ZIMPERIUM®
ADVANCED MOBILE SECURITY

L'anatomie des attaques mobiles

Les endpoints mobiles des entreprises, qu'ils soient détenus ou exploités dans le cadre de politiques de type BYOD (bring-your-own-device), sont des cibles de grande valeur pour les groupes cybercriminels. Les appareils mobiles peuvent accéder aux mêmes données d'entreprise qu'un ordinateur portable d'entreprise, mais ils sont généralement beaucoup moins sécurisés et présentent davantage de vecteurs d'attaque.

La plupart des attaques mobiles réussies utilisent des versions actualisées d'outils malveillants existants qui ont été développés dans le passé, adaptés à des objectifs d'attaque spécifiques et regroupés pour une complexité supplémentaire afin de créer une menace persistante avancée. Cette approche permet aux attaquants de soustraire très tôt l'attaque aux outils de détection des menaces existants, ce qui leur donne l'avantage du temps pour parvenir à leurs fins.

Pour faire face à ces outils mobiles avancés et à ces acteurs malveillants qualifiés, les entreprises doivent réduire leur dépendance à l'égard des défenses statiques existantes et de la formation des utilisateurs finaux pour sécuriser leurs endpoints mobiles. Non seulement ces anciens systèmes sont incapables de prévenir les attaques avancées, mais leurs capacités limitées et leur dépendance à l'égard des signatures les rendent pratiquement inutiles contre les menaces zero-day. Pour sécuriser les endpoints existants contre les attaques modernes, les organisations doivent adopter une solution complète capable de détecter les menaces connues et inconnues tout au long de la Cyber Kill Chain et de s'intégrer de manière transparente dans l'architecture de sécurité globale de l'organisation.

ANATOMIE DES MODÈLES DE CYBERATTAQUES

La Cyber Kill Chain (CKC) et le MITRE ATT&CK pour les matrices mobiles sont des modèles de cas étroitement liés qui fournissent un contexte à la fois sur la stratégie et les aspects tactiques des attaques réalisées. Ces modèles de cas fournissent les capacités nécessaires pour détecter et se défendre contre les attaques qui se produisent à chaque étape de ces modèles, indépendamment du moment où ils sont lancés ou arrêtés.

Que représente le modèle Cyber Kill Chain (CKC) ?

Étape 1 : Découverte et reconnaissance
Les attaquants commencent par faire de la reconnaissance sur la victime et ses appareils pour découvrir des détails concernant l'utilisateur et son identité, l'appareil et/ou le réseau associé. En fin de compte, les attaquants cherchent à comprendre ce qu'ils peuvent exploiter pour atteindre leurs objectifs.

Étape 2 : Armement
À cette étape, les attaquants utilisent les informations de l'étape 1 pour construire un programme malveillant bien adapté.

Étape 3 : Distribution
Au cours de la phase de distribution, les attaquants transmettent le programme malveillant. La distribution peut être réalisée de plusieurs façons, par exemple :

- Réseau Wi-Fi
- Réseau GSM
- USB
- NFC
- Bluetooth
- Message (ex. SMS/MMS/E-Mail)
- Redirection vers un site contenant une charge utile malveillante ou un exploit (ex.
- Stagefright ou Pegasus)
- Image malveillante (ex. iMessage)

Une fois que les attaquants ont délivré leur charge utile et/ou établi leur présence sur le dispositif, ils peuvent passer à l'étape suivante/aux autres étapes comme ils le souhaitent.

Étape 4 : Exploitation et Étape 5 : Installation
Au cours des étapes d'exploitation et d'installation, les attaquants exécutent et installent le programme malveillant pour établir leur présence. Après l'étape 5, l'appareil est entièrement compromis.

Étape 6 : Commande et contrôle
En principe, à cette étape, l'attaquant envoie une commande à l'appareil qui lui permet de contrôler le comportement de l'appareil et d'être en mesure d'exécuter l'objectif visé.

Étape 7 : Actions
Une fois qu'un appareil a été compromis, l'attaquant pourra atteindre l'objectif ultime de a) créer une persistance sur l'appareil dont l'utilisateur ne peut pas se débarrasser facilement ou qu'il ne peut pas détecter et b) extraire les données qui intéressent l'attaquant, comme les fichiers sensibles et les jetons d'identité de l'utilisateur (par exemple, les certifications, les noms d'utilisateur, les mots de passe, etc.).

Quelles sont les tactiques MITRE ATT&CK pour les matrices mobiles ?

- Évasion de défense (19 techniques)
- Accès aux données d'identification (1
- Découverte (9 techniques)
- Mouvement latéral (2 techniques)
- Collecte (17 techniques)
- Commande et contrôle (8 techniques
- Extraction (4 techniques)
- Impact (10 techniques)

- Effets de réseau (9 techniques)
- Effets de service à distance (3 techniques)

DÉCOMPOSER L'ANATOMIE DES ATTAQUES MOBILES

Chaque cas de test ci-dessous couvre les sept différentes étapes du CKC et l'utilisation de 13 différentes catégories de techniques MITRE ATT&CK pour mobile, pour des attaques réelles contre des endpoints mobiles. Bien que certaines ne couvrent que des étapes individuelles, d'autres montrent comment une attaque peut être enchaînée pour couvrir l'ensemble du groupe de modèles, et certaines montrent comment les attaques peuvent commencer plus tard dans le CKC, sans être enchaînées avec des attaques antérieures.

Cas de test 1	
Nom	**Analyses du réseau**
Plate-forme(s)	Android (toutes les versions), iOS 9.x et inférieur
Description	L'analyse du réseau permet aux attaquants de découvrir des cibles potentielles et est généralement un précurseur d'une attaque réelle. Ces cas de test viseront à découvrir les appareils Android sur le réseau en utilisant diverses techniques d'analyse.
Événements menaçants Attendus	• Analyse TCP • Analyse IP • Analyse ARP • Analyse UDP
Étapes du CKC	Étapes = 1
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, découverte
Préconditions	• Le réseau Wi-Fi est connecté à l'Internet • Aucune isolation de l'hôte n'est présente sur le réseau Wi-Fi • Aucun VPN n'a été établi par l'appareil • L'attaquant est connecté au réseau Wi-Fi
Postconditions	L'attaquant a identifié la victime dans le réseau
Étapes d'exécution	• La victime se connecte au Wi-Fi • L'attaquant lance une analyse de reconnaissance du réseau • L'attaquant obtient des informations à la suite de l'analyse

Cas de test 2	
Nom	**Attaques réseau**
Plate-forme(s)	iOS, Android
Description	Les attaquants peuvent prendre le contrôle du trafic réseau produit par un dispositif exécutant un ARP MitM (Man in the Middle) et modifier ensuite le contenu du trafic. Pendant l'attaque, les images affichées sur les pages web seront remplacées pour démontrer le contrôle du trafic.
Événements menaçants Attendus	• ARP MitM • SSL Strip • SSL MitM
Étapes du CKC	Étapes = 2, 3
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, accès initial
Préconditions	• Le réseau Wi-Fi est connecté à l'Internet • Aucune isolation de l'hôte n'est présente sur le réseau Wi-Fi • Aucun VPN n'a été établi par l'appareil • L'attaquant est connecté au réseau Wi-Fi
Postconditions	La victime est connectée à l'attaquant au lieu de la passerelle réseau. L'attaquant a un contrôle total sur le flux de trafic entre la victime et la passerelle réseau, ce qui est démontré par : • Manipulation du trafic http (injection de contenu) • Inspection du trafic http et https (trafic en clair) • Navigation sur diverses pages qui sont clairement manipulées par l'attaquant (par exemple, les images sont remplacées)

Étapes d'exécution	• La victime se connecte au Wi-Fi
	• L'attaquant commence l'attaque du réseau
	  ◦ ARP MitM
	  ◦ SSL MitM
	  ◦ SSL Strip
	• La victime consulte une page sur l'appareil

Cas de test 3	
Nom	**Malware Sideloaded (iOS)**
Plate-forme(s)	iOS (inscrit à MDM)
Description	Téléchargement et installation d'un programme malveillant à partir d'une page personnalisée
Événements menaçants Attendus	• Application douteuse • Application Sideloaded
Étapes du CKC	Étapes = 3, 4
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, accès initial, exécution
Préconditions	• L'attaquant est connecté au réseau Wi-Fi • L'attaquant achemine activement le trafic vers son propre hôte via un AP pirate ou un ARP MitM • Aucune isolation de l'hôte n'est présente sur le réseau Wi-Fi • Aucun VPN n'a été établi par l'appareil • Le réseau Wi-Fi est connecté à l'Internet • Un certificat approuvé par l'appareil est installé sur le serveur Web
Postconditions	• Une application malveillante est installée sur l'appareil • Application Sideloaded détectée sur l'appareil
Étapes d'exécution	• L'attaquant commence l'empoisonnement du cache DNS et lance un serveur web hébergeant une charge utile malveillante • La victime se connecte au Wi-Fi • La victime navigue sur une page qui permet l'installation de diverses applications • La victime clique sur un lien et lance l'installation de l'application

Cas de test 4	
Nom	**Point d'accès non autorisé**
Plate-forme(s)	iOS, Android
Description	Les attaquants peuvent manipuler et contrôler le trafic produit par un appareil une fois que celui-ci a été piégé pour se connecter à un Wi-Fi malveillant avec un SSID préalablement connu par l'appareil. Une fois la connexion établie, le trafic peut être acheminé vers un portail captif malveillant.
Événements menaçants Attendus	Application douteuse
Étapes du CKC	Étapes = 3, 4
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, accès initial
Préconditions	• L'appareil de la victime s'est connecté auparavant à un réseau Wi-Fi ouvert • Le Wi-Fi de l'appareil de la victime est désactivé • L'attaquant a mis en place un point d'accès non autorisé, également appelé « ananas », qui répond activement aux sondes Wi-Fi
Postconditions	• L'appareil de la victime est connecté au point d'accès non autorisé • L'attaquant a le contrôle total du flux de trafic • Le contrôle peut être démontré en acheminant le trafic de sites web spécifiques vers l'hôte de l'attaquant où est hébergée une page de notification

Étapes d'exécution	• L'Attaquant
	  ○ Démarre un serveur web sur son hôte pour servir une page de notification
	  ○ Configure le routage DNS d'une URL particulière vers l'hôte de l'attaquant dans le point d'accès ananas
	  ○ Active un portail captif qui notifie toute personne se connectant au point d'accès non autorisé
	  ○ Commence à répondre activement aux sondes Wi-Fi
	  ○ Commence à capturer activement les SSID qui sont demandés
	• La victime active le Wi-Fi sur l'appareil
	• L'appareil se connecte au point d'accès non autorisé
	• La victime reçoit la notification du portail captif et l'accepte
	• La victime navigue sur une URL particulière et voit apparaître la page de notification

Cas de test 5	
Nom	**Profil malveillant**
Plate-forme(s)	iOS
Description	Lorsque l'utilisateur est connecté au Wi-Fi et navigue sur une page, il est redirigé vers une page qui l'incite à installer un profil malveillant qui connectera l'appareil à un service VPN. Au sein du service, le trafic sera décrypté afin d'obtenir des informations sensibles.
Événements menaçants Attendus	• Point d'accès non autorisé • SSL MitM • Profil suspect (MDM uniquement)
Étapes du CKC	Étapes = 3, 4
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, accès initial, exécution
Préconditions	• L'attaquant achemine activement le trafic vers son propre hôte en utilisant un point d'accès non autorisé ou un ARP MitM • Aucune isolation de l'hôte n'est présente sur le réseau Wi-Fi • Aucun VPN n'a été établi par l'appareil • L'attaquant est connecté au réseau Wi-Fi • Le réseau Wi-Fi est connecté à l'Internet • Un certificat approuvé par l'appareil est installé sur le serveur Web
Postconditions	• Un profil malveillant est installé sur l'appareil • Un VPN est établi depuis l'appareil vers la passerelle VPN d'un attaquant • Le trafic est entièrement compromis et l'attaquant a le contrôle total
Étapes d'exécution	• L'attaquant commence l'empoisonnement du cache DNS et lance un serveur web hébergeant une charge utile malveillante • La victime se connecte au Wi-Fi • La victime navigue sur une page et un avertissement demandant l'installation d'un profil • La victime confirme les étapes de l'installation afin de poursuivre • L'attaquant intercepte le trafic pour extraire des données et/ou injecter du contenu

Cas de test 6	
Nom	**Exploit à distance**
Plate-forme(s)	iOS
Description	Un utilisateur se connecte à un Wi-Fi hébergé par un point d'accès Wi-Fi malveillant. Lorsque l'utilisateur navigue sur une page, il est redirigé vers une page qui l'incite à installer une application malveillante indétectable. Une fois l'application exécutée, elle exploitera l'appareil et fournira un accès élevé à l'attaquant qui l'utilisera pour extraire des données.
Événements menaçants Attendus	• Point d'accès non autorisé • Altération du système / jailbreak
Étapes du CKC	Étapes = 2, 3, 4, 5, 6
Tactiques MITRE ATT&CK pour mobiles	Effets de réseau, accès initial, persistance, escalade de privilèges
Préconditions	• L'attaquant achemine activement le trafic vers son propre hôte en utilisant un point d'accès non autorisé ou un ARP MitM • Aucune isolation de l'hôte n'est présente sur le réseau Wi-Fi • Aucun VPN n'a été établi par l'appareil • L'attaquant est connecté au réseau Wi-Fi • Le réseau Wi-Fi est connecté à l'Internet • Un certificat approuvé par l'appareil est installé sur le serveur Apache
Postconditions	• Une application malveillante est installée sur l'appareil • Un exploit est exécuté sur l'appareil • L'appareil est entièrement compromis et l'attaquant a le contrôle total
Étapes d'exécution	• L'attaquant commence l'empoisonnement du cache DNS et lance un serveur web hébergeant une charge utile malveillante • La victime se connecte au Wi-Fi • La victime navigue sur une page et un avertissement demandant l'installation d'une application s'affiche • La victime clique sur le lien et lance l'application une fois l'installation terminée • L'attaquant se connecte à l'appareil pour extraire des données.

Cas de test 7	
Nom	**Chargeur malveillant**
Plate-forme(s)	Android et iOS
Description	Les chargeurs malveillants constituent un puissant moyen potentiel d'exploiter les appareils qui y sont connectés, notamment les appareils à puce A12 basés sur iOS et sensibles à Checkm8. Les utilisateurs d'appareils mobiles peuvent y être exposés dans les aéroports, les cafés, en voyage, lorsqu'ils utilisent des chargeurs bon¬ marché fabriqués dans des lieux géographiques spécifiques, etc. Les attaquants visent généralement à obtenir des informations et à accéder aux appareils connectés. Après s'être connecté au chargeur malveillant, les utilisateurs ne remarquent rien, mais un exploit est placé sur l'appareil et est exécuté. Ensuite, l'attaquant peut extraire des données et créer une persistance dans le microprogramme.
Événements menaçants Attendus	• Anomalie de processus • Altération du système • EOP • Modification persistante du système d'exploitation
Étapes du CKC	Étapes = 2, 3, 4
Tactiques MITRE ATT&CK pour mobiles	Accès initial, persistance, escalade de privilèges
Préconditions	• La victime a accepté le message demandant de faire confiance à l'empreinte digitale de la station/du périphérique USB connecté(e) • Options du développeur et débogage USB activés • Les magasins d'applications tiers sont activés • L'appareil est en mode avion et le Wi-Fi est désactivé
Postconditions	L'appareil est entièrement compromis et l'attaquant a le contrôle total
Étapes d'exécution	• La victime connecte son appareil à l'USB • L'attaquant envoie un programme d'exploitation à l'appareil • L'attaquant exécute le ou les programmes d'exploitation et obtient des privilèges élevés

ANATOMIE D'UNE SÉCURITÉ MOBILE COMPLÈTE

Bien que les appareils mobiles d'entreprise sont souvent protégés par un ensemble de solutions de base, comme la gestion des appareils mobiles (MDM) et la gestion des accès mobiles (MAM), ces outils ne sont pas axés sur la sécurité. Les applications de gestion ne fournissent pas suffisamment de détection, de prévention ou de remédiation des attaques malveillantes par le biais des quatre vecteurs d'attaque les plus courants : appareil, réseau, application, phishing. Ces outils de gestion ne fournissent également pas aux équipes de sécurité les précieuses données intrinsèques de renseignement sur les menaces, nécessaires pour répondre et remédier aux attaques mobiles, comme elles le feraient avec des endpoints traditionnels.

Les solutions de sécurité mobile d'entreprise doivent disposer d'une solution technologique avancée qui tire parti de l'apprentissage automatique pour se protéger contre les attaques des appareils, des réseaux, des applications et du phishing. Ils doivent également s'intégrer dans les écosystèmes de sécurité existants, en s'intégrant à l'environnement EPP, UEM et EDR pour donner une image complète des endpoints. Et la flexibilité est essentielle pour prendre en charge un large éventail de lois sur l'accès aux données et de besoins de conformité qui ne peuvent être satisfaits que par des options d'hébergement cloud flexibles.
En fin de compte, les entreprises doivent adopter une solution de sécurité qui intègre les données, le contrôle et la couverture nécessaires pour la main-d'œuvre distribuée tout en prenant en charge les flux de travail de sécurité actuels.

Zimperium zIPS est une solution avancée de défense contre les menaces mobiles (MTD) conçue pour les entreprises, qui fournit une protection persistante sur les appareils d'entreprise et BYOD. Grâce à z9, le moteur d'apprentissage automatique de Zimperium, zIPS détecte les menaces connues et zero-day sur les appareils et en temps réel, sans introduire de latence ni violer la vie privée des utilisateurs.

Zimperium fournit une sécurité mobile d'entreprise avancée basée sur l'apprentissage automatique, capable de fonctionner sur n'importe quelle plateforme cloud (AWS, Azure, Oracle, Google), et s'intègre de manière transparente dans l'infrastructure de sécurité existante.

Pour en savoir plus sur la manière dont Zimperium peut protéger les appareils mobiles de votre entreprise, visitez le site www.zimperium.com.

ZIMPERIUM®