Cinalia
Sécurisons votre digitalisation

Fraude Spotlight

La capture et le craquage de mot de passe WiFi

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

La capture et le craquage de mot de passe WiFi

Objectif du hacker

S'introduire dans le réseau de l'entreprise ou du particulier pour le pirater.

Comment ?

En capturant le trafic par air pour découvrir le mot de passe du réseau WiFi.

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

Méthodologie de l'attaque

1. À PROPOS DES ATTAQUES DE RÉSEAUX WIFI
2. UTILISATION DE MATÉRIEL DE SCAN POUR CAPTURER LES PAQUETS DE TRANSMISSION
3. CRAQUAGE DU MOT DE PASSE

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

1 / À propos des attaques de réseaux WiFi

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ À propos des attaques de réseaux WiFi

Ces risques d'attaques sont liés à la propre technologie WiFi qui permet la capture de paquets de transmission par l'air, ainsi qu'aux protocoles d'encryptage.

- Le bande des 2.4G regroupe les principaux réseaux WiFi et les techniques d'attaque sur cette bande sont maintenant bien éprouvées.
- Faiblesse du protocole WPA*2 qui présente des failles de sécurité permettant des attaques KRACK**, une menace sérieuse qui cible le WPA2.
- Contrairement aux attaques spécifiques de type Rogue, Evil-Twin, le craquage de mot de passe est l'option la plus simple : il n'y a rien à mettre en place et cela fonctionne immédiatement car la méthode est inhérente à la technologie (air).

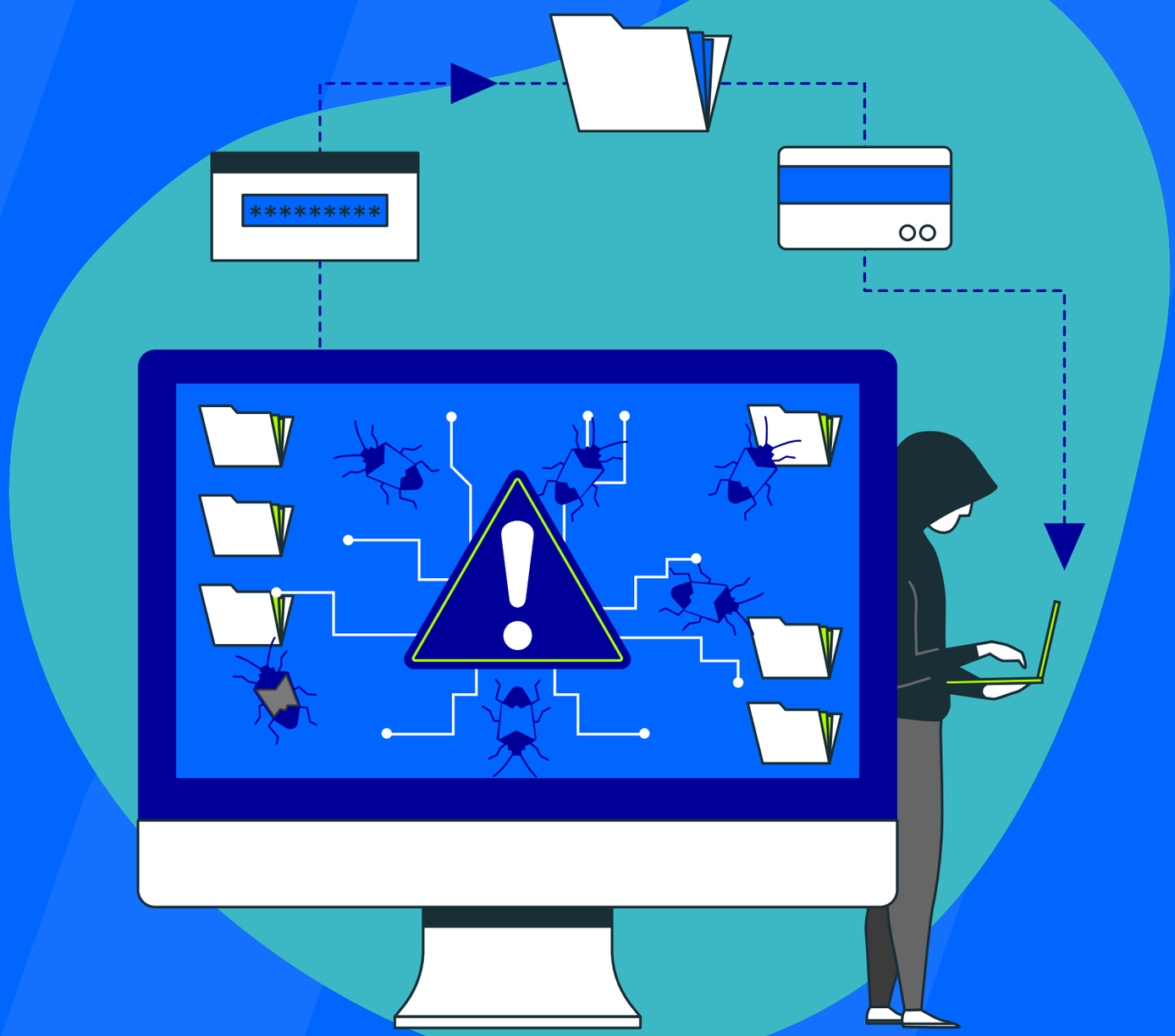
*WiFi Protected Access = Accès WiFi Protégé
** Key Réinstallation Attack = Attaque de Réinstallation de Clé

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

2 / **Utilisation** de matériel de scan pour capturer les paquets de transmission



www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ Utilisation de matériel de scan pour capturer les paquets de transmission

Le matériel de scan fonctionne sur tous les systèmes (Windows, Linux, Android, etc.) et ont une capacité incroyable à capturer des réseaux WiFi et obtenir l'échange de clés.

- Les dispositifs les plus simples et anciens sont les plus efficaces.
- Ils peuvent capturer des réseaux à 500m.
- Ils sont limités à la bande de 2.4G, là où se trouvent la plupart des réseaux.
- Il existe la possibilité de combiner plusieurs dispositifs pour produire différents types d'attaque à la fois.

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

3 / **Craquage** du mot de passe

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ Craquage du mot de passe

L’attaquant exploite les paquets capturés pour trouver des indices sur le mot de passe et le découvrir. Il utilise diverses méthodes et des outils de craquage spécialisés tel que Hashcat ou John The Ripper.

- Ces outils fonctionnent avec des dictionnaires de mots de passe disponibles en ligne ou que l'on peut créer soi-même si on "devine" le format du mot de passe.
- Le craquage nécessite des ordinateurs et des processeurs très puissants que l'on peut réserver sur le cloud.
- Le temps de craquage peut être plus ou moins long selon le format du mot de passe. Par exemple, de moins d'une heure pour un mot de passe de 10 chiffres à 25 jours pour 11 caractères alphanumériques, minuscules, majuscules et symboles.

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

Comment se protéger de la capture et du craquage de mot de passe ?

1. ADOPTER LE PROTOCOLE WPA3
2. UTILISER DU MATÉRIEL DE DERNIÈRE GÉNÉRATION
3. ET SURTOUT UTILISER UN MOT DE PASSE SOPHISTIQUÉ

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ Adopter le protocole WPA3

Adopter le protocole WPA3 et si possible le WPA-E (Entreprise) et lier l'entrée sur le réseau d'entreprise à une connexion à l'AD.

- Il n'existe pour l'instant pas d'outil offensif capable de gérer le WPA3.
- Le WPA-E, connu également sous le nom de mode WPA-802.1X ou WPA-EAP, est conçu pour les réseaux d'entreprise et demande que l'on installe un serveur d'authentification RADIUS. Plus compliqué à mettre en place, il offre plus de sécurité.
- Le protocole EAP* est utilisé pour l'authentification et existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.

*Extensible Authentication Protocol = protocole d'authentification extensible

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ Utiliser du matériel de dernière génération

Le WPA3 date de 2018, et seul le matériel de dernière génération (routeurs, switchs et AP) peut bénéficier de ce protocole.

Cinalia
Sécurisons votre digitalisation

/ Fraude Spotlight

La capture et le craquage de mot de passe WiFi

→ Et surtout utiliser un mot de passe sophistiqué

Le mot de passe doit être choisi au hasard avec au moins 12 caractères alphanumériques combinant majuscules, minuscules et symboles.

Cinalia

Sécurisons votre digitalisation

Vous accompagner dans la maîtrise de vos enjeux de cybersécurité.

Un projet?
Des questions ?
N’hésitez pas à nous contacter.

www.cinalia.com

Synelience GROUP

Smart Connection for Smart Solutions