Livre blanc

Ciblage croissant des périphériques mobiles

Comment protéger sa flotte de smartphones ?

Romain RAVON

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Introduction

Dans le paysage professionnel contemporain, l'intégration des smartphones au sein des entreprises n'est plus une nouveauté mais une nécessité. Ces appareils polyvalents sont devenus des outils indispensables pour la communication, la gestion des tâches, l'accès à l'information et même le contrôle des processus d'affaires en temps réel. Leur capacité à stocker et à traiter des données sensibles, alliée à leur portabilité, offre une flexibilité sans précédent, permettant aux employés de travailler de n'importe où, à tout moment.

Cependant, cette commodité s'accompagne d'une augmentation des risques liés à la sécurité des données. Les smartphones en entreprise sont souvent le siège de données critiques telles que les informations personnelles des clients, les données financières, les secrets commerciaux et la correspondance interne. Cette concentration d'informations sensibles, couplée à la nature connectée des smartphones, en fait des cibles privilégiées pour les cyberattaques. Phishing, logiciels malveillants, attaques par déni de service et espionnage sont autant de menaces que les entreprises doivent désormais considérer comme des risques quotidiens.

Face à ce constat, la mise en place de solutions de cybersécurité robustes et adaptées aux spécificités des smartphones s'avère indispensable.

Il ne s'agit plus seulement de protéger les infrastructures informatiques traditionnelles, mais d'étendre la sécurité à des appareils qui circulent bien au-delà des frontières physiques de l'entreprise.

Cela comprend la mise en œuvre de politiques de sécurité strictes, l'installation de logiciels de sécurité avancés, la formation des employés aux bonnes pratiques en matière de cybersécurité et la création de plans de réponse aux incidents.

L'objectif ultime de ces mesures est double : préserver la confidentialité, l'intégrité et la disponibilité des données d'entreprise, tout en maintenant la productivité et la flexibilité que les smartphones offrent. Dans ce livre blanc, nous explorerons en profondeur les défis et les solutions associés à la sécurisation des smartphones dans l'environnement d'entreprise, avec pour objectif de fournir un cadre de référence pour naviguer dans ce paysage complexe et en évolution rapide.

« L'appareil qui se trouve dans votre poche peut faire bien plus que téléphoner ou envoyer des messages. Votre smartphone stocke presque tous les aspects de votre vie, des souvenirs capturés sous forme de photos aux notes personnelles et aux emplois du temps, en passant par les détails de connexion et divers autres types de données sensibles. »

Lukas Stefanko

Chercheur en logiciels malveillants chez ESET

Chapitre 1 : Utilisation générale du smartphone en entreprise

L'utilisation des smartphones en entreprise a connu une évolution significative ces dernières années, transformant la manière dont les organisations fonctionnent et interagissent tant en interne qu'avec leurs clients et partenaires. Voici un aperçu détaillé de l'utilisation des smartphones en contexte professionnel.

TÉLÉTRAVAIL

La pandémie de COVID-19 a accéléré la transition vers le télétravail, rendant les smartphones encore plus indispensables pour les employés éloignés.

Ces appareils permettent de rester connecté avec les autres salariés, d'accéder à des ressources en ligne, de collaborer sur des documents et de maintenir la productivité en dehors de l'environnement de bureau traditionnel.

UTILISATION PRO/PERSO

Avec l'augmentation du télétravail, les smartphones professionnels sont fréquemment utilisés pour des activités personnelles non prévues, telles que les médias sociaux et les applications personnelles, en plus de leurs fonctions professionnelles comme les emails et les réunions virtuelles.

Cette pratique inappropriée mélangeant les usages soulève d'importantes questions de sécurité, notamment la séparation des données professionnelles et personnelles.

BYOD

Le concept de BYOD (Bring Your Own Device) permet aux employés d'utiliser leurs appareils personnels, tels que les smartphones, pour des tâches professionnelles. La pandémie de COVID-19 a incité 85 %* des organisations à mettre en œuvre des politiques de BYOD.

Cette approche offre une flexibilité accrue et peut améliorer la satisfaction des employés, car ils peuvent utiliser des appareils avec lesquels ils se sentent déjà à l'aise.

Cependant, le BYOD présente également des défis en matière de sécurité des données, car il est difficile de contrôler la façon dont les appareils personnels sont utilisés et sécurisés.

Parmi les entreprises optant pour le BYOD aujourd'hui, 48 % affirment avoir vu des malwares introduits par le téléphone personnel d'un employé, et seulement 4 sur 10 ont déployé une gestion des appareils mobiles (MDM), selon une enquête Samsung de 2023.

Parmi les travailleurs dépendants de la technologie, **66 %** utilisent des smartphones.

«Bring Your Own Device?» par Beyond Identity

*Bring-Your-Own-Device (BYOD) Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021 – 2026).» par Mordor Intelligence

Chapitre 2 : Evolution des menaces sur smartphones

L'univers des technologies mobiles, en constante évolution, s'accompagne malheureusement d'une croissance parallèle des menaces cyber ciblant ces dispositifs. Les smartphones, devenus centraux dans les opérations quotidiennes des entreprises, ne sont pas à l'abri de cette tendance inquiétante. Ce chapitre explore l'évolution des cyberattaques sur mobiles, mettant en lumière les tendances actuelles et fournissant des chiffres récents pour illustrer l'ampleur du problème.

RANSOMWARES

Les logiciels malveillants sur mobiles, particulièrement les ransomwares, ont évolué pour devenir plus sophistiqués. Ces programmes malveillants sont conçus pour infiltrer les smartphones, souvent par le biais d'applications compromises ou de liens malicieux, et peuvent chiffrer les données de l'appareil pour exiger une rançon.

PHISHING

Le phishing, technique bien connue sur les ordinateurs, s'est adapté au monde mobile. Les attaquants utilisent des SMS (smishing), des emails ou des applications de messagerie pour tromper les utilisateurs et les amener à divulguer des informations sensibles ou à télécharger des malwares.

APPLICATIONS MALVEILLANTES

Le nombre d'applications malveillantes disponibles sur les plateformes officielles et non officielles continue d'augmenter. Ces applications peuvent sembler légitimes mais cachent des fonctionnalités malveillantes, allant du vol de données à l'inscription à des services payants sans le consentement de l'utilisateur.

ATTAQUES SUR LE RÉSEAUX SANS FIL

Les attaques via les réseaux WiFi publics non sécurisés restent une menace significative, permettant aux attaquants de intercepter les données transmises depuis et vers un smartphone.

VULNÉRABILITÉS

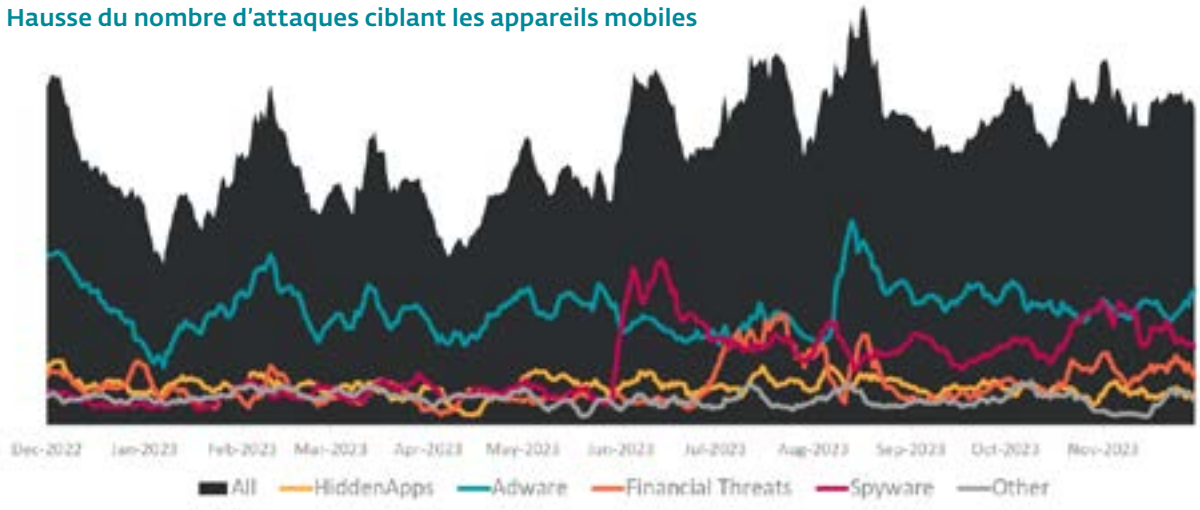
Les vulnérabilités Zero-Day, pour lesquelles il n'existe pas encore de correctif, sont particulièrement prisées par les cybercriminels. Ces failles peuvent être exploitées pour prendre le contrôle total d'un appareil mobile sans que l'utilisateur ne s'en rende compte.

LES ATTAQUES SUR ANDROID EN FORTE HAUSSE

Les attaques se sont multipliées dans différents domaines. Les logiciels publicitaires et les applications cachées étaient les principaux types de malwares ciblant les appareils Android. « Les applications malveillantes cachées changent généralement d'icône et se dissimulent sur l'appareil. Elles commencent alors à afficher des publicités indésirables ou effectuer d'autres actions en arrière-plan » explique M. Kubovic, Security Awareness Specialist chez ESET.

Le nombre de logiciels espions est également en hausse. « Ce type de malware est disponible sur des forums clandestins sous forme de service permettant même à des attaquants peu qualifiés de l'acheter et de l'utiliser pour quelques centaines d'euros. Certains possèdent des fonctionnalités très étendues, notamment d'enregistrement des appels, de prise de contrôle de la caméra, de vol de photos, d'emails et de contacts, » précise M. Kubovic. Les logiciels espions visent généralement à voler autant d'informations et de données que possible, tout en espionnant secrètement l'utilisateur. Pour les attaquants, il s'agit d'un moyen assez simple de gagner de l'argent, puisque les données volées peuvent être revendues sur le dark web, et être utilisées dans d'autres attaques ou à des fins de chantage.

Hausse du nombre d'attaques ciblant les appareils mobiles



Rapport des menaces ESET du 2e semestre 2023

LES SMARTPHONES DEVIENNENT DES CIBLES POPULAIRES

Si les cybercriminels se concentraient auparavant principalement sur les appareils et les logiciels de bureau, leur objectif est en train de changer, car ils ont compris que les services informatiques ont souvent des difficultés à surveiller le trafic et les communications sur les appareils mobiles de l'entreprise.

« Les smartphones ont tendance à être sous-estimés, bien que des données cruciales puissent y être stockées et qu'ils soient utilisés pour accéder à des référentiels et des applications professionnelles.

Les administrateurs informatiques estiment souvent que l'environnement mobile est un peu plus sûr en raison de la compartimentation et du fait que les applications n'ont pas d'accès direct aux activités des autres applications sur l'appareil, mais cela ne suffit pas, » ajoute M. Kubovic.

Les cybervoleurs peuvent néanmoins toujours trouver des moyens d'accéder à l'appareil, comme dans le cas des menaces susmentionnées.

« Les applications mobiles financières ont été récemment ciblées, y compris celles utilisées pour les cryptomonnaies. C'est probablement parce que le bitcoin et d'autres cryptomonnaies sont plus faciles à blanchir, ou n'ont pas besoin d'être blanchies du tout, » explique M. Kubovic, comme l'une des motivations des attaquants. « Les téléphones mobiles sont nos nouveaux portefeuilles, et les cybercriminels le savent. »

Au cours de l'année écoulée, des logiciels malveillants ont été téléchargés sur les appareils **BYOD de 22 %** des entreprises.

Il est alarmant de constater que de nombreuses entreprises ne savent pas ou ne peuvent pas dire si des logiciels malveillants ont été téléchargés sur le lieu de travail.

«Bring Your Own Device?» par Beyond Identity

L'évolution des menaces cyber sur les mobiles exige une vigilance constante de la part des entreprises et des utilisateurs. Les chiffres récents illustrent non seulement l'ampleur du problème mais aussi la nécessité d'adopter des mesures de sécurité robustes, incluant une formation approfondie des employés, l'utilisation de solutions de sécurité mobile avancées, et une mise à jour régulière des systèmes et applications. La protection contre ces menaces en constante évolution est essentielle pour sécuriser les données d'entreprise sensibles et maintenir la confiance des clients.

EXEMPLES CONCRETS

En 2021, la télémétrie ESET a détecté une augmentation annuelle de 428% des malwares bancaires Android. L'année suivante, l'augmentation globale a été entraînée par l'adware. Et 2023 a vu une augmentation significative des cas de logiciels espions Android. L'année dernière, les chercheurs d'ESET ont découvert deux campagnes actives ciblant les utilisateurs Android réparties dans plusieurs magasins d'applications et sites web dédiés.

Les acteurs de la menace ont patché les applications open-source Signal et Telegram pour Android avec un code malveillant que les chercheurs d'ESET ont identifié sous le nom de BadBazaar. Les applications malveillantes portaient le nom de Signal Plus Messenger et FlyGram, et leur but était d'exfiltrer des données d'utilisateur telles que les listes de contacts, les journaux d'appels et la liste des comptes Google.

Signal Plus Messenger est encore plus dangereux que FlyGram, avec sa capacité unique d'espionner les communications de la victime dans l'application Signal originale. Ces informations sensibles pourraient être utilisées pour d'autres attaques d'hameçonnage ciblé contre des responsables d'entreprise.

Un cas similaire a été documenté en juin 2023, lorsque les chercheurs d'ESET ont identifié une version mise à jour du spyware Android GravityRAT. Il était distribué au sein d'applications de messagerie malveillantes mais fonctionnelles, BingeChat et Chatico, toutes deux basées sur l'application OMEMO Instant Messenger. Ce spyware particulier peut exfiltrer les journaux d'appels, les listes de contacts, les messages SMS, la localisation de l'appareil, les informations de base de l'appareil, et des fichiers avec des extensions spécifiques, telles que jpg, PNG, txt, pdf, etc.

Et ce n'est que le début. Les smartphones peuvent être attaqués de nombreuses manières qui mettent en danger les finances et les données des entreprises, telles que par des chevaux de Troie bancaires, le phishing, les vulnérabilités ou le vol physique.

Chapitre 3 : Bonnes pratiques : Comment protéger sa flotte mobile ?

Dans un contexte où les menaces cybernétiques sur les mobiles sont en constante évolution, assurer la sécurité de la flotte mobile d'une entreprise devient un enjeu majeur. La mise en place de stratégies de défense proactive est essentielle pour protéger les données sensibles et préserver l'intégrité des systèmes d'information. Voici une série de bonnes pratiques recommandées pour sécuriser efficacement les dispositifs mobiles en entreprise.

PROTECTION EN TEMPS RÉEL

L'utilisation de solutions de sécurité offrant une protection en temps réel contre les logiciels malveillants, le phishing, et autres cyberattaques est cruciale. Ces outils surveillent en continu les activités suspectes, bloquent les tentatives d'intrusion et avertissent les utilisateurs de potentielles menaces. Ils constituent la première ligne de défense pour détecter et neutraliser les attaques avant qu'elles n'atteignent les données critiques.

MDM

Les solutions de Gestion des Dispositifs Mobiles (MDM) permettent un contrôle centralisé des smartphones et tablettes utilisés dans le cadre professionnel. Elles facilitent la mise en œuvre de politiques de sécurité, l'installation à distance de mises à jour et d'applications sécurisées, ainsi que la suppression à distance des données en cas de perte ou de vol de l'appareil. Le MDM est un outil essentiel pour maintenir la cohérence des pratiques de sécurité sur l'ensemble de la flotte mobile.

AUTHENTIFICATION MULTIFACTEUR (2FA)

L'authentification multifacteur (MFA) ajoute une couche supplémentaire de sécurité lors de l'accès aux applications et données d'entreprise, en exigeant une preuve d'identité additionnelle au-delà du simple mot de passe. Cela peut inclure un code temporaire envoyé par SMS, un appel téléphonique, ou l'utilisation d'une application d'authentification sur n'importe quel appareil défini. Le MFA réduit considérablement le risque d'accès non autorisé en cas de compromission des identifiants de connexion

SÉCURITÉ DES RÉSEAUX WIFI

Encourager l'utilisation de VPNs sécurisés lors de la connexion à des réseaux WiFi publics pour chiffrer le trafic de données et protéger contre l'interception des informations.

FORMATION ET SENSIBILISATION

La formation et la sensibilisation des employés aux risques de sécurité liés à l'utilisation des smartphones en entreprise sont essentielles. Des sessions régulières doivent être organisées pour éduquer le personnel sur les meilleures pratiques de sécurité, la reconnaissance des tentatives de phishing, et les procédures à suivre en cas de suspicion d'attaque. La sensibilisation est une composante critique pour renforcer le comportement sécuritaire au quotidien.

POLITIQUES DE SÉCURITÉ STRICTES

La définition et l'application de politiques de sécurité strictes sont fondamentales pour encadrer l'utilisation des terminaux mobiles. Cela inclut des directives claires sur les types d'applications autorisées, les protocoles de connexion sécurisée, le stockage et le partage des données, ainsi que les procédures en cas de dispositif perdu ou compromis. Ces politiques doivent être régulièrement revues et mises à jour pour s'adapter à l'évolution du paysage des menaces.

AUDIT ET TESTS DE SÉCURITÉ RÉGULIERS

L'évaluation périodique de la sécurité des terminaux mobiles par des audits et des tests de pénétration aide à identifier et à corriger les vulnérabilités avant qu'elles ne soient exploitées par des attaquants.

En intégrant ces pratiques dans la stratégie de sécurité globale de l'entreprise, il est possible de minimiser significativement les risques associés à l'utilisation des terminaux mobiles et de renforcer la posture de cybersécurité de l'organisation.

Chapitre 4 : ESET, partenaire idéal de votre sécurité

Vous l'avez compris, il est important de déployer une protection en temps réel sur les terminaux mobiles et de centraliser cette protection sur une plateforme de cybersécurité unifiée. Si vous souhaitez protéger ce talon d'Achille, nous clôturons cette étude avec un chapitre sur ce qu'ESET, acteur majeur européen, met en place pour vous protéger.

Considérant ces menaces, la mise en œuvre d'une politique de Gestion des Appareils Mobiles (MDM) représente un grand pas en avant. Par exemple, **ESET Mobile Threat Defense** offre aux administrateurs la possibilité de surveiller et de contrôler les applications pour Android et iOS. Avec la protection des endpoints incluse, **ESET Mobile Threat Defense** fournit également des fonctionnalités antivirus et anti-hameçonnage, offrant aux entreprises davantage de capacités de prévention des cyberattaques.

SÉCURITÉ

Les fonctionnalités de sécurité vont de l'anti-malware, l'anti-hameçonnage, l'anti-vol, la sécurité des appareils au contrôle de l'accès web, et bien plus encore.

GESTION

La gestion inclut l'effacement à distance des appareils, la restriction des installations d'applications, la préconfiguration des appareils pour les utilisateurs, et d'autres éléments liés à la gestion informatique.

MULTIPLES OS

La protection mobile couvre généralement les appareils Android et Apple, les deux systèmes d'exploitation mobiles les plus répandus. Comme ces systèmes sont différents, les capacités de protection mobile peuvent également varier entre eux.

INTERFACE UNIQUE

ESET Mobile Threat Defense est intégré nativement dans la plateforme **ESET PROTECT**, sur site ou dans le Cloud. Il est donc possible de centraliser la protection de l'ensemble de ces appareils (PC, mobiles et serveurs) sur une même plateforme de gestion.

DÉPLOIEMENT À DISTANCE

Les administrateurs informatiques sélectionnent simplement les employés avec des terminaux mobiles à protéger, et ils recevront automatiquement un QR code pour télécharger ensuite la protection ESET. Rien de plus simple. La synchronisation est transparente avec les plateformes de gestion cloud. ESET prend en charge Microsoft Intune, Microsoft Entra ID, VMware Workspace ONE et Apple Business Manager.

AUTHENTIFICATION A DOUBLE FACTEUR

ESET offre d'autres couches de sécurité pour vous appareils mobiles.

L'authentification à deux facteurs (MFA) par exemple, est une méthode d'authentification qui, pour vérifier l'identité d'un utilisateur, se base sur deux informations distinctes. La 2FA est beaucoup plus puissante qu'une authentification traditionnelle avec mot de passe ou code PIN statique. En complétant l'authentification traditionnelle grâce à un deuxième facteur dynamique, la 2FA réduit efficacement les risques de violations de données dues à des mots de passe trop faibles ou divulgués. ESET Secure Authentication est compatible avec les applications sur site mais également avec les connexions aux systèmes d'exploitation, les VPN, Remote Desktop, les services Web/Cloud tels que Microsoft ADFS 3.0, Office 365, Google Apps, Dropbox, Outlook Web Acces, en proposant une multitude de méthodes d'authentification.

GOOGLE PLAYSTORE

Depuis 2019, ESET est membre de l'App Defense Alliance et un partenaire actif du programme d'atténuation des logiciels malveillants, qui vise à trouver rapidement les applications potentiellement dangereuses et à les arrêter avant qu'elles n'arrivent sur Google Play.

ESET a été méticuleusement sélectionné par Google pour son expertise éprouvée en détection d'applications malveillantes dans Google Play Store.

ESET a identifié certaines des menaces les plus sophistiquées ciblant les appareils mobiles Android ces dernières années. Avec ce partenariat important, les équipes de chercheurs d'ESET sont étroitement impliquées dans l'analyse de toutes les applications et contribuent à la protection proactive des utilisateurs de Google Play Store.

Ce partenariat contribue fortement à alimenter la puissante télémétrie mondiale d'ESET. C'est pourquoi nos produits sont constamment mis à jour pour faire face aux menaces les plus récentes.

« Notre partenariat avec
un membre respecté du secteur
de la cybersécurité comme ESET
renforce la protection
de l'écosystème Google Play »

Dave Kleidenmacher, Responsable
Sécurité et Respect de la Vie Privée
Android chez Google.

Chez ESET, notre vision ne s'arrête pas au poste de travail. Nous estimons qu'aujourd'hui, un utilisateur possède un PC et un smartphone en entreprise. C'est pourquoi notre champ de protection s'élargit à l'utilisateur.

Le module **ESET Mobile Threat Defense** est entièrement gratuit à partir du bundle **ESET PROTECT Advanced** (et tous les bundles supérieurs). Pour chaque licence Endpoint acquise, vous avez la possibilité de sécuriser également un mobile, sans frais supplémentaires. Autrement dit, une seule licence vous permet de protéger à la fois l'ordinateur et le smartphone de chaque utilisateur.

À propos d'ESET

Quand la technologie engendre le **progrès**, ESET est là pour **le protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

protégé par ESET depuis 2016
plus de 32 000 endpoints

T

partenaire FAI depuis 2008
2 millions d'utilisateurs

Allianz Suisse

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

protégé par ESET depuis 2017
plus de 9 000 endpoints

Plus de 30 ans
d'innovation continue

1er éditeur Européen
de solutions de sécurité

Focus continu sur la
technologie

Croissance continue
depuis sa création

www.eset.com/fr