Relever le défi de la sécurisation des smartphones personnels utilisés dans le cadre professionnel

Conférenciers :

- LCL Bruno CAMEL, Chef de la section transformation numérique et données de l'armée de Terre
- Renaud Gruchet, Chief Business Innovation Officer chez Pradeo

Résumé de la conférence :

Aujourd'hui, de nombreuses technologies permettent de sécuriser les flottes de smartphones professionnels. Mais qu'en est-il des appareils mobiles personnels utilisés dans le cadre du travail ?

Contrairement aux terminaux fournis par les entreprises à leurs membres, qui sont administrés et sur lesquels le service IT peut contrôler les usages et les menaces, les mobiles personnels représentent un espace privé ou les organisations ont un champ d'action réduit.

Ainsi, les entités s'appuyant sur les smartphones personnels de leurs membres pour proposer des services métiers se retrouvent dans une impasse : comment sécuriser l'usage des mobiles BYOD sans envahir l'espace personnel et dans le respect des lois sur la protection des données ?

Lorsque l'Armée de Terre française nous a partagé cette problématique, nous avons conçu ensemble une réponse de sécurité adaptée à leur réalité opérationnelle.

Cette conférence présentera le déroulement d'un cas réel, des premiers défis rencontrés jusqu'à l'innovation technologique aujourd'hui téléchargée par plus de 14.000 utilisateurs.

La présentation sera assurée par le LCL Bruno CAMEL, Chef de la section transformation numérique et données de l'armée de Terre et Renaud Gruchet, Chief Business Innovation Officer de Pradeo.

SOMMAIRE

1. Usages mobiles : menaces et risques encourus

Les appareils mobiles sont de véritables mines d'or pour les cybercriminels à la recherche de données sensibles. En effet, ils ont des capacités inhérentes qui, lorsqu'elles sont exploitées illégalement, peuvent fournir un accès direct à toutes les données qu'ils possèdent. Pour compromettre un mobile, les attaquants exploitent les applications, le réseau, le système d'exploitation ou une combinaison de ces trois vecteurs. Le système peut être compromis pour s'octroyer des privilèges d'administration sur le téléphone, les applications installées peuvent avoir des comportements malveillants à l'insu de l'utilisateur pour voler ses données (liste de contacts, captures d'écran…), et les réseaux peuvent être attaqués pour intercepter les communications.

2.1. Les applications mobiles, principale source d'attaque

Depuis le lancement du premier iPhone en 2007 et l'ouverture des magasins d'applications officiels App store et Google Play en 2008, le nombre d'applications mobiles a explosé atteignant aujourd'hui 5,2 millions selon le cabinet d'étude Statista.

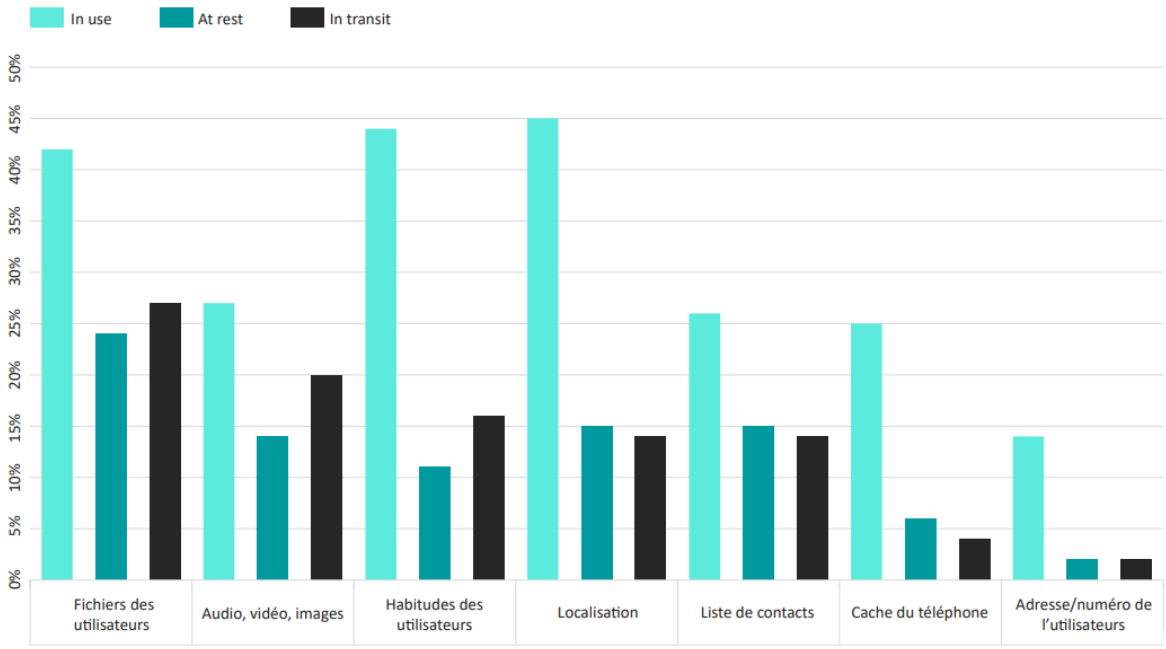
Pour fonctionner, une application mobile nécessite d'accéder à certaines données de l'appareil sur lequel elle s'exécute (par exemple la version de l'OS pour adapter son fonctionnement), et de manipuler des données appartement à l'utilisateur (par exemple des informations de connexion, la géolocalisation, les contacts…).

Par nature, les applications traitent des données critiques et peuvent les exposer lorsque leur raison d'être est malveillante ou lorsqu'elles sont développées sans respecter les bonnes pratiques de sécurité. Ainsi, elles représentent un danger pour la confidentialité des informations de leurs utilisateurs, et par extension pour les organisations s'appuyant sur des mobiles pour mener leurs opérations.

D'après une étude menée par Pradeo en mars 2023, 76% des attaques détectées sur mobile exploitent des applications pour parvenir à leurs fins.

1.1.1 Les applications intrusives, ou *leakware*

Le rapport de sécurité mobile annuel publié en 2022 par Pradeo dévoile le volume de données personnelles les plus collectées par les applications mobiles. L'étude réalisée sur une centaine de milliers de terminaux mobiles protégés par l'entreprise démontre entre autres que 14% des applications exfiltrent la géolocalisation et la liste de contacts de l'appareil vers des serveurs distants. Ce graphique est extrait de ce rapport, il montre le pourcentage d'applications mobiles traitant les données des utilisateurs et quels types de traitement sont effectués.



In use = Donnée accédée
At rest = Donnée stockée
In transit = Donnée envoyée hors de l'appareil

Ces fuites de données sont le plus souvent programmées par les propriétaires d'applications dans le but de monétiser leur activité. Pour ce faire, ils incluent volontairement dans leurs programmes des librairies publicitaires qui collectent les données personnelles des utilisateurs. Ils reçoivent en contrepartie une compensation financière calculée au volume.

Une application mobile gratuite contient en moyenne 6 bibliothèques de marketing qui font d'elle un espace publicitaire à part entière, sur lequel des annonces ciblées peuvent être diffusées et à partir duquel les données des utilisateurs sont récoltées et revendues.

Lorsque l'on regarde sur une plus grande échelle, on s'aperçoit que les mêmes bibliothèques publicitaires reviennent fréquemment. Pradeo a identifié les 3 bibliothèques les plus courantes sur un échantillon d'applications représentant toutes les catégories, dans plus d'une quarantaine de pays à travers le monde. La première est présente dans 43% des applications, la deuxième dans 10% et la suivante dans 8%. Plus concrètement, ce sont des millions d'applications mobiles concernées et des milliards de données qui sont envoyées sur les serveurs de ces 3 entreprises publicitaires.

Lors d'une étude, Pradeo a constaté que les applications de jeu et de réseau social sont celles qui intègrent le plus de bibliothèques publicitaires. Cependant, c'est en se concentrant sur des applications vouées à des opérations plus sérieuses, dans le domaine financier et de la santé, que les résultats sont plus troublants. En effet, certaines de ces applications sont également dotées de modules publicitaires, malgré la haute confidentialité des données qu'elles manipulent.

D'un point de vue technique, la méthode généralement utilisée par les développeurs pour intégrer les bibliothèques de publicité est basique. Celle-ci fait simplement appel à l'API afin de lancer le service principal de la bibliothèque. Lorsqu'aucune spécification supplémentaire n'est donnée, les sociétés marketing sont autorisées à récupérer toutes les données collectées par les applications qui intègrent leur bibliothèque.

Bien que ces pratiques soient autorisées, peu d'utilisateurs mobiles savent identifier avec précision les données auxquelles accèdent leurs applications et très peu d'entre eux sont au courant que celles-ci sont quasi systématiquement revendues et envoyées aux quatre coins du monde. La variété des catégories d'applications touchées et l'utilisation généralisée des 3 bibliothèques observées démontrent que certaines entreprises établissent des profils très précis de chacun de nous, comprenant nos contacts, notre journal d'appels, nos photos, nos SMS, notre emploi du temps, nos déplacements, nos préférences...

Le terme *leakware* a été utilisé pour la première fois par Gartner dans son Market Guide for Mobile Threat Defense publié en janvier 2023 pour faire référence à ces applications qui recueillent massivement les données de leurs utilisateurs pour les envoyer hors de leurs mobiles, sans que cette collecte de données ne soit nécessaire à leur fonctionnement.

L'interdiction récente d'utiliser TikTok pour les membres de nombreux gouvernements met l'emphase sur ce procédé généralisé qui consiste à tirer profit des applications mobiles pour collecter à outrance les données personnelles des utilisateurs. Au-delà de TikTok, ce sont des millions d'applications populaires officielles qui partagent les mêmes pratiques et qui mettent en péril la sécurité des utilisateurs et de leurs organisations.

Tout ceci a des conséquences bien réelles. Par exemple, dans la nuit du 31 décembre 2022 au 1er janvier 2023, la concentration de militaires russes à Makiivka en Ukraine a été repérée par l'activité de leurs téléphones personnels et notamment via la collecte de leur géolocalisation, ce qui a déclenché une frappe d'artillerie ukrainienne.

1.1.2 Les applications malveillantes

Un logiciel malveillant est spécifiquement conçu pour perturber, endommager, ou obtenir un accès illégal à un appareil ou à des données, alors que la victime est le plus souvent inconsciente de l'attaque. Le nombre d'appareils infectés par des logiciels malveillants, tels que les spywares, les droppers, les banking trojan ne cesse de croître.

Cette hausse des tentatives de piratage pousse les utilisateurs mobiles à faire preuve d'un minimum de vigilance. Pour les duper, les pirates sont amenés à travailler l'apparence de leurs outils et à améliorer leurs tactiques pour se montrer plus convaincants. L'un des leviers fréquemment utilisé est la publication de malware sur les magasins d'application officiels, espace considéré sécurisé, mais qui ne l'est en réalité que peu.

Par exemple, pour contourner les contrôles standard de sécurité effectués par les magasins d'application officiels (les non-officiels n'en réalisent pas ou peu), les cybercriminels y publient régulièrement des applications qui ne comportent pas de programmes malveillants mais en revanche, sont programmées pour les télécharger une fois installés sur les appareils des utilisateurs.

C'est ce que l'on qualifie de trojan-dropper, parfois appelé dropper, programme conçu pour installer un malware sur l'appareil de son utilisateur. Sur mobile, un dropper se présente sous la forme d'une véritable application, livrant un service fonctionnel. Une fois installée, cette application malveillante effectue des vérifications du système sur lequel elle est exécutée et lance l'installation du malware lorsque le moment est opportun.

L'utilisation de dropper n'est pas nouvelle, mais au fil des années l'outil s'est perfectionné pour assurer sa survie et améliorer son efficacité. Avant, un dropper contenait dans son code le malware (aussi appelé payload) qu'il prévoyait d'installer, ainsi que les lignes de commande pour l'installer.

Maintenant, les dernières versions de dropper se connectent à des serveurs de C&C (Command & Control) et téléchargent leur payload via le réseau internet, une fois installés sur un appareil.

Au cours des 12 derniers mois, 4,92% des applications mobiles que nous avons testées se connectent à des serveurs C&C et 2,45% installent des applications téléchargées depuis le réseau. En procédant ainsi, les pirates optimisent leur chance de passer avec succès les tests de sécurité des magasins d'applications qui ne réalisent pas d'analyse comportementale.

Début 2022, les chercheurs de Pradeo ont identifié une application de type trojan-dropper distribuée sur Google Play et installée par plus de 10 000 personnes. L'application en question, appelée 2FA Authenticator, fournissait un véritable service d'authentification à double facteur en utilisant le code open-source de l'application officielle Aegis, auquel les pirates avaient injecté du code malveillant.

L'analyse a révélé que le dropper en question réalisait son attaque en deux étapes. Lors de la première, il collectait des informations sur ses utilisateurs afin de savoir quelles applications bancaires ils utilisaient, et il désactivait des fonctionnalités de sécurité du terminal. Le lancement de la seconde étape était conditionné aux informations récoltées lors de la première. Si le contexte lui paraissait favorable, il installait le malware Vultur, un type de malware avancé qui cible principalement les interfaces bancaires en ligne pour voler les informations d'identification des utilisateurs et d'autres informations financières confidentielles.

1.1.3 Les applications vulnérables aux attaques

Les applications web et mobiles peuvent être vulnérables en raison de mauvaises pratiques au cours de leur développement ou à cause des bibliothèques qu'elles intègrent. Ces vulnérabilités les exposent à des attaques. Des centaines de vulnérabilités sont référencées par la US National Vulnerability Database, le projet de sécurité mobile OWASP, l'USCERT, etc. pour aider les développeurs à créer et maintenir des applications sécurisées. Pourtant, 3 applications mobiles sur 5 présentent des vulnérabilités qui les exposent à des fuites de données (Source : Rapport de sécurité mobile 2022 de Pradeo), des attaques par déni de service (DoS), et des attaques Man-In-The-Middle.

Début 2023, la société Hopinnov, pionnière dans la digitalisation de la logistique hospitalière et utilisatrice de la solution d'analyse de code source de Pradeo. A découvert une vulnérabilité dans le code d'une bibliothèque open source très répandue, à destination des développeurs. Disponible en téléchargement libre auprès de la communauté, ce module d'interface qui permet de laisser des commentaires comportait une faille permettant de récupérer un droit administrateur sur l'application.

Dans le cadre de la solution POC & PICK d'Hopinnov, le module de commentaire touché par la faille permettait aux accédants de partager leurs retours concernant les protocoles opératoires : la préparation des salles opératoires, le matériel utilisé, la disposition de la salle, l'installation du patient…

Cette vulnérabilité ouvrait la porte à une élévation des privilèges qui aurait pu s'avérer problématique concernant les données de l'hôpital. Un cybercriminel aurait pu récupérer des identifiants et mots de passe d'administrateur et ainsi se connecter simplement à l'interface. Ouvrant la possibilité de modifier à souhait les protocoles opératoires et de récupérer toutes les informations disponibles dans l'application.

2.2. Les risques liés au réseau

En quelques années, les smartphones et tablettes sont devenus le principal point d'accès à internet dans le monde. Cette évolution a entrainé la création de nombreux réseaux Wi-Fi permettant d'être connecté en permanence et offrant un nouveau terrain de jeu aux pirates. Le nombre grandissant de réseaux publics et de personnes s'y connectant a démultiplié les opportunités d'attaques du type Man-In-The-Middle. Une attaque MITM, se réalise lorsqu'une communication entre deux parties est interceptée par une entité tierce. L'auteur de l'attaque espionne illicitement la communication et l'altère parfois, tout en s'assurant que l'échange paraisse normal. Cette attaque peut également se réaliser via une antenne relais malveillante.

En février 2023, des malfaiteurs ont été arrêtés après avoir mené une cyberattaque d'envergure visant des utilisateurs mobiles, à Paris. L'attaque se distinguait par l'emploi inattendu d'un outil d'espionnage généralement réservé aux services de renseignements, appelé IMSI catcher.

L'IMSI catcher, pour International Mobile Subscriber Identity, n'a rien de nouveau puisque la première implémentation de ce type d'outil remonte à 1993. De nombreuses entreprises en fournissent aux gouvernements. Ces dispositifs sont notamment utilisés pour assurer la sécurité lors de grands rassemblements ou de célébrations.

L'IMSI catcher permet d'espionner les communications des utilisateurs mobiles situés dans sa zone de proximité, en se substituant aux antennes relais classiques tout en assurant le maintien du service. Dans la récente attaque découverte, l'équipement était disposé dans un véhicule qui a sillonné les rues de Paris. Les appareils mobiles étant constamment à la recherche du signal le plus fort pour se connecter sur un relais, près de 16000 smartphones s'y seraient connectés selon Les Numériques. Bien qu'une partie du trafic soit chiffrée, de nombreuses données personnelles peuvent tout de même être exploitées.

En l'occurrence, l'IMSI catcher a été utilisé pour récolter des numéros de téléphone pour enrichir une vaste campagne de smishing, hameçonnage via SMS, se faisant passer pour l'Assurance Maladie. Cette attaque illustre encore une fois la convergence des techniques de piratage utilisées par les criminels pour parvenir à leurs fins.

Finalement, cet outil particulièrement intrusif n'est pas l'apanage des Etats, le chercheur en sécurité Chris Paget en a fait la démonstration à la DEF CON de 2010 en perpétrant l'attaque en direct. Il a déclaré avoir mis en place l'IMSI catcher à base de matériel générique pour la somme de 1 500 $.

2.3. L'exploitation des vulnérabilités des systèmes Android, iOS et des applications

Régulièrement, des failles de sécurité sont découvertes dans les systèmes d'exploitation des terminaux Android et iOS. Une fois détectées, les éditeurs développent des correctifs qu'ils diffusent aux utilisateurs par le biais de mises à jour, puis ils divulguent simultanément les vulnérabilités existantes (CVE). Une fois rendues publiques, les cybercriminels peuvent exploiter les failles de sécurité des appareils fonctionnant sous des versions obsolètes pour obtenir des droits étendus et accéder illégalement aux données ou aux communications.

Parmi les mobiles des flottes d'entreprise, 81% des appareils iOS et 82% des appareils Android utilisent des versions d'OS obsolètes (rapport de sécurité mobile annuel de Pradeo, 2022), pour de multiples raisons. Le plus souvent, les utilisateurs ne sont pas au fait des risques encourus lorsqu'ils retardent

les mises à jour système et ne les activent pas pour gagner du temps. Fréquemment aussi, les mobiles ne sont pas de dernière génération et leurs modèles ne supportent pas les nouvelles versions.

Pegasus illustre parfaitement ce type d'attaque, car le programme espion qui a fait son grand retour en 2022 exploite les vulnérabilités des applications et des systèmes d'exploitation pour se déployer. La résurgence récente de Pegasus fait 50 000 victimes directes, mais les informations volées concernent également toutes les personnes en contact avec ces personnes.

Pour compromettre des cibles critiques, le logiciel espion Pegasus exploite les vulnérabilités d'applications courantes telles que iMessage, FaceTime, Safari, WhatsApp, etc. possédant un module web (WebKit, WebView...) afin d'atteindre des URLs générées dynamiquement, invisibles et non classifiées. Les pages atteintes exécutent alors du code JavaScript pour exploiter d'autres vulnérabilités afin de sortir des sandboxes des applications, contournant ainsi tous les mécanismes en place dans les systèmes Android et iOS.

Une fois dans les couches du système, Pegasus exploite une séquence de vulnérabilités connues et zeroday du processeur afin d'exécuter du code arbitraire (Arbitrary Code Execution) sans nécessiter que le système soit rooté ou jailbreaké. Le code est chargé directement dans la RAM et non en tant qu'application, ce qui le rend délicat à détecter. Après avoir franchi toutes ces étapes, Pegasus exfiltre massivement les données des utilisateurs, y compris les données chiffrées (conversations whatsapp, telegram, signal...).

2.4. Conséquences dans le domaine militaire

Des usages mobiles non sécurisés peuvent mettre en péril les opérations militaires et la sécurité nationale.

- **Mise en danger des militaires :** Les mobiles sont devenus des outils essentiels pour la communication et la coordination dans les opérations militaires. S'ils sont compromis, cela entraîne des fuites d'informations sensibles, la perturbation des opérations et même la mise en danger des soldats sur le terrain.
- **Cyberespionnage :** Les cybercriminels et les acteurs étatiques hostiles ciblent activement les smartphones pour collecter des informations sur les activités militaires, les stratégies et les plans. Les militaires manipulent des informations confidentielles. Les cyberattaques visant les mobiles peuvent exposer ces données.
- **Interception et modifications des communications :** Les cyberattaques peuvent altérer les communications militaires, créant ainsi des confusions, des désinformations ou des ordres erronés.
- **Arrêt des services :** Un seul appareil mobile compromis peut potentiellement infecter tout un réseau, en déployant par exemple un rançongiciel, entraînant ainsi une inopérabilité des services et des perturbations majeures.

2.5. Spécificités des usages mobiles personnels

Le système d'information d'une organisation (courriels, outils, ressources…) est généralement rendu accessible à ses membres via leurs terminaux mobiles. Parmi ces mobiles, on retrouve :

- Les terminaux administrés par l'organisation, qui peuvent être la propriété de l'utilisateur (BYOD pour *Bring Your Own Device*) ou de l'entité dont il fait partie. On distingue sur Android

la possibilité de créer 2 profils, pour scinder les usages professionnels et personnels au sein d'un même appareil.
- Les terminaux non-administrés par l'organisation, personnels.

Selon le propriétaire d'un appareil ou d'un profil, professionnel ou personnel, la nature des usages et le niveau de vigilance de l'utilisateur diffèrent. D'autre part, la sécurisation face aux cybermenaces ne peut pas se faire de la même manière. Deux causes majeures induisent cette différence de traitement, la première étant d'ordre légal : le Règlement Général sur la Protection des Données (RGPD) a des exigences strictes en matière de traitement des données personnelles. La deuxième étant liée l'utilisateur lui-même, qui se soucie de protéger sa vie privée et n'est pas prêt à laisser son organisation contrôler son appareil ou profil personnel sans garantie de confidentialité.

1.5.1 Des usages libres, plus risqués par nature

Les usages sur un mobile personnel sont généralement plus risqués que sur un mobile professionnel en raison de plusieurs facteurs clés. Tout d'abord, les mobiles personnels sont souvent utilisés pour des activités diverses telles que les réseaux sociaux, le téléchargement d'applications non vérifiées, et la navigation sur des sites potentiellement dangereux. Cette variété d'usages expose les utilisateurs à un éventail plus large de menaces telles que les logiciels malveillants, les escroqueries en ligne et les cyberattaques. Qui plus est, les utilisateurs de mobiles personnels ont tendance à accorder moins d'attention à la sécurité, utilisant souvent des mots de passe faibles ou réutilisés et ignorant par exemple les mises à jour de sécurité.

En revanche, les mobiles professionnels sont généralement soumis à des politiques de sécurité plus strictes établies par l'organisation propriétaire, ce qui limite dans une certaine mesure les risques. Les applications et les activités non autorisées sont restreintes, réduisant ainsi les risques liés aux logiciels malveillants et aux violations de données. De plus, les entreprises déploient souvent des solutions de gestion des appareils mobiles (MDM pour Mobile Device Management) et de détection et réponse aux menaces (MTD pour Mobile Threat Defense) pour surveiller et sécuriser leur flotte.

En somme, les usages sur un mobile personnel comportent un niveau plus élevé de risque en raison de l'absence de contrôles de sécurité rigoureux et de la propension des utilisateurs à adopter des pratiques moins sécurisées.

1.5.2 Réticence des utilisateurs

Les utilisateurs mobiles peuvent hésiter ou s'opposer à l'idée que leur organisation sécurise leurs appareils mobiles personnels. Tout d'abord, il y a une préoccupation fondamentale liée à la vie privée. Les utilisateurs craignent que les mesures de sécurité imposées par leur organisation impliquent un accès accru à leurs données personnelles, ce qui peut engendrer un sentiment d'intrusion dans leur sphère privée. Cette crainte est notamment renforcée par des précédents où des entreprises ont été impliquées dans des violations de la vie privée ou des abus de données. Un exemple notable d'espionnage des salariés d'une organisation est l'affaire de l'entreprise Uber en 2017. Il a été révélé que Uber avait utilisé un outil secret appelé "God View" pour suivre en temps réel les déplacements des chauffeurs et des salariés de l'entreprise. Ces révélations ont suscité une indignation généralisée.

En outre, certains utilisateurs perçoivent que les mesures de sécurité imposées par l'organisation restreignent leur contrôle sur leurs appareils personnels. Cela peut inclure des restrictions sur les applications qu'ils peuvent télécharger, les sites web qu'ils peuvent visiter ou même des limitations

quant à l'utilisation générale. Cette perte de liberté perçue est alors considérée comme une atteinte à leur expérience d'utilisation.

Enfin, la sécurisation d'un appareil rend souvent son utilisation plus complexe ou moins pratique. Les mesures de sécurité telles que l'authentification à deux facteurs ou les politiques de gestion des appareils pourraient potentiellement ajouter des étapes supplémentaires lors de l'accès à l'appareil ou aux applications, ce qui est perçu comme fastidieux. Certains utilisateurs craignent que cela perturbe leur flux de travail ou leur expérience de divertissement sur leurs appareils personnels.

Pour surmonter ces réticences, il est crucial de communiquer de manière transparente sur la légitimité de la sécurisation et les avantages qu'elle apporte, tout en respectant les préoccupations légitimes des utilisateurs en matière de vie privée et d'expérience utilisateur.

1.5.3. Ce que le RGPD requiert en matière de traitement des données personnelles

Lorsqu'une organisation traite les données personnelles de citoyens européens, le Règlement Général sur la Protection des Données (RGPD) lui impose des mesures de sécurité strictes y compris lorsque son objectif est d'assurer la sécurité d'un appareil (ordinateur, smartphone, tablette…). Voici quelques-unes des principales exigences imposées par le RGPD :

- **Base légale du traitement :** Le RGPD stipule que le traitement des données personnelles doit reposer sur une base légale spécifique. Cela peut inclure le consentement de la personne concernée, l'exécution d'un contrat, le respect d'une obligation légale, la protection des intérêts vitaux de la personne, l'exécution d'une mission d'intérêt public ou l'intérêt légitime du responsable du traitement ou d'un tiers.
- **Transparence et informations :** Les organisations doivent fournir des informations claires et compréhensibles aux personnes concernées concernant le traitement de leurs données personnelles. Cela comprend des détails sur les finalités du traitement, les catégories de données traitées, les destinataires des données, la durée de conservation, ainsi que les droits des personnes concernées.
- **Consentement éclairé :** Lorsque le traitement repose sur le consentement, celui-ci doit être donné de manière libre, spécifique, éclairée et univoque. Les personnes doivent être en mesure de retirer leur consentement à tout moment.
- **Droits des personnes concernées :** Le RGPD renforce les droits des personnes concernées, notamment le droit d'accès aux données, le droit de rectification, le droit à l'effacement (ou "droit à l'oubli"), le droit à la limitation du traitement, le droit à la portabilité des données et le droit d'opposition au traitement dans certaines circonstances.
- **Protection des données sensibles :** Les catégories spéciales de données personnelles, telles que les données de santé ou les données à caractère racial ou ethnique, sont soumises à des protections accrues en vertu du RGPD. Leur traitement est généralement interdit, sauf si des exceptions spécifiques s'appliquent.
- **Responsabilité du responsable du traitement :** Les organisations sont tenues de démontrer leur conformité au RGPD en mettant en place des politiques, des procédures et des mesures de sécurité adéquates pour protéger les données personnelles.
- **Notifications de violation de données :** En cas de violation de données personnelles susceptible de présenter un risque pour les droits et libertés des personnes, les organisations sont tenues de notifier l'autorité de contrôle compétente et, dans certains cas, les personnes concernées, dans un délai de 72 heures.
- **Transferts internationaux de données :** Le RGPD impose des restrictions aux transferts de données personnelles en dehors de l'UE vers des pays qui ne garantissent pas un niveau

adéquat de protection des données, à moins que des garanties appropriées ne soient mises en place.

Toutes ces mesures peuvent limiter le champ d'action d'une solution de cybersécurité, mais aussi, s'avérer très chronophages et délicates à gérer.

2. Le projet Milistore de l'armée de Terre

En 2018, la cellule transformation numérique de l'armée de Terre française a engagé un projet visant à sécuriser l'usages des mobiles personnels de ses ressortissants. L'objectif majeur était de prévenir la fuite de renseignements tactiques (géolocalisation, horaire des rondes, matériel à disposition, etc…) disponibles sur ces appareils non-administrés et non-sécurisés.

Les responsables du pilotage de ce projet avaient conscience qu'il était illusoire de vouloir empêcher les soldats d'utiliser leurs appareils mobiles personnels, qui sont un vrai lien avec leur base arrière et qui contribuent ainsi au moral des troupes. Aucune interdiction ni confiscation n'était envisageable, car elle se serait avérée inefficace. Les smartphones font désormais parti de notre quotidien, et le projet avait pour but d'accompagner la numérisation grandissante de l'espace de bataille.

D'une part, il était question de protéger les services mobiles de l'armée de Terre utilisés sur les appareils personnels et d'autre part, de sensibiliser aux risques provenant des mobiles et d'accompagner dans la sécurisation de leur usage.

Le MINARM s'est alors tourné vers Pradeo avec une problématique : comment sécuriser l'usage des mobiles BYOD sans envahir l'espace personnel et dans le respect des lois sur la protection des données ? Les deux organisations ont alors conçu ensemble une réponse de sécurité adaptée à la réalité opérationnelle des militaires.

2.1. Contexte et genèse du projet

L'irruption des téléphones portables et des smartphones dans la société civile s'est tout naturellement fait ressentir dans les forces armées, étant donné qu'elles ne sont que le reflet de la société. L'armée de Terre a constaté que les téléphones portables étaient utilisés de plus en plus, que ce soit à des fins de simple communication téléphonique en point-à-point, de communication groupée (ex : vie d'une unité, d'un bureau ou d'une promotion) via des applications de messagerie instantanée comme WhatsApp, Signal ou Tchap, ou que ce soit même via des applications mobiles développées par le MINARM, notamment pour former les nouvelles recrues ou pour répondre à d'autres besoins que nous ne pouvons détailler ici.

Pour faire simple, la vie quotidienne des militaires est de plus en plus liée à internet et le MINARM encourage ses ressortissants à accomplir un nombre croissant de formalités administratives sur internet et ces projets continuent. L'avènement de l'authentification unique MinDef Connect en est un exemple, les parcours utilisateurs évoluent et grandissent sur internet.

Pour l'armée de Terre, cette problématique est d'autant plus cruciale que la majorité de son personnel est constituée de soldats en unités de combat, dont le métier ne nécessite pas un accès quotidien à des systèmes d'information métier sur l'environnement de travail habituel du ministère, Intradef. Autrement dit, un soldat a besoin d'une arme pour faire son métier, il n'a pas besoin d'avoir un

ordinateur derrière un bureau. Dans les régiments de l'armée de Terre, le nombre de stations reliées au réseau Intradef est relativement limité, il est donc impossible de modifier des usages à destination des soldats, essentiellement les militaires du rang, si on se cantonne à des projets sur le réseau de travail Intradef. Ce manque d'accessibilité à Intradef est vraiment spécifique à l'armée de Terre, la problématique n'est pas aussi marquée dans les autres armées, directions et services du ministère des armées, pour diverses raisons organisationnelles.

2.2. Défis

L'enjeu de cybersécurité représenté par les smartphones et exposé précédemment est un impératif majeur de protection de la force, car les militaires sont une cible pour les services et forces armées adverses. Les mobiles sont un vecteur privilégié pour recueillir du renseignement sur l'ennemi. Or, les militaires emportent systématiquement leurs téléphones personnels dans leurs déplacements professionnels, c'est l'engin qu'ils portent sur eux quasiment en permanence, parfois même dans des zones protégées où les téléphones portables sont prohibés, ce n'est un secret pour personne. Comment faire pour concilier ces deux extrêmes, apporter des usages sur internet et encadrer l'usage de téléphones personnels sur le lieu de travail, tout en protégeant les militaires contre les vulnérabilités et les menaces que peuvent représenter ces téléphones ?

Un vrai défi supplémentaire était le caractère hétérogène de la flotte de terminaux mobiles, lié au fait qu'ils étaient personnels : cela implique que l'utilisateur a tous les droits sur son terminal, que l'armée ne peut rien imposer et que l'armée ne peut pas – et ne souhaite pas – administrer les terminaux personnels des militaires.

Un contrôle par l'armée sur les téléphones aurait été perçu comme intrusif par les utilisateurs finaux qui ne souhaitent évidemment pas que leur smartphone personnel soit géré par leur employeur, même militaire. Pourtant, il fallait protéger les ressortissants de l'armée de Terre contre les adversaires de la France en améliorant leur posture de cyber protection.

Il fallait que le projet ait vraiment une double facette, promouvoir des usages qui seraient vraiment disponibles à tous, sur Internet, via des smartphones, et offrir gracieusement aux ressortissants de l'armée de Terre une protection efficace, à l'état de l'art, sur ces smartphones.

2. 3. La réponse apportée par le projet Milistore

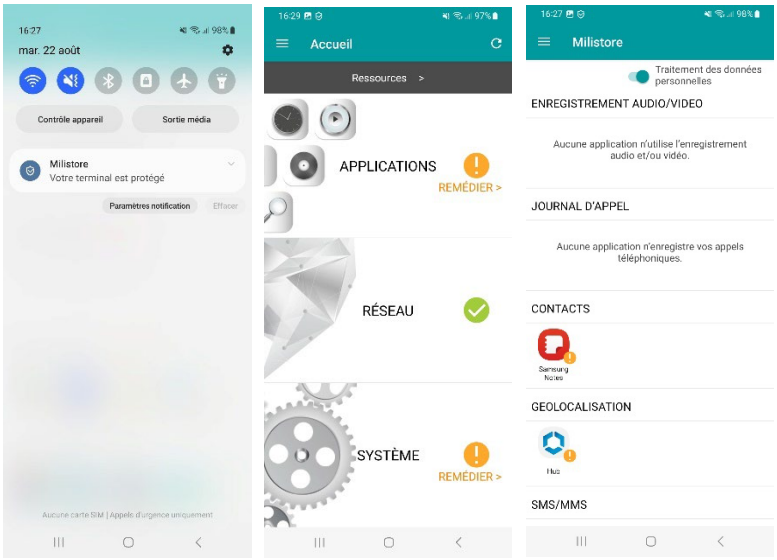
2.3.1. Concept

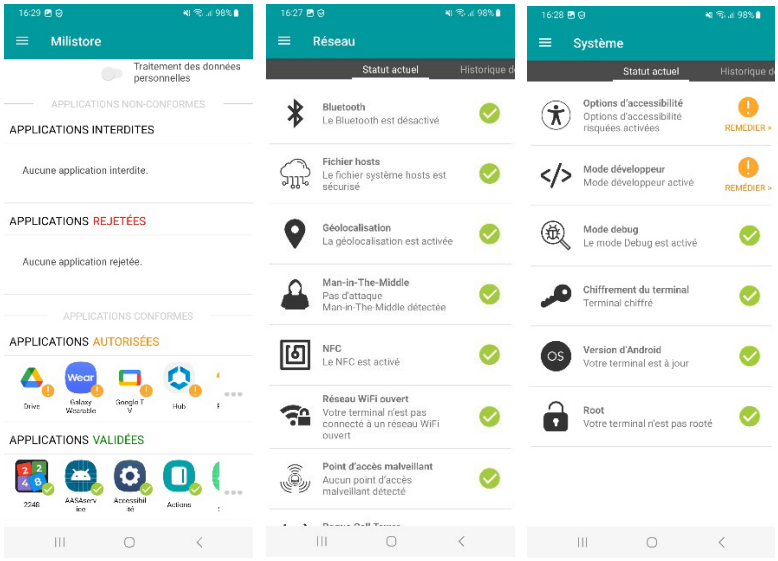
Le Milistore est un outil qui a été lancé par la cellule transformation numérique de l'armée de Terre en collaboration avec Pradeo. Il s'agit avant tout d'une solution de sécurité sur le smartphone personnel, couplée à une boutique d'applications privées sécurisée qui est utilisée par l'armée de Terre pour distribuer à ses membres des applications mobiles privées et sécuriser les usages mobiles, professionnels et personnels. Milistore se présente sous la forme d'une application mobile, disponible pour Android et iOS. Son usage est strictement réservé aux ressortissants de l'armée de Terre.

L'application offre aux utilisateurs deux fonctionnalités complémentaires :

- Un service de sécurité mobile pour établir un diagnostic de sécurité du terminal de l'utilisateur et l'accompagner dans la remédiation des menaces.

- Une boutique privée pour accéder à des applications privées du ministère, à des applications publiques recommandées, à des sites web référencés, ou à des documents mis à leur disposition.





2.3.2. Réponses aux contraintes liées au caractère personnel des mobiles

L'application Milistore est utilisée sur des smartphones contenant des données personnelles, si elle les collectait, elle devrait répondre à des exigences de confidentialité strictes pour se conformer aux lois de protection des données (RGPD, recommandations de la CNIL…).

Sécuriser les usages mobiles est une base légale valable pour collecter des données personnelles, mais cela demande une sécurisation accrue de toutes les données récoltées, et surtout, les utilisateurs finaux ne perçoivent pas cette intrusion comme acceptable. Ainsi, au début du projet Milistore, un choix structurant a été fait : celui de ne collecter aucune donnée personnellement identifiable. Cette contrainte était inévitable pour convaincre les utilisateurs d'adopter la solution.

D’autre part, l’expérience utilisateur a toute son importance. L’application Milistore ne doit jamais être perçue comme étant restrictive ou intrusive, au risque de diminuer son adoption. A contrario, elle doit apporter une plus-value pour les utilisateurs. Ainsi, même si cela est possible techniquement et que cela se fait sur les appareils professionnels via des solutions de Mobile Threat Defense, Milistore ne remédie par les menaces détectées. Son champ d’action comprend la sensibilisation, l’alerte en cas de menace, l’accompagnement à la remédiation des menaces pour retrouver un environnement sécurisé et un accès aux ressources professionnelles conditionné à la sécurité.

2.3.3. Diagnostic de sécurité

Le diagnostic de sécurité réalisé par Milistore porte sur les applications (pour identifier les applications malveillantes ou intrusives collectant à l’excès et de manière inappropriées des données personnelles), sur les connexions réseau établies depuis le terminal et sur d’éventuelles failles du système d’exploitation et vulnérabilités de configuration. Ce diagnostic est réalisé via une collecte d’événements de sécurité qui ne sont pas personnellement identifiables. Aucune donnée personnelle n’est collectée par le Milistore.

Le Milistore s’appuie sur la technologie Pradeo Security, développée par Pradeo, l’éditeur français de solutions de cybersécurité spécialisé dans la sécurité des terminaux et applications mobiles. Cette technologie met en pratique les principes de l’intelligence artificielle pour détecter avec précision les menaces opérant sur les smartphones et tablettes, même dans un contexte d’exécution restreint tel que sur des appareils personnels.

Le processus d’analyse breveté de Pradeo utilise des algorithmes avancés issus de la Théorie des Graphes afin de modéliser les relations entre les éléments de sécurité et lancer le processus de détection.

La détection des menaces est réalisée par le moteur pilotant son analyse via de l’intelligence artificielle. Il effectue une analyse multidimensionnelle et passe les éléments de sécurité au crible de ses règles de détection. La base de règles est constamment autoenrichie par les nouveaux contextes à risque détectés par le moteur et par l'équipe de recherche de Pradeo. La précision du processus de détection de Pradeo provient de l’intelligence artificielle, élément fondamental du moteur affiné au fil des ans par l’analyse de milliards d’événements de sécurité.

2.3.3.1. Détection des menaces provenant des applications

Afin de prévenir les risques de fuite et de vol de données provenant des applications mobiles, Milistore évalue la sécurité de toutes les applications installées sur les appareils de ses utilisateurs. Cette évaluation repose sur une analyse approfondie qui vise à identifier les comportements potentiellement dangereux des applications.

Il est important de noter que de nombreux logiciels malveillants ne sont plus identifiables par des signatures virales classiques. C'est pourquoi l'analyse réalisée par le moteur de Pradeo ne se limite pas à la simple vérification de signatures virales. Elle va plus loin en recherchant des comportements ou des combinaisons de comportements suspects, pour détecter également les logiciels malveillants dits *"zero-days"* qui n'ont pas encore été répertoriés dans les bases virales mais sont tout autant voire plus dangereux que les malware connus, car plus sophistiqués.

Par ailleurs, l'analyse mise en œuvre est capable de repérer les traitements de données programmés pour être effectués par les applications mobiles, avant qu'ils ne soient concrètement réalisés. Elle apporte des précisions quant aux types de :

- Données manipulées : personnelles (géolocalisation, contacts, courriels…), à propos de l'appareil (réseau utilisé, modèle et version de l'appareil…) et présentes dans les applications.
- Traitements effectués :
    - In use : L'information est accédée par l'application.
    - At rest : L'information est stockée par l'application dans le système de fichier, dans une base de données locale, les ressources partagées, les logs, le presse-papier…
    - In transit : L'information est envoyée hors de l'appareil via internet ou le réseau cellulaire.

Cette mesure proactive est un atout dans la lutte contre les exfiltrations de données provenant d'applications récréatives populaires, telles que les réseaux sociaux, les programmes de tracking d'activité physique, etc…

L'outil Milistore offre à ses utilisateurs des rapports détaillés sur les comportements des applications qu'ils possèdent. Ces rapports permettent d'identifier clairement les applications qui entrent en conflit avec la politique de sécurité de l'armée de Terre.

2.3.3.2. Détection des menaces provenant du réseau

Les appareils mobiles sont sujets à diverses formes d'attaques provenant des multiples réseaux auxquels ils se connectent. Qu'il s'agisse du WiFi, des antennes relais, du Bluetooth ou encore de la technologie NFC, chaque canal de communication représente une opportunité pour les cybercriminels d'exploiter des vulnérabilités et de compromettre la sécurité des appareils et des données des utilisateurs et de leur organisation.

Face à cette menace omniprésente, Milistore se positionne en tant que rempart protecteur en mettant en œuvre des mesures de détection des risques et attaques provenant des réseaux. Un aspect de cette approche réside dans la surveillance en temps réel de la configuration des paramètres réseau. Bien que souvent sous-estimée, une configuration trop permissive, qui autorise par exemple une connexion automatique à des WiFi publics ou laisse le Bluetooth activé en permanence, peut facilement être exploitée par des attaquants.

D'autre part, Milistore va au-delà de la simple surveillance des paramètres en établissant un contrôle des connexions. Cela signifie que chaque fois qu'un appareil mobile se connecte à un réseau WiFi ou à une antenne relais, l'application examine minutieusement les paramètres associés. En détectant les éventuelles anomalies, l'outil identifie les connexions potentiellement malveillantes et prévient les attaques de type Man-In-The-Middle qui interceptent les informations transitant via le réseau.

2.3.3.3. Détection des menaces provenant du système

L'application Milistore effectue un contrôle de la sécurité du système d'exploitation des appareils mobiles sur lesquels elle est installée, afin de l'empêcher de s'exécuter dans des environnements hostiles et vulnérables aux attaques.

Elle assure notamment la détection des :

- Altérations du système, telles que le *root* d'un mobile Android ou le *jailbreak* d'un mobile iOS, réalisées par les utilisateurs pour augmenter leurs droits sur l'appareil, mais qui permettent également aux cybercriminels de bénéficier d'accès privilégiés.
- Configurations à risque, comme l'activation des options d'accessibilité, l'autorisation des applications mobiles depuis des store non officiels, qui peuvent entrainer des vols de données ou des fraudes.
- Systèmes fonctionnant sous des versions obsolètes et dont les vulnérabilités ont été rendues publiques, constituant ainsi des cibles faciles pour les attaquants.

2.3.4. Réponses de sécurité

Le caractère personnel des terminaux protégés par le Milistore et le besoin de favoriser l'adoption de l'outil par le plus grand nombre a influencé la manière dont il remédie les menaces. Techniquement, Milistore pourrait s'appuyer sur une technologie Mobile Threat Defense de Pradeo pour automatiquement remédier les menaces, comme bloquer les applications non conformes ou encore empêcher les connexions aux réseaux publics. Mais lorsque déclenchées lors d'usages personnels, ces réponses de sécurité sont perçues comme trop intrusives et limitatives. Si mises en œuvre, l'attrait pour l'application s'en verrait amoindri alors que l'adhésion des militaires est un prérequis du succès du projet et donc une priorité.

Ainsi, le choix a été fait de procéder de deux manières : Milistore assure une première réponse de sécurité automatique : l'accès conditionnel, puis la deuxième réponse est menée par l'utilisateur : la remédiation assistée des menaces.

D'une part, Milistore protège activement ses services professionnels en contrôlant la sécurité des appareils qui y accèdent. Lorsqu'un mobile a un niveau de sécurité inférieur au niveau défini comme conforme par la cellule transformation numérique, son utilisateur ne peut pas accéder aux ressources du Milistore. Cette mesure de sécurité proactive permet de protéger toutes les données disponibles dans le store et stockées ou transitant depuis et vers les applications privées de l'armée de Terre. Lorsqu'une menace est détectée lors du diagnostic de sécurité, l'application avertit l'utilisateur qu'elle bloque l'accès aux applications et ressources professionnelles jusqu'à disparation de la menace. Les applications et usages personnels ne sont jamais restreints.

D'autre part, l'utilisateur est informé en temps réel via des notifications et au sein du Milistore des vulnérabilités et/ou tentatives d'attaques en cours sur son appareil. Une vue agrégée lui permet en un coup d'œil de voir le vecteur de la menace, à savoir une application, le réseau ou l'OS. Le parcours utilisateur le guide ensuite dans la compréhension rapide du problème et surtout, indique comment le remédier immédiatement.

Outre la sécurité assurée par des actions directes, Milistore sensibilise aux cybermenaces qui visent les mobiles tout en favorisant une culture de la sécurité. Compte tenu de l'évolution rapide des technologies et des cybermenaces, la sensibilisation régulière est essentielle pour que les militaires restent au fait des dernières tactiques utilisées par les cybercriminels. Cela leur permet de s'adapter et de renforcer constamment leurs pratiques, en créant un environnement où la cybersécurité devient une priorité naturelle.

2.3.5. Lancement et constats

Déployé en 2019, le Milistore a trouvé sa place parmi les rangs de plus de 10 000 militaires, 80% sur Android et 20% sur iOS.

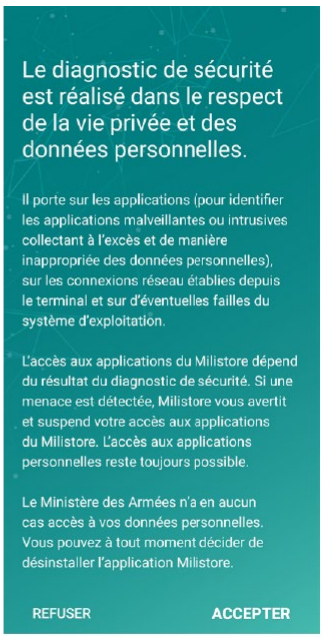
Une étape majeure du lancement a été l'inauguration officielle, orchestrée par le Major général de l'armée de Terre, ambassadeur du Milistore. Cet événement s'est tenu au cœur du régiment pilote, qui a été le premier à bénéficier de l'outil.

Le déploiement du Milistore a été méthodiquement planifié et déployé, se propageant progressivement de régiment en régiment. Afin d'augmenter son adoption, l'armée de Terre a proposé la mise à disposition d'applications privées et publiques et des liens vers des services spécifiques au sein de l'application.

Cependant, les débuts ont été marqué par une certaine hésitation de la part de l'audience cible, principalement en raison d'autorisations demandées par le Milistore à ses utilisateurs. En effet, pour assurer la détection des menaces, en 2019, le Milistore s'appuyait par exemple sur un accès en local au journal d'appels et à la liste de contacts. Même si ces données n'étaient en aucun cas collectées, les utilisateurs n'acceptaient pas ou peu d'accorder ces accès au Milistore.

Pour dissiper ces inquiétudes, l'armée a adopté une approche proactive en organisant des sessions d'éclaircissement. De plus, des efforts de communication interne ont été déployés, renforçant ainsi la compréhension des enjeux et des avantages offerts par la plateforme.

Au fil des années, les travaux de recherche et développement opérés sur la technologie de Pradeo lui permettent aujourd'hui de protéger les mobiles sans nécessiter ces accès perçus comme intrusifs : l'adoption du Milistore en est grandement facilitée. Une stratégie de transparence a également été mise en place grâce à la création d'un guide interactif qui s'affiche lors de l'ouverture de l'application, démystifiant ainsi son fonctionnement.



Il est intéressant de noter que les autorités hiérarchiques ont manifesté une sensibilité accrue envers les questions de cybersécurité. Cette prise de conscience a contribué à accélérer l'adoption au sein de cette cible.

Aujourd'hui, le Milistore, autrefois restreint à un usage limité, est devenu accessible à l'ensemble des membres de l'armée de Terre, y compris les soldats de réserve qui bénéficient également de ses avantages. Il est prévu d'étendre l'accès aux autres armées, directions et services dont les professionnels civils du MINARM. Cette évolution incarne une transition audacieuse vers une utilisation plus large des technologies numérique et cyber au sein de l'armée.

Conclusion et ouverture

Milistore fût le premier store privé sécurisé développé par Pradeo, et ce pour le compte de l'armée de Terre. Depuis son lancement, Pradeo commercialise la solution pour des administrations et entreprises d'autres secteurs, en marque blanche.

Les fonctions remplies par le store privé sécurisé sont souvent recherchées par les administrations publiques, qui ont des budgets restreints mais un fort besoin de digitalisation, et par des entreprises qui ont beaucoup d'applications mobiles qui manipulent des données sensibles, auquel cas le store leur permet de les déployer simultanément tout en les sécurisant.

Plus globalement, la technologie de détection et réponse des menaces mobiles derrière le Milistore est désormais largement utilisée via une solution de protection de flotte mobile qui répond aux besoins de sécurisation des terminaux mobiles managés. Par ailleurs, elle est intégrée via des API (Application Programming Interface) et un SDK mobile (Software Development Kit) dans des solutions informatiques offrant :

- Des outils complémentaires à la sécurité mobile (Antivirus, EDR, Mobile Device Management),
- Une cybersécurité étendue à plusieurs types de terminaux (PC et mobile),
- Une cybersécurité étendue à l'ensemble du système d'information (eXtended Detection and Response)