sous le contrôle de personnes mal intentionnées, ces appareils sont transformés en une sorte d'immense botnet* qui peut lancer des attaques par déni de service* sur des sites web, et les faire tomber rapidement. Le site Krebs on Security, par exemple, a été récemment la cible d'une attaque par déni de service à 620 Gbps utilisant le logiciel malveillant Mirai. Ars Technica a aussi fait état d'une attaque à 1 Tbps visant l'hébergeur français OVH. […] Cela a été rendu possible par la combinaison du simple nombre d'appareils connectés à internet, et de la médiocre sécurité associée à la plupart de ces produits.

[…]

Selon Ars Technica, les caméras IP et les magnétoscopes numériques sont parmi les appareils connectés les plus souvent compromis. Cela se tient, car des millions de ces appareils sont en ligne, et la plupart sont livrées avec des identifiants de connexion qui ne sont jamais changés par la suite. Le problème est que les caméras, les caméscopes, les imprimantes et les capteurs sans fil ne semblent pas dangereux parce qu'ils sont en périphérie des réseaux professionnels.

[…]

Comment donc les fabricants et les vendeurs d'objets connectés peuvent-ils inverser la tendance et stopper Mirai* dans sa course ? La première solution est les mots de passe. Les vendeurs d'appareils doivent s'assurer que chaque appareil connecté possède un mot de passe unique, ou forcer les utilisateurs à changer le mot de passe dés que l'appareil est installé.

Extraits d'articles du Wikipédia francophone, par les contributeurs et contributrices de Wikipedia.

https://fr.wikipedia.org/

Mirai : Mirai est un logiciel malveillant qui transforme des ordinateurs utilisant le système d'exploitation Linux en bots contrôlés à distance, formant alors un botnet utilisé notamment pour réaliser des attaques à grande échelle sur les réseaux.

Attaque par dénie de service : Une attaque par déni de service […] est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

IoT : L'Internet des objets, ou IdO (en anglais Internet of Things, ou IoT) est l'interconnexion entre Internet et des objets, des lieux et des environnements physiques.

Botnet : Un botnet […] est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. […] Le sens de botnet s'est étendu aux réseaux de machines zombies, utilisés notamment pour le minage de cryptomonnaies mais aussi des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).

Snt > Informatique embarquée > Enjeux Virus

Douglas Bonderud, SecurityIntelligence.com, *Leaked Mirai Malware Boosts IoT Insecurity Threat Level* (traduit par Louis Paternault), 4 octobre 2016.

https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level

Les mots marqués d'une astérisque sont définis dans le second document.*

Comme expliqué par le magazine Infosecurity, Mirai* est conçu pour tirer profit de l'IoT* en parcourant le web à la recherche d'appareils protégés par des mots de passe par défaut, ou par des identifiants codés en dur, les rendant facile à compromettre et à infecter. Une fois sous le contrôle de personnes mal intentionnées, ces appareils sont transformés en une sorte d'immense botnet* qui peut lancer des attaques par déni de service* sur des sites web, et les faire tomber rapidement. Le site Krebs on Security, par exemple, a été récemment la cible d'une attaque par déni de service à 620 Gbps utilisant le logiciel malveillant Mirai. Ars Technica a aussi fait état d'une attaque à 1 Tbps visant l'hébergeur français OVH. […] Cela a été rendu possible par la combinaison du simple nombre d'appareils connectés à internet, et de la médiocre sécurité associée à la plupart de ces produits.

[…]

Selon Ars Technica, les caméras IP et les magnétoscopes numériques sont parmi les appareils connectés les plus souvent compromis. Cela se tient, car des millions de ces appareils sont en ligne, et la plupart sont livrées avec des identifiants de connexion qui ne sont jamais changés par la suite. Le problème est que les caméras, les caméscopes, les imprimantes et les capteurs sans fil ne semblent pas dangereux parce qu'ils sont en périphérie des réseaux professionnels.

[…]

Comment donc les fabricants et les vendeurs d'objets connectés peuvent-ils inverser la tendance et stopper Mirai* dans sa course ? La première solution est les mots de passe. Les vendeurs d'appareils doivent s'assurer que chaque appareil connecté possède un mot de passe unique, ou forcer les utilisateurs à changer le mot de passe dés que l'appareil est installé.

Extraits d'articles du Wikipédia francophone, par les contributeurs et contributrices de Wikipedia.

https://fr.wikipedia.org/

Mirai : Mirai est un logiciel malveillant qui transforme des ordinateurs utilisant le système d'exploitation Linux en bots contrôlés à distance, formant alors un botnet utilisé notamment pour réaliser des attaques à grande échelle sur les réseaux.

Attaque par dénie de service : Une attaque par déni de service […] est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

IoT : L'Internet des objets, ou IdO (en anglais Internet of Things, ou IoT) est l'interconnexion entre Internet et des objets, des lieux et des environnements physiques.

Botnet : Un botnet […] est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. […] Le sens de botnet s'est étendu aux réseaux de machines zombies, utilisés notamment pour le minage de cryptomonnaies mais aussi des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).