ZIMPERIUM®

Indice du rapport mondial sur les menaces mobiles en 2022

With contributions by:

intertrust

Ping Identity

SentinelOne

Sommaire

La sécurité mobile à l'heure actuelle

Shridhar Mittal, PDG, Zimperium

Vous savez comme moi que ces dernières années ont complétement révolutionné la main-d'œuvre moderne, comme personne n'aurait pu l'imaginer il y a dix ans. Les forces distribuées et hybrides, les appareils toujours connectés, la connectivité 5G à haut débit et l'augmentation de l'accès aux données critiques depuis des sites distants se sont répandus dans les entreprises à travers le monde. Je n'ai pas non plus besoin de vous rappeler que l'année 2022 sera très différente de 2021 ou encore 2020. Comme nous le savons tous, en ce moment, on en est à des années-lumière de ce à quoi le travail, la collaboration et la productivité ressemblaient avant et jusqu'à la fin de l'année 2019.

Pendant des décennies, les équipes chargées de l'informatique et de la sécurité ont mis en place une infrastructure dite « on-premise » (ou encore « sur site ») afin d'aider les employés sur place, et quelques rares personnes ont dépassé les murs du bureau. La sécurité et les services ont été mis en œuvre afin de développer une forteresse numérique composée de plusieurs couches dans le but de protéger les employés, les terminaux et les données. Mais les services hors site traditionnels, comme les VPN, n'ont pas été conçus pour gérer cette vague de connexions externes vers l'entreprise. Une fois que la plupart des employés sont passés au-delà des protections physiques et numériques, et que les outils de productivité installés localement sont passés à des modèles de logiciels en tant que service (SaaS), les organismes de sécurité ont commencé à investir dans des contrôles de sécurité avancés pour les terminaux et l'infrastructure qu'ils prenaient en charge.

Heureusement, plusieurs entreprises ont montré la motivation et la mentalité nécessaires pour permettre une collaboration à distance sécurisée avant même l'apparition de COVID-19, alors que les entreprises mondiales poursuivaient des initiatives de mobilité, d'accès à distance, de confiance zéro et de productivité. Les entreprises ont commencé à investir dans les services et les applications en nuage, en déplaçant les données depuis les serveurs de stockage sur site vers des solutions évolutives dans le monde entier. Puisque certaines bases étaient déjà posées, la pandémie mondiale a davantage servi de validation et de catalyseur que de perturbateur pour leurs activités. Dans ce cadre, la souplesse, l'évolutivité et l'accessibilité étaient une priorité pour ces nouveaux investissements. Mais qu'en est-il de la sécurité ?

En dépit de leurs efforts, la réalité est que le lieu de travail a évolué beaucoup plus rapidement que ce que plusieurs équipes et stratégies avaient prévu. **Durant les deux dernières années précisément, plusieurs organismes ont sacrifié la sécurité dans le but de soutenir la productivité et d'assurer la continuité de leurs activités.** Il va sans dire que les organismes spécialisés dans la technologie de l'information et de la sécurité ont toujours investi massivement dans la sécurité des points d'extrémité, mais ont historiquement sous-estimé les impacts potentiels de la démarcation floue entre les points d'extrémité mobiles et traditionnels.

Selon nos données, 66 % des organismes interrogés ont récemment mis en place des programmes BYOD ou « bring your own device » (PAP pour « prenez vos appareils personnels » ou AVEC pour « apportez votre équipement personnel de communication ») actifs, et 11 % envisagent de mettre en œuvre cette politique au cours de l'année prochaine.[1]

Aujourd'hui plus que jamais, les dispositifs gérés et non gérés se connectent aux données de l'entreprise via des réseaux inconnus et non gérés. Les équipes de sécurité doivent obligatoirement aborder chaque point d'extrémité avec une toute nouvelle approche. Tout commence par la vérification de tous les appareils connectés aux systèmes de l'entreprise, qu'ils soient gérés ou non. Le cas échéant, les équipes chargées de la sécurité perdent de vue ces menaces et ces risques introduits chaque jour sans même pouvoir attribuer les données ou encore attester les appareils. Les organismes doivent dépasser les outils de gestion des dispositifs et des applications mobiles et s'attaquer aux plus grands problèmes de sécurité posés par les dispositifs mobiles.

Selon les données disponibles, 10 % des applications installées sur le terminal mobile BYO moyen sont centrées sur l'entreprise, qu'il s'agisse de l'authentification multifactorielle (MFA), des outils d'accès aux données ou des communications.[2]

Tandis que les entreprises évoluent, elles introduisent également davantage d'applications connectées à des systèmes de données critiques pour mieux soutenir leurs effectifs devenus mondiaux, ce qui signifie que ces nouveaux risques dépassent le dispositif mobile lui-même. **La surface d'attaque des entreprises s'élargit avec chaque nouvelle application adoptée et déployée pour soutenir la productivité.** Après tout, chacune de ces applications présente un ensemble unique de risques pour un environnement, qu'il s'agisse d'un code mal configuré, d'API exposées ou de connexions en nuage non protégées permettant de découvrir les données des clients.

Lors de la pandémie mondiale, la connectivité mobile a été d'une grande aide, permettant à un grand nombre d'entreprises de se maintenir à flot. Qu'il s'agisse d'entreprises mondiales alimentées par des travailleurs intellectuels accédant aux données de l'entreprise depuis leurs dispositifs personnels ou de petits restaurants s'appuyant sur les codes QR des menus, les commandes en ligne et les paiements sans contact, la connectivité mobile a offert au monde la possibilité de rester connecté dans des moments où le confinement était une étape indispensable pour atténuer la pandémie. Et il n'est pas possible de « sortir un lapin de son chapeau ». Ce niveau de connectivité mobile restera l'attente des travailleurs, des clients, des électeurs, des utilisateurs et des entreprises pour les prochaines décennies. Il est maintenant temps de trouver un moyen efficace de sécuriser ces connexions afin de pouvoir continuer à les rendre possibles.

La bonne méthode d'utilisation du rapport de cette année

Pour toutes ces raisons, et plus précisément en ce moment de l'histoire, nous avons voulu permettre de mieux apprécier le rôle que jouent les menaces mobiles sur les dispositifs et les applications dans le paysage global des menaces de cybersécurité.

Notre rapport 2022 sur les menaces mobiles mondiales a pour but de collecter, d'organiser et de fournir des informations qui permettent aux entreprises et aux organismes mondiaux de prendre des mesures éclairées et décisives pour sécuriser leurs données. Nous avons exploité nos données pour en dégager du sens à partir de différentes perspectives, dont la sollicitation de personnes extérieures à notre organisme, afin de vous permettre de voir le paysage des menaces mobiles sous plusieurs angles.

- **Dans le présent rapport, nous nous penchons tout d'abord sur la surface d'attaque mobile, en examinant une année de données sur les menaces mobiles, et en nous concentrant plus précisément sur les tendances des menaces liées aux dispositifs et aux applications mobiles.**
- **Ensuite, nous examinerons l'impact des menaces mobiles et d'une bonne stratégie de sécurité mobile moderne sur l'écosystème de sécurité, avec la participation de notre réseau de partenaires, notamment SentinelOne, Ping Identity et Intertrust.**
- **Nous présentons ensuite un récapitulatif et une analyse thématique des données concernant les menaces mobiles provenant du terrain, notamment les principaux vecteurs d'attaque mobiles, les analyses régionales, les vulnérabilités mobiles exploitées, les tendances en matière de phishing mobile et de logiciels malveillants mobiles.**

Nous espérons vivement que ces informations et ces perspectives influenceront directement la stratégie et les investissements de votre organisme pendant l'année à venir, alors que nous faisons tous notre part pour promouvoir un monde plus sécurisé et de plus en plus connecté.

La sécurité mobile et la vaste stratégie de sécurité de l'entreprise

Jon Paterson, directeur des nouvelles technologies, Zimperium

Depuis quelques années, des outils de sécurité comme XDR et SOAR sont apparus pour améliorer la sécurité traditionnelle face à l'avancée des menaces. Les outils de gestion des identités et des accès (IAM) se sont développés pour prendre en charge l'accès à distance à grande échelle, et **36 % des entreprises interrogées donnent la priorité à l'investissement dans des architectures de confiance zéro au cours de l'année prochaine.**[3] Ces couches de sécurité avancées permettent à chaque entreprise de se développer efficacement en dehors de ses murs, de s'intégrer dans les flux de gestion de l'identité des effets et d'établir un périmètre unique autour des appareils et des applications connectés via la myriade de réseaux.

Mais tous ces investissements en matière de sécurité tombent en poussière sans l'inclusion de la téléphonie mobile. Qu'il s'agisse de la protection des points terminaux modernes et mobiles, de l'attestation des dispositifs ou de la sécurisation des applications d'entreprise tout au long du cycle de développement, les entreprises ont besoin que leur sécurité évolue avec leurs données, leurs accès, leurs employés et leurs clients.

L'intégration de la sécurité des terminaux et des applications modernes et mobiles dans l'esprit des entreprises n'est pas la dernière étape mais le début de ce qui est à venir.

L'intégration des appareils dans notre quotidien ouvre la voie à la convergence des terminaux modernes. Apple a déjà commencé à intégrer les services OSX et iOS sur toutes ses plateformes, et Windows 11 introduira bientôt la possibilité d'exécuter des applications Android en mode natif sur les ordinateurs de bureau. Le projet ChromeOS de Google brouille de plus en plus les frontières entre les postes de travail et les terminaux mobiles grâce à des applications, des extensions et des services partagés.

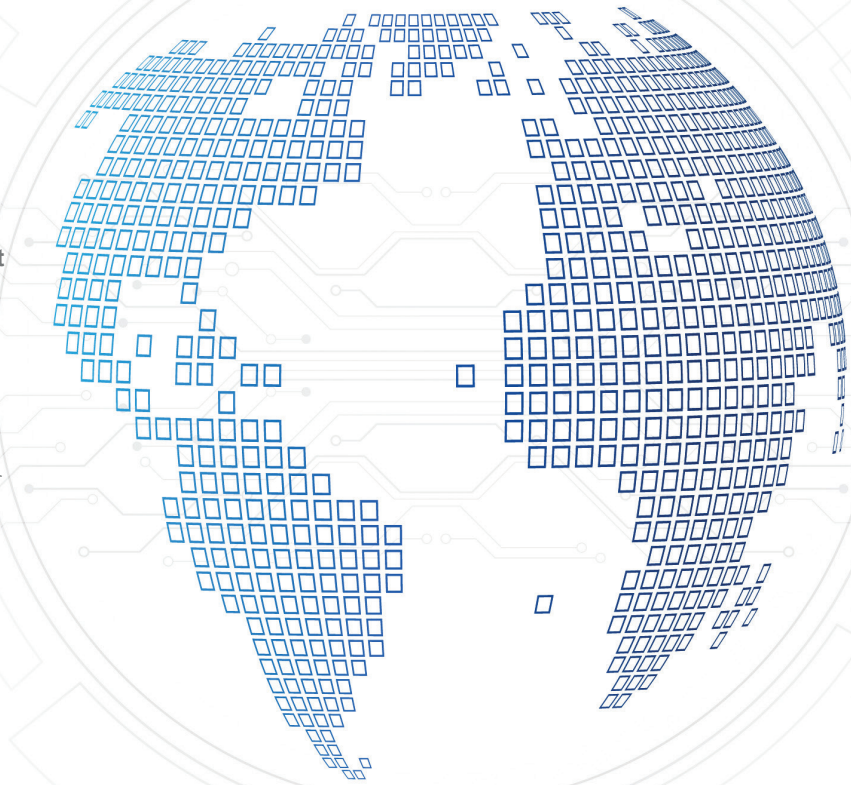
Quand nous envisageons de développer des applications pour les terminaux modernes, le fait de créer des applications sécurisées et conformes commence toujours par choisir une architecture et un cadre appropriés pour les dispositifs et les plateformes qui répondent aux besoins de votre entreprise. La sécurité dès la conception permet de prendre de bonnes décisions fondamentales concernant la protection du code, des données et des clés cryptographiques. Les mesures de sécurité devront prendre en considération la fragmentation du matériel et des logiciels. **En tant que gestionnaires de données, les entreprises doivent présumer que les applications fonctionneront, et fonctionnent, dans des environnements hostiles, ce qui fait de la visibilité et de la protection des données au repos, en cours d'utilisation et en transit une priorité.**

Les entreprises qui prennent une longueur d'avance en établissant des architectures de confiance zéro et en appliquant des principes de sécurité depuis la phase de développement d'applications seront prêtes pour cette prochaine évolution des points terminaux modernes. Les menaces et les risques peuvent passer d'un appareil à un autre, tout comme les données et les services légitimes, les vulnérabilités des systèmes critiques seront donc partagées également. Aussi récemment que septembre 2021, la première inclinaison d'une faille unique et multi-appareils (CVE-2021-30860) a été dévoilée dans le cadre de l'attaque du logiciel espion Pegasus, impactant iMessage sur les appareils iOS et OSX.

Et ce n'est qu'un début. Le fossé entre les terminaux mobiles et traditionnels va continuer à se combler et, avec lui, les mentalités en matière de sécurité devront être prêtes à fournir une visibilité, une attestation et un accès sécurisé aux entreprises depuis nos terminaux modernes.

Les plateformes de développement multi-expérience continueront à transformer la façon dont les applications sont conçues et construites, mais elles augmenteront considérablement le besoin de plateformes de sécurité complètes et intégrées.

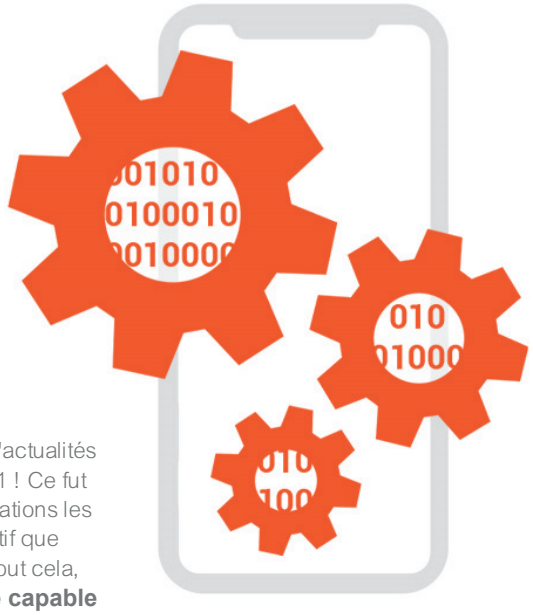
La surface d'attaque de l'entreprise, quant à elle, continuera de changer et d'évoluer, en raison des défis et des opportunités que représentent les surfaces d'attaque en constante évolution. Qu'il s'agisse de techniques parrainées par l'État, d'exploits des applications ou de menaces disponibles dans le marché, le secteur de la cybercriminalité ne cesse de croître et n'affiche aucun signe de rémission. **L'incidence sur l'entreprise n'est pas faible non plus, puisque le coût d'une violation de données en 2021 est passé de 3,86 millions à 4,24 millions de dollars.**[4]



Depuis plus d'une décennie, nous repoussons les limites de la sécurité des terminaux et des applications mobiles, en collaborant avec des partenaires avant-gardistes afin de garder une longueur d'avance sur les risques et les menaces qui pèsent sur la population active moderne. Personne n'aurait pu prédire l'incidence des trois dernières années sur le commerce mondial, mais Zimperium était prêt à s'adapter aux besoins mobiles des entreprises du monde entier.

Que vous désiriez comprendre les risques que les terminaux mobiles introduisent à l'environnement de votre entreprise ou que vous étudiiez les menaces qui s'infiltrent dans vos applications mobiles développées en interne, j'espère que le rapport 2022 sur les menaces mobiles mondiales vous fournira de nouvelles données et analyses sur l'état de la sécurité mobile.

Le rôle permanent de l'IA et de l'apprentissage automatique dans la sécurité mobile



Esteban Pellegrino, Directeur scientifique, Zimperium

Vers la fin de l'année 2019, une histoire incroyable a commencé à circuler sur divers sites d'actualités scientifiques, déclarant qu'un iPhone est plus puissant que l'ordinateur de bord d'Apollo 11 ! Ce fut une exploration passionnante de l'histoire de la puissance informatique de l'une des réalisations les plus incroyables de l'humanité, 50 ans plus tôt, et de sa comparaison avec le petit dispositif que nous glissons dans notre poche chaque jour. Sans entrer dans les détails techniques de tout cela, **on peut dire avec certitude que l'iPhone 11 de 2019 d'Apple aurait été plus que capable de traiter les données et d'alimenter les six alunissages en même temps. Et avec une puissance de traitement en réserve.**

Les capacités de ces dispositifs mobiles sont désormais souvent prises pour acquises par les utilisateurs, qui regardent le minuscule écran toujours connecté à un réseau, naviguent, explorent et calculent. Elles sont des fois même utilisées pour passer un appel. Mais de nos jours, le plus grand pourcentage d'appareils iPhone et Android qui dominent le marché des technologies mobiles est constitué des ordinateurs plutôt que des téléphones mobiles, connectés à des systèmes de données critiques, remplis de données personnelles et utilisés au quotidien dans le cadre du travail et de la vie privée.

Il y a 15 ans, le premier iPhone a été lancé et nous avons témoigné le développement du smartphone dans les entreprises par le biais de programmes gérés ou encore rudimentaires et non gérés. Ces petits ordinateurs de poche sont passés du statut d'accessoires grand public à celui d'outils professionnels, permettant aux employés de rester connectés à leur travail pendant leurs déplacements. Au départ, l'accès était basique, mais au fil des années, le dispositif mobile est passé du statut d'accessoire à celui de dispositif d'accès critique aux services, aux données et à l'identité, avec une importance pareille à l'accès à l'ordinateur portable fourni. Mais contrairement à l'ordinateur portable, les terminaux mobiles et les applications qu'ils exécutaient habituellement ne disposaient pas de la sécurité avancée nécessaire pour s'adapter au contexte actuel des menaces.

Il y a 10 ans, l'équipe qui a fondé Zimperium a remarqué ce manque d'outils de sécurité mobile avancée pour sécuriser les données et les accès. **Nous savions que nous devions comprendre les menaces qui dépassent les capacités humaines, détecter les tendances impossibles à voir même pour les experts et, surtout, tirer au maximum de l'expérience mobile toujours en évolution.**

En 2012, nous avons inventé et breveté[5 6] Zimperium z9, le moteur d'apprentissage automatique à mise à jour dynamique qui a fait de Zimperium le premier fournisseur de solutions de lutte contre les menaces mobiles (MTD), entièrement alimenté par l'intelligence artificielle sur les appareils.

Depuis une dizaine d'années, nous avons fourni la sécurité la plus avancée aux points terminaux et aux applications dans le monde entier, en conservant une longueur d'avance sur les menaces croissantes du marché mobile. **Notre mission est désormais d'unifier la sécurité des applications et des points terminaux par le biais d'une technologie unique, en réduisant au minimum la surface d'attaque des appareils mobiles et des applications qui y sont installées.** Notre objectif est de fournir la protection contre les vulnérabilités zero-day la plus avancée et la mieux adaptée aux entreprises, pour les terminaux et les applications mobiles pendant les deux phases de développement et d'exécution.

De nos jours, notre IA avancée protège les dispositifs contre les logiciels malveillants, les attaques par reconnaissance et par interception du trafic réseau, l'hameçonnage ou le phishing, l'altération, le débogage et l'exploitation malveillante des appareils et applications mobiles. Les terminaux et les applications exploitent notre technologie d'IA pour être prêts à agir lorsque de nouvelles menaces apparaissent dans l'environnement, et notre expérience continuera à assurer toute la sécurité nécessaire afin de rester à l'avant-garde de la menace.

Les dispositifs mobiles et traditionnels convergent, et les versions mobiles remplacent de plus en plus leurs équivalentes traditionnelles, puisqu'elles sont capables d'accéder de plus grands flux de données et de les traiter en dehors du bureau. L'avancée technologique de chaque nouvelle application s'accompagne de risques et de menaces inconnus à surmonter. Il est temps donc de s'y attaquer, de booster la confiance dans la sécurité mobile et d'être prêt à affronter tout ce que l'avenir nous réserve.

Nos dispositifs mobiles iront un jour sur la lune et bien au-delà, des dispositifs de communication libérés des murs mais reliant comme jamais les explorateurs du futur. Comme les scientifiques d'Apollo n'avaient pas pu prédire la puissance informatique des appareils de nos jours, nous ne savons pas quelle sera la prochaine avancée technologique, mais nous pouvons être certains que le mobile est là pour rester.

La gestion du risque mobile en 2022

Préface de Malcolm Harkins, responsable de la sécurité et de la confiance chez Epiphany Systems

> **« Le risque nous entoure et nous enveloppe. Sans le comprendre, nous risquons tout, et sans en tirer parti, nous perdons tout ».**

Cette citation est de Glynn Breakwell dans son livre « *The Psychology of Risk* » résume tout. J'ai constaté, vécu et contribué à promouvoir l'informatique mobile pendant des décennies, depuis l'époque où j'étais responsable de la sécurité et de la confidentialité chez Intel.

Quand le premier ordinateur portable véritablement mobile doté d'une connectivité sans fil omniprésente (plateforme Centrino) a vu le jour en mars 2003, mon équipe et moi-même l'avons autorisé. Lorsque l'iPhone a été lancé en 2007, nous l'avons autorisé, 50 000 appareils BYOD ont été donc créés immédiatement du jour au lendemain. Quand plusieurs applications d'entreprise sont devenues mobiles, nous les avons autorisées. Depuis le début de la mobilité, les appareils et les applications ont continué leur flambée, créant de nouvelles possibilités de croissance économique et d'avantages sociaux qui ont eu un impact positif sur les entreprises et les consommateurs.

Mais avons-nous vraiment compris les risques que nous avons pris et leurs conséquences possibles ? Dans certains organismes, la réponse est clairement affirmative, mais malheureusement, dans plusieurs autres organismes, la réponse est négative.

Par exemple, le rapport signale que plusieurs entités ont autorisé les iPhones et les appareils mobiles dans leur écosystème. Était-ce un risque calculé qui valait la peine d'être pris alors que la sécurité n'était pas instaurée pour ces canaux d'accès aux données ? Ou bien, la quête d'éventuels avantages a-t-elle provoqué une distorsion qui a non seulement éliminé le risque réel pour l'organisme, mais aussi créé un risque substantiel pour les personnes dont les données personnelles et financières sont désormais menacées ?

Zimperium a créé le rapport le plus détaillé sur les menaces mobiles publié à ce jour. Il contient un aperçu général des tendances en matière de menaces et de vulnérabilités ainsi que de l'impact qu'elles pourraient avoir sur la sécurité de nos organismes. Le rapport de l'enquête sur la perception des risques mondiaux menée par le Forum économique mondial en 2022 indique que « les cybermenaces croissantes dépassent la capacité de la société à les prévenir et à les gérer efficacement ». La surface d'attaque augmentera et changera toujours parallèlement à l'évolution de l'informatique, mais le fait de cerner l'ampleur de l'attaque dans le contexte de l'infrastructure de votre entreprise demeure la seule et unique solution afin de comprendre comment les applications et les dispositifs mobiles peuvent générer une exposition matérielle qui pourrait avoir un impact sur votre entreprise.

Dans le présent rapport, l'équipe de recherche sur les menaces avancées Zimperium zLabs partage des informations détaillées qui fournissent une vision complète dont les équipes de sécurité ont besoin pour comprendre le paysage des risques mobiles. L'une de ces tendances qui va redéfinir le paysage des risques, expliquée dans le rapport, est la convergence des systèmes, le flou des applications mobiles et des applications de bureau dans le système d'exploitation moderne. Cette tendance, en particulier, va « nous entourer et nous envelopper », et si des mesures d'atténuation appropriées ne sont pas mises en œuvre, nous allons « tout risquer ».

Voici une autre de mes citations préférées, cette fois d'Art Turock :

> **« Il y'a une différence entre l'intérêt et l'engagement. Lorsque quelque chose vous intéresse, vous vous y adonnez seulement lorsque cela vous convient. Lorsque vous vous engagez envers quelque chose, il n'y a pas d'excuses et seuls les résultats comptent ».**

Compte tenu des tendances, il est clair que nous avons tous sous-estimé les risques liés au mobile et à l'exposition qui en découle. Il y a bon nombre d'années, j'ai appris que deux types d'erreurs existent. Des erreurs que vous devez vivre avec et d'autres que vous pouvez résoudre. Quand je me suis trouvé face au deuxième type, je me suis considéré chanceux et je les ai corrigées. Tous nos investissements en matière de sécurité tombent à l'eau si on ne prend pas en compte les terminaux et les applications mobiles. Nous pouvons corriger les erreurs du passé en matière de sécurité de la mobilité et mieux nous positionner afin d'éviter les erreurs de risque dans le futur.

Le choix vous incombe et le moment est venu. Si vous ne décidez pas de vous engager à attaquer ces risques de front, il devrait être clair, d'après ce rapport, que c'est inévitablement le choix qu'il vous fera.

Aperçu des menaces mobiles en 2021

42 %

Reported mobile devices & web applications led to security incident

42 %

Reported unauthorized apps & resources accessing enterprise data

10 %

Reported unsecured applications due to lack of authentication or encryption

56 %

Rely on at least four to eight enterprise applications on their mobile device

17 %

Depend on more than eight work-specific apps on their mobile device

Les dispositifs mobiles ne sont pas seulement un accessoire de communication personnel—aujourd'hui, ils font partie intégrante du processus du travail au sein d'une entreprise. Grâce à des capacités et une connectivité élevées, les smartphones et les tablettes peuvent désormais accéder aux mêmes données et services que les dispositifs traditionnels, ainsi qu'à plusieurs nouveaux services professionnels basés sur le cloud. Pour soutenir à la fois la productivité des travailleurs à distance et la sécurité des actifs de l'entreprise, les points d'extrémité mobiles doivent être protégés de manière proactive et intelligente.

Les points d'extrémité traditionnels continuent toujours d'être utilisés, les équipes de sécurité doivent donc relever le défi d'obtenir la visibilité dont elles ont besoin sur l'utilisation et l'activité des dispositifs mobiles. Ce manque de visibilité rend très long et difficile pour les équipes de détecter les menaces et de prioriser les efforts correctifs. En plus, avec chaque nouveau point d'extrémité qui commence à accéder aux systèmes de l'entreprise, la surface d'attaque de l'organisation s'élargit, ce qui augmente le risque d'activité malveillante.

Dans le cadre d'une enquête récente, il a été demandé aux leaders du domaine technologique de soulever les cinq menaces qui ont eu l'impact le plus important sur leurs systèmes au cours des douze derniers mois. **42 % des personnes interrogées ont déclaré que les dispositifs mobiles et les applications web avaient provoqué un incident de sécurité.** Les terminaux mobiles ne sont pas les seuls à introduire des risques dans les systèmes d'entreprise : 42 % des personnes interrogées ont signalé des applications et des ressources non autorisées accédant aux données d'entreprise, et 10 % ont signalé des applications non sécurisées en raison du manque d'authentification ou de chiffrement.[7]

Il est aujourd'hui plus important (et plus difficile que jamais) de trouver un équilibre entre l'autorisation de l'accès mobile et la réduction de l'exposition de l'entreprise aux attaques. Si une entreprise mise sur les terminaux gérés qu'elle détienne ou si elle dispose d'un programme BYOD (Bring-your-own-device) actif, les terminaux et les applications mobiles l'exposeront à des risques accrus. 56 % des leaders du domaine technologique interrogés utilisent au moins quatre à huit applications d'entreprise pour leur productivité. **17 % des leaders du domaine technologique interrogés dépendent de plus de huit applications professionnelles sur leur dispositif mobile.**[8] Même si ces applications varient entre les services assurés par les fournisseurs et les outils développés en interne, l'efficacité de ces deux catégories repose sur l'accès aux systèmes de données de l'entreprise.

Les attaques contre les dispositifs et les applications mobiles ont eu un impact négatif sur les systèmes, la vie privée, les données des clients, etc. Puisque ces dispositifs traitent et accèdent à des données critiques comme les mots de passe, les applications d'authentification multifactorielle, les fichiers ou encore les communications de l'entreprise, il n'est donc guère surprenant que les menaces aient augmenté au cours des dernières années - et que les acteurs malveillants continuent encore d'investir dans le ciblage de ces dispositifs et applications avec des des niveaux de complexité croissants.

Avant l'apparition de la pandémie de COVID-19, 60 % des organismes n'avaient pas de politique BYOD implémentée.[9] Au cours des deux dernières années, de nombreuses équipes sont intervenus de façon rapide et héroïque pour soutenir les travailleurs à distance. Mais l'augmentation de l'introduction de politiques BYOD qui en résulte continue de brouiller les lignes de démarcation entre les dispositifs et les données, et entre les menaces des consommateurs et celles des entreprises. En outre, il est important de savoir que, tout comme les consommateurs, les employés se préoccupent de leur vie privée. En effet, les préoccupations des employés en matière de confiance et de confidentialité continuent de ralentir l'adoption de politiques de gestion des appareils dans les entreprises.

En analysant le paysage des menaces mobiles, 2021 fut l'année des grandes révélations et des rénitialisations de logiciels malveillants déjà découverts. Pegasus, le logiciel espion vendu aux gouvernements du monde entier, est réapparu dans l'actualité après les révélations d'une campagne visant 50 000 journalistes, militants des droits de l'homme, dirigeants politiques, etc. Initialement dévoilée par Amnesty International, la campagne de logiciels espions comportait des exploits de type « zero-day » visant les appareils iOS. L'onde de choc de cette découverte s'est poursuivie pendant des mois, à mesure que des informations supplémentaires sur les attaques et les victimes étaient révélées.

Initialement découvert en 2017, le cheval de Troie Joker est réapparu en 2021, ciblant les appareils Android dotés de fonctionnalités mises à jour. Ces chevaux de Troie sont des applications Android malveillantes connues pour frauder les factures et abonner les utilisateurs à des services premium. Comme pour les formes précédentes de ces attaques, les logiciels malveillantes de type cheval de Troie nouvellement découverts avaient le même objectif : le bénéfice financier. Les infections réussies d'appareils mobiles passent souvent inaperçues jusqu'à ce que l'argent ait disparu, n'offrant aucun recours aux victimes pour le récupérer.

Plus de 1 000 échantillons du logiciel malveillant Joker ont été découverts à la mi-2021, et ces variantes plus récentes comportaient de nouvelles techniques de contournement de la sécurité intégrées à leur code.

Qu'il s'agisse de l'exploitation des appareils, de la mauvaise configuration des applications, des logiciels malveillants ou de la fuite de données, les dispositifs mobiles sont devenus une meilleure cible pour les cybercriminels au niveau mondial. Les données 2021 de Zimperium prouvent qu'il n'y avait pas de pénurie de menaces dans les écosystèmes mobiles. Cela dit, grâce aux leçons tirées de l'année dernière, 2022 devrait être l'année dans laquelle les gens commenceront à aborder les dispositifs et les applications mobiles avec la même mentalité de sécurité avancée que les points terminaux traditionnels.

Points importants de la recherche des équipes zLabs de Zimperium en 2022

Les équipes de recherche avancée zLabs de Zimperium enquêtent constamment sur les menaces qui visent les dispositifs et les applications mobiles des utilisateurs du monde entier. En les comparant à celles des années passées, les données et la couverture médiatique des menaces mobiles ont augmenté en 2021, et l'accent a été mis davantage sur les vecteurs d'attaque iOS et Android. **En 2021, l'équipe zLabs de Zimperium a découvert de nombreuses menaces ayant un impact sur plus de 10 millions de dispositifs dans plus de 214 pays.**

Ci-dessous un résumé des découvertes les plus marquantes de l'équipe de recherche zLabs de Zimperium sur les menaces avancées :

Selon les experts, cette attaque active du cheval de Troie Android, que nous avons baptisée **GriftHorse**, est menée par le groupe menaçant depuis novembre 2020. Au début, ces applications malveillantes ont été distribuées via Google Play et des magasins d'applications tiers. Cette énorme action qu'on peut qualifier de « campagne » a ciblé les utilisateurs mobiles de plus de 70 pays. L'attaque GriftHorse est exceptionnellement polyvalente. Cette campagne pourrait changer la langue et le contenu affichés en fonction de l'adresse IP de l'utilisateur. Entre novembre 2020 et septembre 2021 (date de sa divulgation publique), GriftHorse a infecté plus de 10 millions d'appareils. Google a supprimé les applications malveillantes après leur déclaration par l'équipe zLabs de Zimperium.

Jusqu'à présent, l'équipe zLabs de Zimperium a identifié 23 applications ciblant des citoyens sud-coréens. Cette campagne de logiciels espions a infecté des milliers d'appareils des victimes. Ces applications Android malveillantes sont conçues pour espionner leurs victimes sans arrêt. Elles fonctionnent silencieusement en arrière-plan en mode incognito. Nous pensons que les acteurs malveillants responsables du malware espion **PhoneSpy** ont collecté d'importantes quantités de données personnelles et professionnelles concernant leurs victimes, notamment des communications et des photos personnelles. Après la divulgation publique, cette campagne a été désactivée, et le serveur de commande et de contrôle a été mis hors service. Les dispositifs infectés ne sont plus visés ni contrôlés par ces attaquants.

Selon les experts, cette attaque active du cheval de Troie Android, que nous avons baptisée **FlyTrap**, est menée par le groupe menaçant depuis novembre 2020. Cette campagne de détournement est en cours depuis mars 2021. Au début, ces applications malveillantes ont été distribuées via Google Play et des magasins d'applications tiers. Les auteurs des menaces profitent du fait que les utilisateurs pensent souvent, à tort, que se connecter au bon domaine est toujours sécurisé, quelle que soit l'application utilisée. Les domaines ciblés sont des plateformes de médias sociaux populaires, et cette campagne s'est avérée exceptionnellement efficace pour collecter les données des sessions de médias sociaux d'utilisateurs dans 144 pays. Ces comptes compromis peuvent être utilisés en tant que botnet pour plusieurs objectifs. Par exemple, ces auteurs peuvent augmenter la popularité de pages, de sites et de produits bien déterminés. De plus, ces comptes peuvent être utilisés pour diffuser des informations erronées ou de la propagande politique. Après avoir été signalées par l'équipe zLabs de Zimperium, Google a supprimé les applications malveillantes.

L'application « System Update » a été identifiée par l'équipe zLabs de Zimperium grâce au moteur de détection de logiciels malveillants z9, qui permet de localiser les dispositifs par zIPS. Après une enquête qui a été menée, les chercheurs ont déterminé qu'il s'agissait d'une campagne de logiciels espions sophistiqués aux capacités complexes. L'application mobile constitue une menace pour les appareils Android en agissant comme un cheval de Troie d'accès à distance (RAT). L'application reçoit et exécute des commandes qui permettent de collecter et d'exfiltrer une énorme quantité de données et d'effectuer une variété d'actions malveillantes. Dès qu'ils en ont le contrôle, les pirates peuvent enregistrer des appels audio et téléphoniques, prendre des photos, examiner l'historique du navigateur, accéder aux messages WhatsApp, etc.

Grâce à l'analyse effectuée par l'équipe zLabs de Zimperium, les experts ont découvert que 14 % des applications iOS et Android distribuées dans le monde entier présentaient plusieurs problèmes de configuration importants. Ces applications utilisaient le stockage en nuage avec des configurations non sécurisées. Ces mauvaises configurations ont exposé des informations personnellement identifiables (IPI), permis la fraude et exposé des adresses IP ou des systèmes et configurations internes. Des applications mal configurées ont été localisées dans presque toutes les catégories.

L'image ci-dessous montre la répartition des applications qui présentent des problèmes de stockage non sécurisé dans différentes catégories.

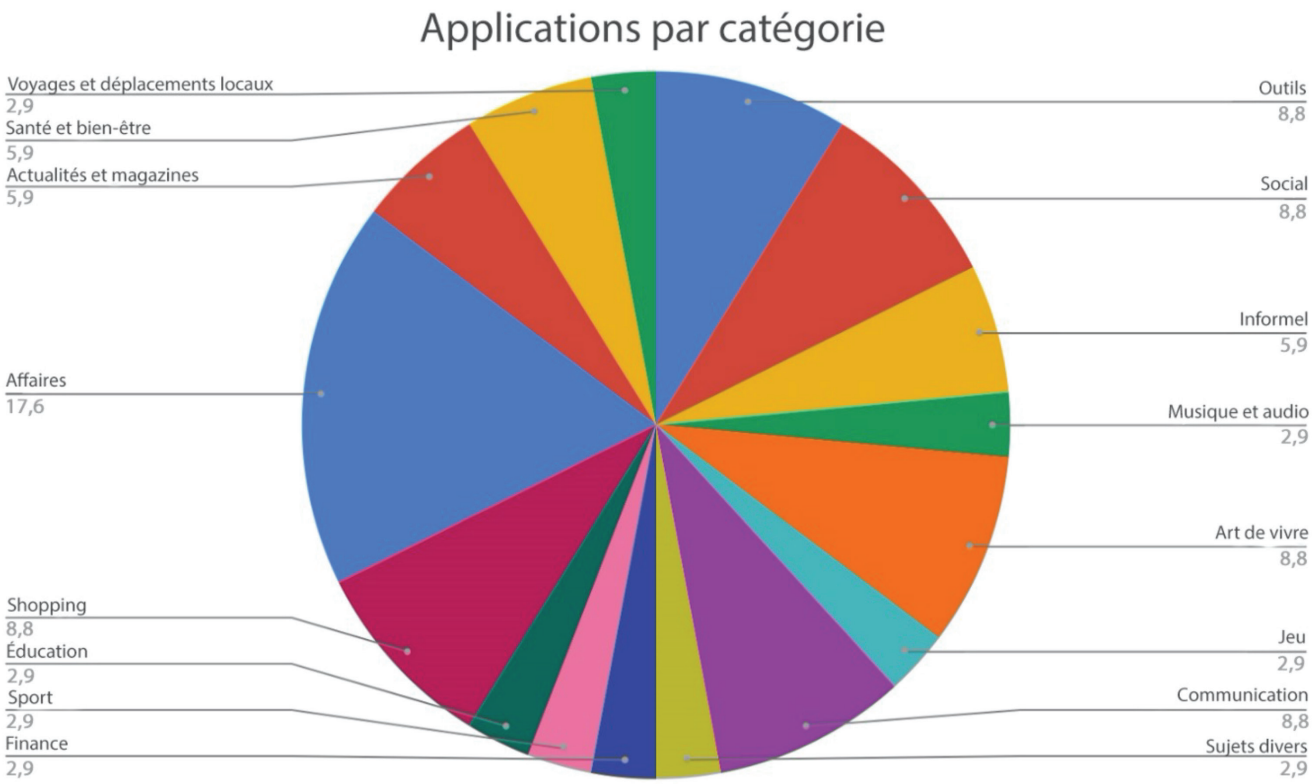


Figure # : Applications avec stockage en nuage non sécurisé, par catégorie.

Les 10 attaques qui ont fait des menaces mobiles les gros titres des journaux en 2021

Avec la montée en puissance des attaques sophistiquées, des vulnérabilités zero-day ou 0-day et des exploits notables, il n'est pas étonnant que la couverture médiatique de ces sujets ait été importante. Selon Cision, la base de données médiatiques, l'actualité de la sécurité d'iOS et d'Android a été largement couverte par des entreprises médiatiques mondiales.

Voici les dix menaces les plus fréquemment couvertes et des liens vers des exemples d'articles.

1 Apple iOS : iOS 14.4.2 - Vulnérabilité dans WebKit, le moteur de rendu web d'Apple

Couverture : Forbes, CNET, 9to5Mac, MacObserver, MacWorld, MacRumors, Appleosophy, TechGig, Laptop Mag

2 Android : GriftHorse (Zimperium divulgué)

Couverture : WIRED, PC Magazine, Forbes, ZDNet, CPO Magazine, Security Week, Threatpost, Security Affairs, The Record, SensorsTechForum, HackRead, Android Headlines, Android Authority, TechTimes, iTechPost

3 Apple iOS : iOS 14.8 - Faille dans les logiciels espions (Pegasus)

Couverture : Forbes, CNET, The Verge, ComputerWorld, TechRepublic, TechRadar, TechNadu, Macworld, Ubergizmo, Apple Insider, TechStory, MacRumors, PhoneScoop

4 Android : FlyTrap (Zimperium divulgué)

Couverture : Business Insider India, InfoSecurity Magazine, TechRepublic, PC Magazine, ZDNet, Threatpost, Bleeping Computer, Security Affairs, TechRadar, TechNadu, TechTimes, iTechPost

5 Android : Vulnérabilités affectant les pilotes de noyau pour les GPU Qualcomm et Mali

May 2021 - CVE-2021-1905 (Score NIST-CVSS : 7,8)
May 2021 - CVE-2021-1906 (Score NIST-CVSS : 5,5)
May 2021 - CVE-2021-28663 (Score NISTCVSS : 8,8)
May 2021 - CVE-2021-28664 (Score NIST-CVSS : 8,8)

Couverture : ArsTechnica, Security Week, Threatpost, Security Affairs, Bleeping Computer, The Record, IT Pro UK, TechNadu, Tom's Guide

6 Android : PhoneSpy (divulgation de Zimperium)

Couverture : TechCrunch, ZDNet, The Hacker News, Security Week, Threatpost, Bleeping Computer, Security Affairs, TechRadar, HackRead, Android Community, Android Headlines

7 Android : SharkBot

Couverture : SC Magazine, ZDNet, BankInfoSecurity, The Hacker News, Security Week, Security Affairs, The Record, TechTimes, The Digital Hacker

8 Apple iOS : 14.7 - Faille WifiDemon

Couverture : The Hacker News, Bleeping Computer, Threatpost, Security Week, The Record, Help Net Security, We Live Security, Security Affairs, HackRead, Tom's Guide, iPhone Hacks

9 Android : Vulnérabilité de Qualcomm

CVE-2020-11261 (Score NIST-CVSS : 7,8)

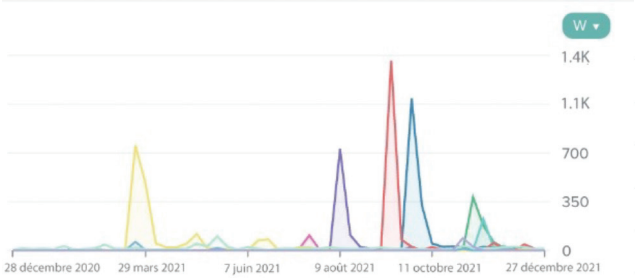
Couverture : Security Week, The Hacker News, Threatpost, Security Affairs, The Record, IT Pro UK, SensorsTechForum

10 Android : Vulnérabilité du noy au -

November 2021: CVE-2021-1048 (Score NIST-CVSS : 7,8)

Couverture : Security Week, Threatpost, Security Affairs, Bleeping Computer, We Live Security, 9to5 Google, SensorsTechForum

Total des mentions au fil du temps

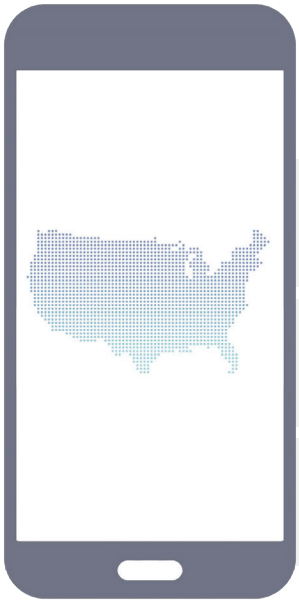


CHERCHER UN NOM	TOTAL DES MENTIONS
iOS 14.4.2	1.8K
GriftHorse	1.7K
iOS 14.8	1.7K
FlyTrap	999
CVEs May 2021	902

CHERCHER UN NOM	TOTAL DES MENTIONS
PhoneSpy	688
SharkBot	299
WifiDemon	131
CVE-2021-1048	126
CVE-2020-11261	119

Crédit : Cision

État de la sécurité des terminaux mobiles en 2022



Marché des dispositifs mobiles

Nos smartphones continuent de nous permettre d'innover, de nous divertir et de profiter d'une meilleure qualité de vie. Les achats de dispositifs mobiles continuent donc de croître. En 2020, près de 1,38 milliard de smartphones ont été vendus dans le monde. Aux États-Unis, on compte plus de 290 millions d'utilisateurs de smartphones. Le taux de pénétration a augmenté de manière constante d'année en année, pour atteindre 85 % en 2021.[11]

NOMBRE D'UTIL ISATEURS DE SMARTPHONES AUX ÉTATS-UNIS

294,15 millions

EXPÉDITIONS DE SMARTPHONES AUX ÉTATS-UNIS EN 2021

147,48 millions

VALEUR PRÉVUE DES VENTES DE SMARTPHONES AUX ÉTATS-UNIS EN 2021

73 milliards USD

Le marché américain des smartphones devrait atteindre 73 milliards de dollars, ce qui représente une augmentation considérable par rapport à 2010, où les revenus étaient de 18 milliards de dollars.[12] Sur le marché américain, Apple et Samsung sont les principaux fabricants de smartphones. Tous les deux, ils représentent 82 % des ventes.[13] Le marché des appareils mobiles continue de croître, tout comme les menaces mobiles.

Pour les équipes chargées de la sécurité, la triste réalité est qu'il suffit d'un seul mot de passe partagé, d'un seul employé induit en erreur, d'un seul dispositif compromis pour exposer l'entreprise à une violation catastrophique. Dans le contexte de la pandémie et de la croissance explosive correspondante du travail à distance et hybride, les menaces résultant des dispositifs mobiles se sont rapidement développées. Tout en combattant les attaques en constante évolution, les équipes de sécurité doivent protéger de plus en plus de points d'extrémité et de vecteurs d'attaque toujours plus nombreux.

BYOD Stats

Malgré la montée en puissance des menaces, les entreprises continuent d'appliquer des politiques de BYOD. Trop souvent, dans la course de la prise en charge des exigences du travail à distance, les équipes manquent d'implémenter les mécanismes de sécurité robustes indispensables pour protéger ces dispositifs.

Dans une enquête, nous avons constaté que 74 % des personnes interrogées ont indiqué avoir implémenté une politique BYOD. Cependant, dans une autre enquête, 30 % des personnes interrogées considéraient les dispositifs BYOD comme une priorité en matière de sécurité des terminaux au sein de leur organismes.[14]

Principales sources d'inquiétude en matière de sécurité des terminaux

35 % Bureau / Utilisateur distant

30 % BYOD

11 % Téléphones / dispositifs mobiles

Time to Patch

Dans les équipes décentralisées, les employés utilisent leur propre réseau et, dans certains cas, leurs dispositifs personnels pour effectuer leurs tâches. Ces pratiques introduisent un risque élevé dans une entreprise, élargissant ainsi la surface d'attaque et limitant la capacité de l'équipe de sécurité à détecter ou à remédier aux activités malveillantes. Tandis que les équipes luttent contre les risques et l'accès non autorisé aux données sensibles de l'entreprise, l'application des politiques BYOD et d'accès invité représente un défi majeur, comme cité par 42 % des personnes interrogées.[15]

Afin d'implémenter un correctif d'urgence ou de haute priorité, les équipes ont besoin de :[16]

moins de deux jours selon 42 % des personnes interrogées

trois à sept jours selon 28 % des personnes interrogées

une à deux semaines selon 20 % des personnes interrogées

En 2021, près de **50 %** des personnes interrogées ont déclaré que leur stratégie de travail à domicile était principalement à l'origine des incidents de cybersécurité.

Points terminaux mobiles : Un élément essentiel du paysage de la cybersécurité

Si les organismes ne sécurisent pas leurs terminaux mobiles, leur centre d'opérations de sécurité (Security Operations Center ou SOC) ne pourra pas établir un point de vue unique quant à leur stratégie de cybersécurité. Quand un employé utilise un dispositif mobile personnel pour envoyer un courriel, répondre à des SMS ou accéder à des applications sécurisées de l'entreprise, le SOC ne peut pas surveiller cette activité ni détecter les éventuels risques. Au lendemain de la croissance des stratégies BYOD et des scénarios de télétravail, les responsables doivent commencer à changer leur perception des dispositifs mobiles.

Près de la moitié des personnes interrogées à l'enquête (44 %) ont ajouté des politiques ou des exigences de sécurité à cause d'incidents de cybersécurité survenus au sein de leurs équipes décentralisées. Parmi ces personnes, 40 % ont modifié les procédures d'authentification des employés, alors que 34 % ont changé de fournisseur de solution de sécurité ou de prestataire de services.[17]

Microsoft Office est une cible de choix pour les cybercriminels Conformément à un rapport, **Microsoft Office est à l'origine de plus de 72 % des exploits, les navigateurs représentant 13 %.[18]**

Ces chiffres peuvent sembler troublants, mais près de la moitié des leaders technologiques pensent que les procédures actuelles sont suffisantes pour réagir aux incidents de type « zero-day ».[19] Or, en réalité, sans une défense intégrale contre les menaces mobiles, les points terminaux mobiles continueront à représenter un « trou noir » quand il s'agit de faire face aux incidents. 39 % de ces leaders comprennent que le temps de réaction est trop lent avec leurs procédures actuelles.[20]

48 %

des organismes révisent régulièrement leur stratégie de cybersécurité et l'adaptent en cas de besoin.

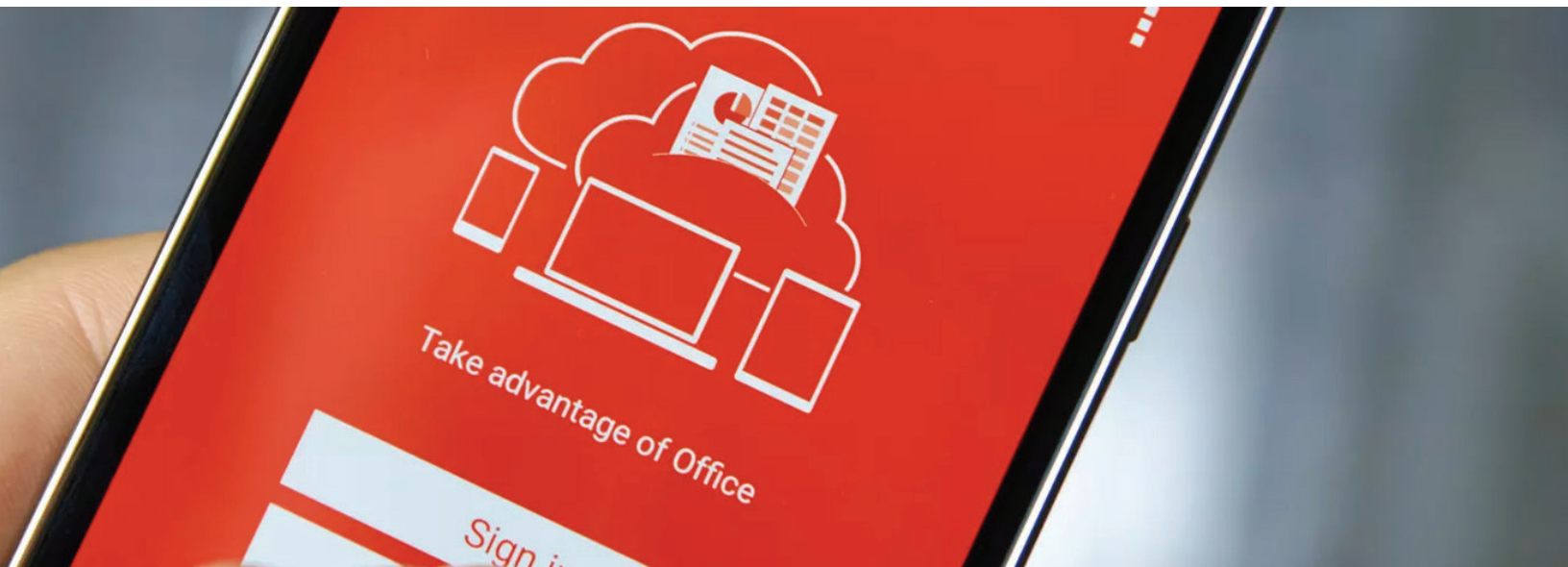
26 %

des organismes élaborent leur stratégie de cybersécurité en temps réel ou selon les besoins.

23 %

des organismes disposent d'une politique de sécurité bien structurée mais la révisent très rarement, voire n'ont aucune stratégie.

Figure # : La répartition de la stratégie de cybersécurité de l'entreprise[21]



Les dispositifs mobiles dans l'écosystème de l'entreprise

Les équipes informatiques et de sécurité continueront à subir une pression au fur et à mesure de la croissance des cyber-menaces, notamment lorsque les responsables de la sécurité informatique mettent en œuvre des politiques de cybersécurité plus strictes et que les employés expriment des préoccupations croissantes en matière de protection de leur vie privée. **Plus de la moitié (61 %) reconnaissent qu'il est presque impossible de définir et d'appliquer des politiques d'entreprise en matière de cybersécurité, puisque cette démarche supprime les frontières entre la vie personnelle et professionnelle.**[22] Si 46 % des personnes interrogées estiment qu'elles acceptent les dispositifs mobiles dans l'écosystème de l'entreprise, 34 % s'inquiètent quant à la protection de la vie privée.[23]

66 %

des smartphones au sein de l'entreprise appartiennent aux employés.[24]

29 %

des smartphones au sein de l'entreprise sont achetés par l'entreprise.

55 %

des tablettes au sein de l'entreprise appartiennent aux employés.[25]

39 %

des tablettes au sein de l'entreprise sont achetées par l'entreprise.

Figure # : La répartition des dispositifs mobiles dans les entreprises.

Le paysage des menaces mobiles dans l'entreprise

En 2021, Zimperium a analysé plusieurs menaces mobiles, notamment les logiciels malveillants, les accès non autorisés et les vulnérabilités par dispositif. Les attaques mobiles qui réussissent ont une incidence sur les résultats financiers et coûtent des millions de dollars aux entreprises. Ceci peut notamment causer la perte de confiance des consommateurs, des dépenses juridiques, des pénalités, des dommages à la réputation, le vol de données sensibles, etc.

Les menaces internes peuvent coûter le plus cher à détecter et à corriger. Alors que les dispositifs appartenant à l'entreprise ou encore BYO sont utilisés pour accéder aux données de l'entreprise, sans outils de sécurité contre les menaces mobiles, les services informatiques ont une vision très limitée de ces dispositifs mobiles et peuvent prendre plus de temps pour détecter des activités malveillantes, voire pas du tout. Selon les données de l'enquête, le département financier est le groupe qui représente la plus grande menace interne pour les entreprises en raison des données financières et d'entreprise sensibles que ces équipes traitent quotidiennement.[26] Ces statistiques expliquent pourquoi les PDG et les responsables des systèmes d'information doivent se concentrer sur cette question et augmenter les investissements dans la sécurité des terminaux.

En 2021, le financement par capital-risque de la cybersécurité a atteint le chiffre record de 11,5 milliards de dollars. Les personnes interrogées estiment que 43 % de leur financement sera consacré à la sécurité du cloud, 14 % au conseil en sécurité et 14 % à la gestion du risque et de la conformité. Durant la pandémie de COVID-19, les organismes ont obtenu le meilleur retour sur investissement grâce aux dépenses consacrées à la sécurité des points d'accès, suivies de près par les investissements dans la continuité des opérations et la planification de la reprise après sinistre.[27] En parallèle, 45 % des leaders technologiques déclarent que la sécurité des dispositifs mobiles reste la plus faible.[28]

Menaces affectant l'entreprise au cours des 12 derniers mois[29]

54 %
Logiciel malveillant (Virus, phishing, ransomware)

46 %
Vol d'identité ou de compte

42 %
Problèmes de sécurité des applications mobiles ou de Web

42 %
Accès non autorisé aux applications ou aux ressources

Marché de la sécurité mobile

Les investissements dans la détection et la réponse aux incidents pour les terminaux connaissent une forte croissance à cause de l'augmentation des cybermenaces qui touchent les dispositifs mobiles. Une grande part de cette croissance est due aux paiements mobiles et au besoin croissant de sécuriser les programmes BYOD dans l'entreprise.

L'Amérique du Nord détient la plus grande part d'investissement par rapport aux principales régions du marché mondial de la sécurité, avec 41,1 %.[30] Cependant, cela pourrait rapidement changer car plusieurs pays asiatiques, dont la Chine, Singapour et le Japon, ont investi massivement dans le développement de défenses nationales de cybersécurité, notamment en matière de sécurité mobile.

La défense contre les menaces mobiles ou Mobile Threat Defense (MTD) est une catégorie spéciale de technologie de sécurité mobile dont la part de marché augmente rapidement, car elle améliore la détection et la réponse sur les dispositifs mobiles. Les experts en sécurité ont défendu l'idée que la solution MTD doit au minimum être efficace contre les menaces mobiles modernes, car elle peut protéger contre les attaques au niveau des dispositifs, du réseau et des applications. En outre, MTD protège les utilisateurs finaux contre les attaques de phishing qui ciblent des vecteurs tels que les SMS, les applications de messagerie, les e-mails personnels et professionnels, alors que MDM (mobile device management ou « gestion de terminaux mobiles ») ne dispose pas de ces capacités.

MTD va bien au-delà de la gestion des paramètres et des codes d'accès et de la protection du réseau grâce à un réseau privé virtuel (VPN) intégré. Les capacités de détection alertent les administrateurs des bornes Wi-Fi malveillantes, analysent les risques de l'écosystème mobile et localisent les systèmes d'exploitation (OS) obsolètes, permettant ainsi aux équipes de lutter contre les activités malveillantes. Les informations sur les menaces provenant des dispositifs permettent à la solution MTD d'offrir la visibilité requise pour améliorer la détection et identifier les mouvements latéraux des attaquants. Ainsi, la solution MTD peut être intégrée à une infrastructure de sécurité unifiée des terminaux ou Unified Endpoint Security (UES) plus étendue. La solution MTD continuera à jouer un rôle très important dans la sécurité mobile et constituera un élément essentiel d'un système UES ou d'un système de détection et réponse étendues ou Extended detection and response (XDR), améliorant ainsi la stratégie de sécurité globale de n'importe quelle organisation.

État de la sécurité des applications mobiles en 2022

Pour une période relativement courte, notre utilisation des dispositions et des applications mobiles a évolué et s'est considérablement développée. Grâce à l'évolution des technologies mobiles et du cloud, les applications mobiles innovantes continuent de stimuler la transformation digitale des entreprises et d'éliminer les problèmes de notre vie quotidienne.

De nos jours, la portée du marché des applications mobiles est considérable. **Il y a eu plus de 218 milliards de téléchargements d'applications rien qu'en 2020.**[31] À l'horizon de 2023, le chiffre d'affaires annuel des applications mobiles devrait atteindre 935 milliards de dollars, des catégories comme le streaming vidéo, les jeux et les cours de fitness en ligne générant toutes des milliards de dollars de revenus.[32] Le segment des paiements représentait à lui seul 1,3 trillion de dollars à l'échelle mondiale en 2020.[33]

Tendances en matière de développement d'applications

Motivée par la rentabilité des applications, l'innovation dans le développement des applications mobiles s'est également accélérée. Voici quelques-unes des principales tendances en matière de développement d'applications qui modifient le paysage des applications mobiles :

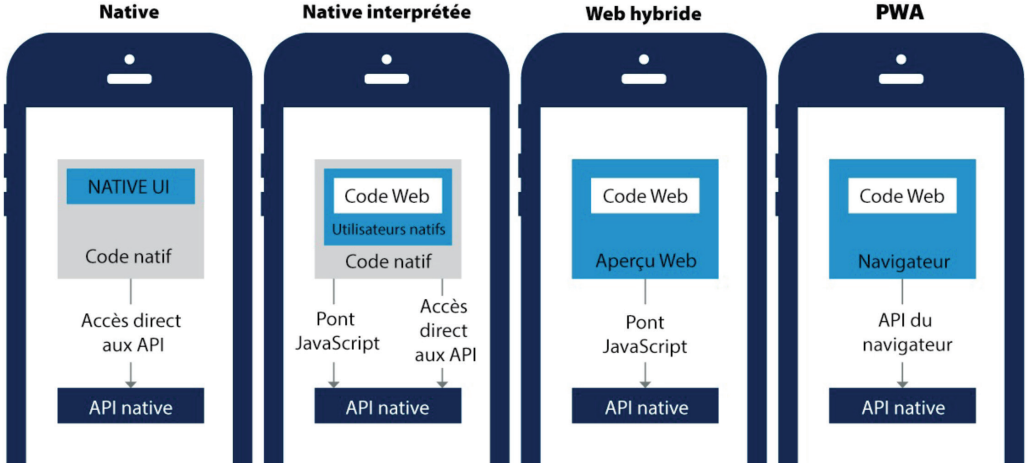
Développement d'applications mobiles multiplateformes

Grâce aux approches d'applications hybrides, les développeurs peuvent travailler avec une base de code unique qui peut fonctionner à la fois sur les plateformes Android et iOS, ce qui génère plusieurs avantages intéressants. Les développeurs peuvent choisir parmi une panoplie d'architectures d'applications mobiles modernes. Ces alternatives prennent en charge tous les types de dispositifs (dont les téléphones et les tablettes) et toutes les plateformes (dont Android et iOS). Ces approches hybrides offrent des avantages considérables en matière de portabilité, de maintenance et de distribution. Il n'est donc pas étonnant que la popularité des frameworks hybrides, comme React, Flutter, Uno, Kotlin et Xamarin, ait considérablement augmenté.

Les applications hybrides natives ou web contiennent toutes les deux une combinaison de code natif et web, mais à différents degrés. Les applications Web hybrides sont autonomes, à exécuter dans un navigateur Web standard. Dans les deux scénarios, le code web est plus difficile à sécuriser à cause du manque de fonctions de sécurité dans le contrôle du web et de l'absence des kits de développement logiciel (SDK) et des outils pour le code web.

Les applications Web progressives sont une évolution des applications Web classiques, ayant l'aspect et la convivialité des applications mobiles natives. Une base de code unique prend en charge plusieurs plates-formes à des fins de portabilité, mais rend exceptionnellement difficile la sécurisation des données et du code.

Profils d'architecture des applications mobiles

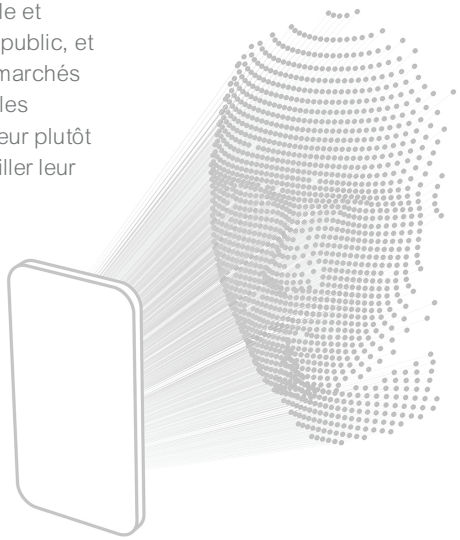


Plateformes de développement low-code / no-code (LCNC)

Si la migration vers des plates-formes de développement low-code / no-code (LCNC) est en cours depuis quelque temps, l'énorme pénurie de talents ayant frappé les organisations ces dernières années a permis d'accélérer considérablement cette transition. Eu égard à cette pénurie de personnel, le développement passera de plus en plus de la simple écriture de code à un effort d'assemblage et d'intégration de composants open-source ou propriétaires.

Expérience utilisateur mobile immersive et sans friction

Désormais, les percées en matière d'authentification sans mot de passe et d'intégration vocale continueront à rendre les interactions avec les applications mobiles plus fluides et immersives. Le marché mondial de la biométrie devrait dépasser 8,79 milliards de dollars à l'horizon de 2026.[34] La reconnaissance faciale et d'autres éléments biométriques sont devenus de plus en plus fréquents dans les applications grand public, et l'évolution permanente des protocoles Fast ID Online (FIDO) continuera d'alimenter l'expansion des marchés des applications mobiles des entreprises. L'intégration renforcée de la reconnaissance vocale dans les applications mobiles est incontournable, car il y a certaines choses plus simples pour le consommateur plutôt que de demander quelque chose. De cette façon, les utilisateurs ne seront plus obligés de déverrouiller leur téléphone des centaines de fois par jour.

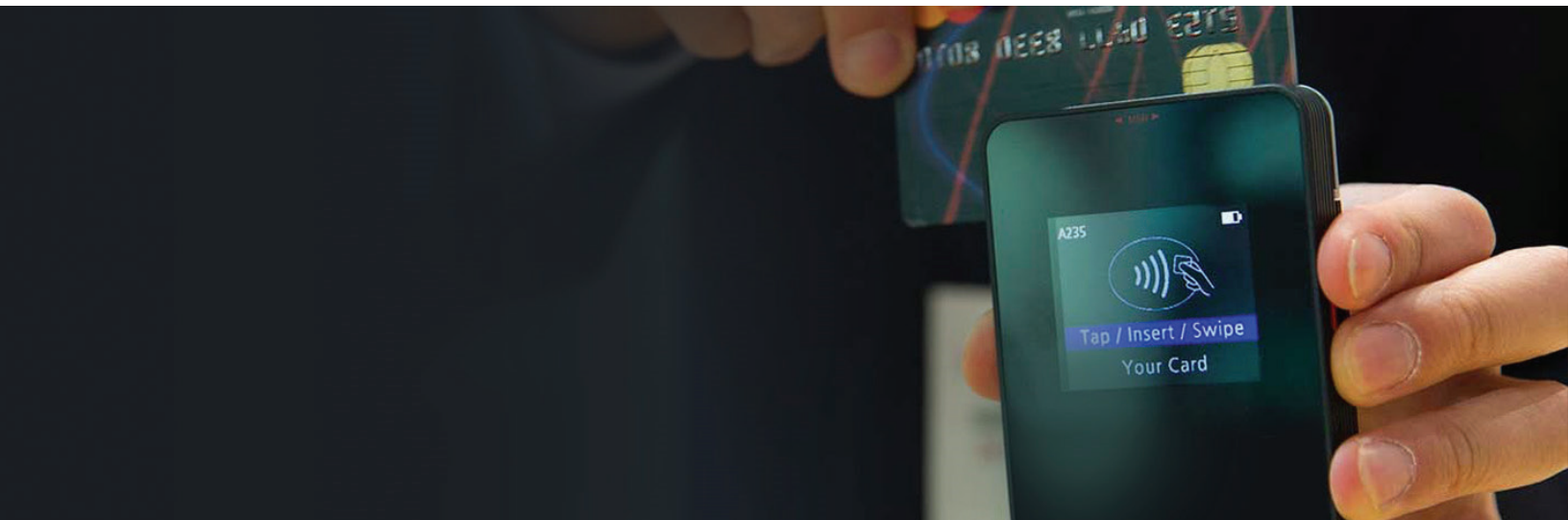


La technologie vocale devient de plus en plus accessible aux développeurs, et la sécurité devra être à l'avant des préoccupations à mesure que les progrès de l'IA, du traitement du langage naturel ou natural language processing (NLP) et de l'apprentissage automatique continuent. Mais les applications mobiles dotées d'interfaces vocales soulèvent plusieurs questions relatives à la confidentialité (l'application est-elle toujours à l'écoute ?) et à la sécurité (comment sauvegardez-vous en toute sécurité ce que j'ai dit ?). Le RGPD et les autres règlements sur la protection de la vie privée à l'échelon international devront évoluer avec cette tendance afin de pouvoir protéger les données vocales comme les autres données personnelles d'identification.

Les principales tendances technologiques ayant des répercussions sur la sécurité des applications mobiles

5G : Avec la prolifération de l'utilisation des dispositifs mobiles et de l'adoption du cloud, le volume de données sensibles partagées ne cesse d'augmenter. Désormais, les réseaux de communication 5G sont capables d'offrir des vitesses de transfert de données plus élevées avec une plus faible latence. **Vers la fin de 2024, il est prévu qu'il y aura 1,5 milliard d'abonnements mobiles 5G, et que la 5G gérera 25 % de tout le trafic de données mobiles.**[35] Cela signifie bien entendu qu'il y aura davantage de données sensibles partagées, transmises ou encore consultées, ce qui, à son tour, se traduit par davantage de données ciblées par les cybercriminels.

Paiements mobiles : Ces dernières années, les téléphones Android et iOS ont commencé à être utilisés en tant que terminaux de point de vente (PoS), ce qui a contribué à l'essor de l'adoption et de l'utilisation des paiements sans contact. Le chiffre d'affaires du marché des paiements mobiles a atteint 1,3 trillion de dollars en 2020 et devait atteindre 1,7 trillion de dollars en 2021.[36] Des technologies telles que NFC, Bluetooth et les codes QR permettront de plus en plus aux smartphones de remplacer les terminaux de paiement et les portefeuilles physiques.



Codes QR : La réapparition des codes QR pendant la pandémie nous a amenés à croire que leur utilisation est non seulement pratique, mais très sécurisée de par leur omniprésence. Plus que jamais, les codes QR transforment les produits et les emballages en produits intelligents. Selon une étude de Statista, **rien qu'aux États-Unis, le nombre de ménages qui auront scanné un code QR en 2020 est estimé à 11 millions.** En plus, cette adoption est visiblement plus importante en Asie, notamment en Chine et en Inde.

Mais cyber-criminels utilisent les codes QR en tant que vecteur d'attaque contre les entreprises et les particuliers. Aux États-Unis, le Federal Bureau of Investigations (FBI) a publié un message d'intérêt public qui avertit les utilisateurs de téléphones mobiles de la montée en puissance des escroqueries et des vecteurs d'attaque tirant parti de l'utilisation accrue des codes QR.[37] Les pirates falsifient ou concoivent leurs propres codes QR afin de de voler les informations financières ou les données critiques d'une victime, et de compromettre l'appareil par des applications malveillantes.

Mobile Cloud Computing : Le cloud mobile fait référence aux données, applications et services basés sur le cloud et conçus spécifiquement pour être utilisés sur des dispositifs mobiles et autres appareils portables. En 2020, le marché du cloud mobile a atteint une valeur de 30,71 milliards de dollars, et il devrait atteindre 118,70 milliards de dollars d'ici fin 2026.[38] Dans ces applications, la communication entre les dispositifs mobiles et les services cloud est assurée par un réseau sans fil. Puisque nous ne pouvons pas nous fier à la stratégie de sécurité du dispositif mobile à tout moment, il est important de sécuriser les données, les clés et les connexions au cloud au sein de l'application.

Quelques motifs apparaissent lorsque l'on examine l'origine des violations critiques liées aux applications mobiles :

Vulnérabilités des applications. À maintes reprises, le code des développeurs d'applications mobiles expose les données des employés et des clients, compromettant ainsi la confidentialité et la sécurité. Parmi les exemples récents d'applications compromises, on peut citer l'application mobile utilisée par les clients des sonnettes de porte,[39] la version Android de l'application de communication professionnelle Slack[40] et l'application de paiement Klarna.[41]

Composants et développeurs tiers. Les développeurs d'applications mobiles s'appuient de plus en plus sur des composants et de fournisseurs de services tiers, ce qui entraîne un niveau de risque trop élevé. **En 2021, les données privées de 21 millions de clients de ParkMobile, une application mobile de stationnement, ont été exposées par un logiciel tiers utilisé par l'entreprise.** Les bibliothèques tierces continueront à dominer les applications mobiles, car elles simplifient le développement, accélèrent la mise sur le marché et permettent de réaliser des économies considérables. Mais ils représentent une arme à double tranchant. Ils agrandissent la surface d'attaque et créent des applications sur-privilégiées, deux caractéristiques que les cybercriminels recherchent dans les applications exploitables.

Des services cloud mal configurés. Une enquête portant sur 23 applications mobiles a révélé que les données de plus de 100 millions d'utilisateurs étaient exposées.[42] Le responsable ? Les développeurs n'ont pas bien configuré leurs services cloud tiers. **En fonction de notre analyse de plus de 1,3 million d'applications Android et iOS, nous avons constaté que 131 000 d'entre elles utilisaient des services du cloud public dans leur backend, et que 14 % de ces applications présentaient des erreurs de configuration, ce qui expose les données personnelles des utilisateurs.**[43]

> “Cyberspace is not a specific environment. In 2022, cyberspace has become a free fire zone with a multiplicity of actors. As the physical world and cyberspace have converged via smart phones; mobile malware, proximity attacks and application attacks are allowing for cybercriminals and spies to manifest in both your digital and physical life. From stealing your money; to turning on the microphone and camera specific to your location, to using your device to compromise your work network, cybercrime cartels have gone wireless. Security and safety are dependent on mobile security."
>
> **Tom Kellermann**
> *Head of Cybersecurity Strategy for VMware and Global Fellow for Cyber Policy at the Wilson Center*

Répartition de la menace mondiale par région

Généralement, on ne peut pas nier que les terminaux mobiles sont exposés à des menaces accrues, mettant en danger les données et les services des entreprises. Plusieurs observations ressortent des clients de ces entreprises et les données relatives au risque sont rapportées par les appareils Android et iOS sécurisés par Zimperium au niveau mondial. Il est à noter que les données représentées dans les présents graphiques contiennent toutes les menaces et tous les risques détectés et évités au niveau des clients d'entreprise sécurisés par Zimperium. Ces données d'entreprise rendues anonymes comprennent également les menaces détectées signalées pendant l'installation dans le cadre de l'étape de visibilité du déploiement.

Unless stated otherwise, the following data and analysis is derived from the anonymized and aggregated data provided with permission to Zimperium from its enterprise clients.

Les logiciels malveillants mobiles sont plus prolifiques que beaucoup semblent le croire, avec une moyenne mondiale de 23 % des points terminaux rencontrant une forme ou une autre de ces applications malveillantes en 2021.

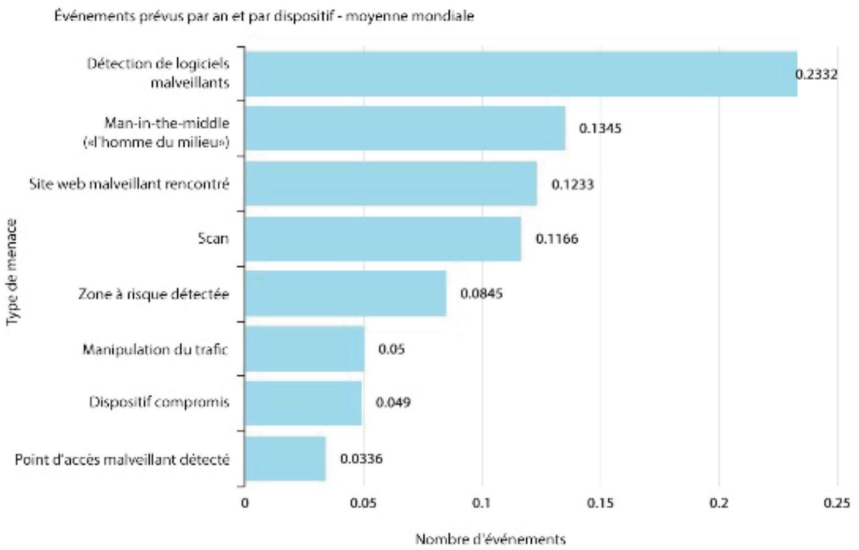
Qu'ils soient téléchargés depuis une source tierce ou directement d'un magasin OEM, ces logiciels malveillants constituent le plus grand risque statistique pour les dispositifs mobiles, les utilisateurs et les données connectées au cloud.

Les attaques de type « Man in The Middle » (MiTM) et celles par scans présentent également des risques accrus pour les points terminaux dans le cadre de chaînes d'attaques plus larges contre les systèmes d'entreprise afin d'accéder à des données très précieuses, ces attaques représentent donc des étapes très importantes dans les chaînes d'attaques en matière de renseignement et de reconnaissance.

Une moyenne de 12 % des terminaux mobiles, soit 1 sur 10, ont été victimes du phishing et des sites web malveillants, mettant en danger les informations d'identification des utilisateurs, l'intégrité des appareils et la sécurité de l'entreprise.

Expected Events per Year per Device | Global Average

Global Mobile Threat Events



23 % ont été confrontés à des logiciels malveillants

13 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

12 % ont été confrontés à un site web malveillant

12 % ont été confrontés à des attaques par scans

8 % ont été confrontés à un réseau malveillant connu

5 % ont été confrontés à une manipulation du trafic

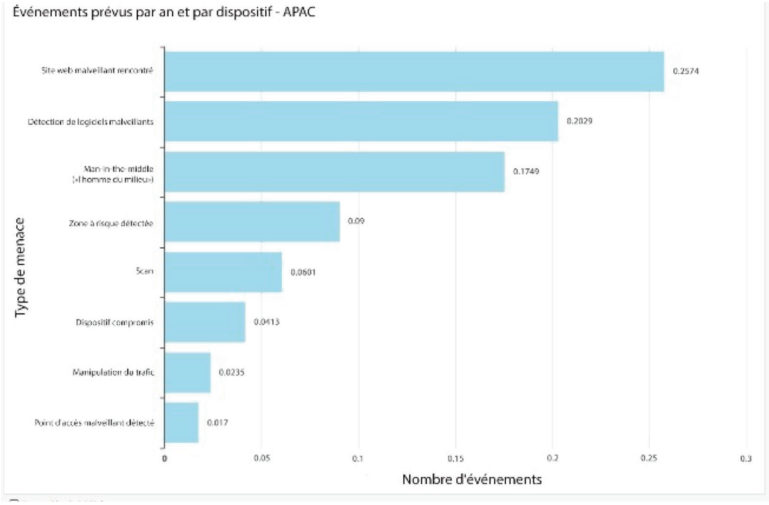
5 % de dispositifs compromis

3 % ont été confrontés à un point d'accès malveillant

Menaces sur les terminaux mobiles par région

Expected Events per Year, per Device | APAC

Asia/Pacific, Mobile Threat Events (2021)



26 % ont été confrontés à un site web malveillant

20 % ont été confrontés à des logiciels malveillants

17 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

9 % ont été confrontés à un réseau malveillant connu

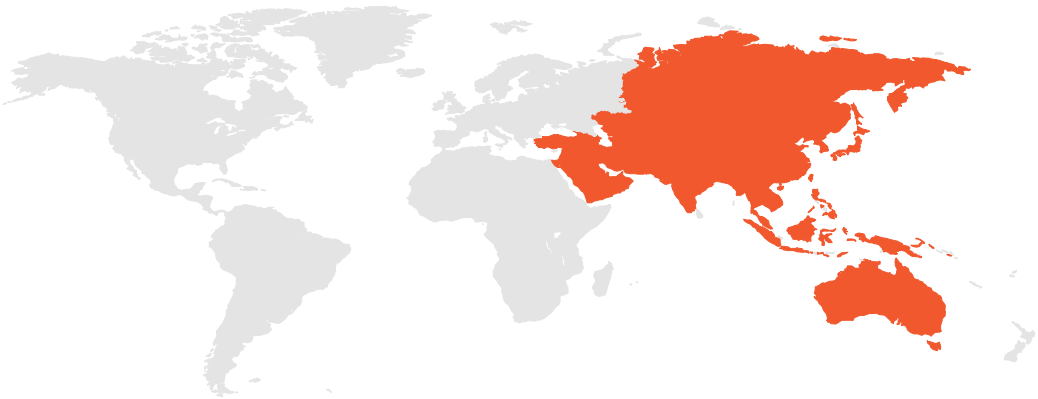
6 % ont été confrontés à des attaques par scans

4 % de dispositifs compromis

2 % ont été confrontés à une manipulation du trafic

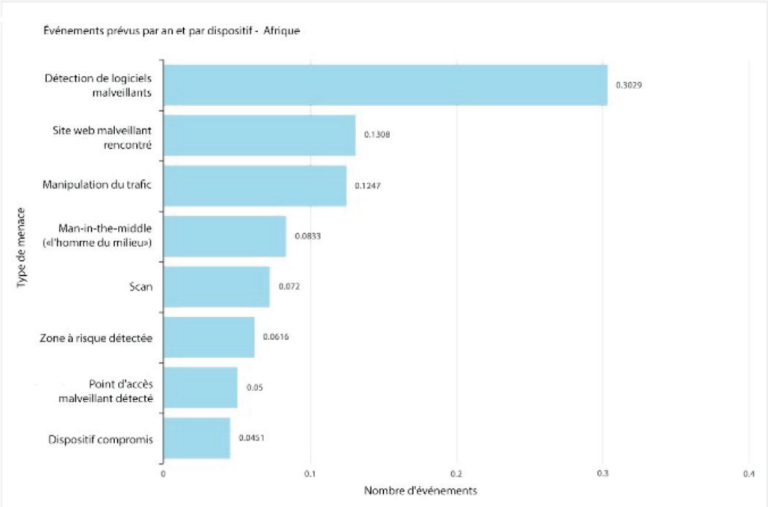
2 % ont été confrontés à un point d'accès malveillant

Asie / Pacifique - Les utilisateurs des dispositifs mobiles en Asie sont susceptibles de rencontrer des sites web malveillants deux fois plus que la moyenne mondiale. 1 sur 4 - soit 25 % - des dispositifs mobiles professionnels ont été victimes d'attaques de type phishing au moins une fois en 2021. Les attaques du type phishing ont été prépondérantes dans la région Asie / Pacifique, elles ciblent principalement les dispositifs mobiles via des outils de communication ordinaires comme les SMS, les médias sociaux et autres programmes de chat. Les messages in-app (dialogues avec les utilisateurs dans l'appli) contournent également plusieurs contrôles de sécurité externes, en diffusant des sites de phishing directement sur le dispositif mobile. Un dispositif mobile sur cinq a été infecté par des logiciels malveillants, les principaux responsables étant les magasins d'applications tiers et le sideloading par hameçonnage. 17 % des dispositifs mobiles professionnels sécurisés ont été victimes d'attaques du type « Man in The Middle » (MiTM), et un peu moins de 10 % ont vu leurs dispositifs analysés par un réseau et privés de données et d'informations indispensables.



Expected Events per Year, per Device | Africa

Africa, Mobile Threat Events (2021)



Afrique - En 2021, un pourcentage alarmant de 30 %, soit 1 sur 3, des points terminaux mobiles en Afrique ont été victimes des logiciels malveillants, ce qui représente le plus grand risque pour les entreprises et les utilisateurs de la région. Des attaques de type phishing ou sa variante spear-phishing qui utilisent des SMS ou des moyens de communication ont été détectées sur 13 % des dispositifs mobiles, soit un peu plus de 1 sur 10. Par ailleurs, 13 % des points d'extrémité ont été confrontés à une manipulation du trafic, ce qui a eu un impact sur la sécurité réelle de la connexion du dispositif mobile avec son réseau. Environ 8 % des dispositifs sont connectés à des réseaux à risque, et ces connexions mettent en danger la communication et les données en les exposant à des attaques de type « Man in The Middle » (MiTM).

30 % ont été confrontés à des logiciels malveillants

13 % ont été confrontés à un site web malveillant

13 % ont été confrontés à une manipulation du trafic

8 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

7 % ont été confrontés à des attaques par scans

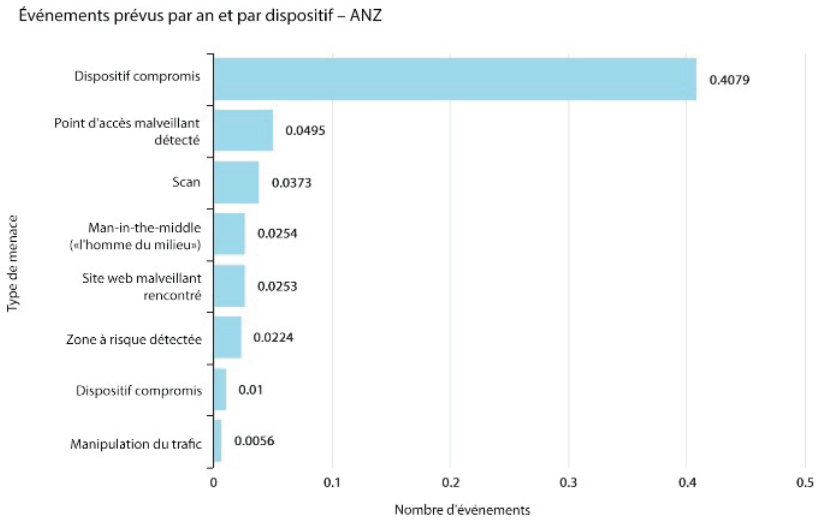
6 % ont été confrontés à un réseau malveillant connu

5 % ont été confrontés à un point d'accès malveillant

5 % de dispositifs compromis

Expected Events per Year, per Device | Australie

Australie, Mobile Threat Events (2021)



Australie / Nouvelle-Zélande - Les utilisateurs de dispositifs mobiles en Australie et en Nouvelle-Zélande sont susceptibles de rencontrer des logiciels malveillants presque deux fois plus que la moyenne mondiale, avec 40 % des dispositifs confrontés à des applications malveillantes. Les utilisateurs des dispositifs mobiles de la région sont également plus susceptibles de rencontrer des points d'accès malveillants que la moyenne mondiale, ce qui expose leurs données et leurs connexions à plus de risque. Dans les deux pays, les attaques du type « Man in The Middle » (MiTM) et les sites web malveillants sont à part égale avec 2 % des utilisateurs qui rencontrent ces risques sur leurs terminaux mobiles.

40 % ont été confrontés à des logiciels malveillants

4 % ont été confrontés à un point d'accès malveillant

3 % ont été confrontés à des attaques par scans

2 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

2 % ont été confrontés à un site web malveillant

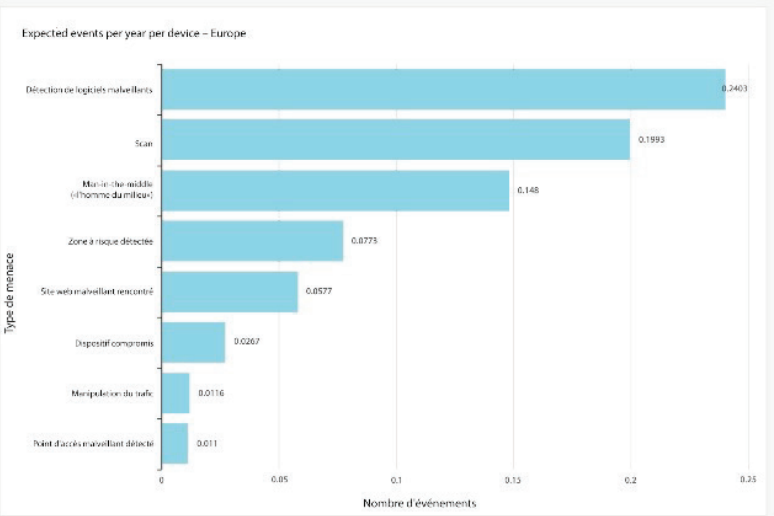
2 % ont été confrontés à un réseau malveillant connu

1 % de dispositifs compromis

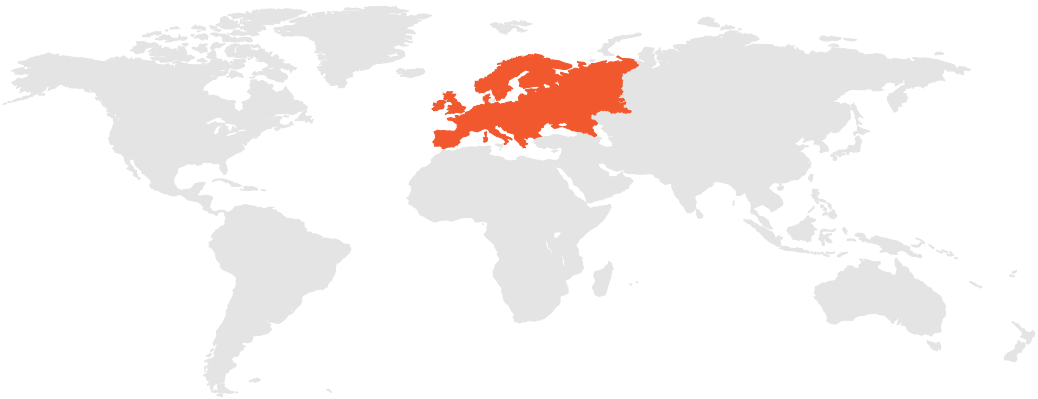
0.5 % ont été confrontés à une manipulation du trafic

Expected Events per Year, per Device | Europe

Europe, Mobile Threat Events (2021)



Europe - 1 utilisateur de dispositif mobile européen sur 4, soit 24 %, a rencontré des logiciels malveillants sur ses dispositifs, exposant ainsi ses données personnelles et professionnelles à plus de risque. Au total, les réseaux compromis et malveillants en plus de la manipulation des données représentent le plus grand risque pour les utilisateurs des dispositifs mobiles dans les pays européens. Un utilisateur mobile sur cinq, soit 19 %, a été confronté à une reconnaissance du réseau par le biais de scans, ce qui a pu divulguer des données critiques sur le dispositif. 14 % des dispositifs ont subi des attaques de type « Man in The Middle » (MiTM), et 7 % se sont connectés à des réseaux présentant des risques et des problèmes de sécurité élevés.



24 % ont été confrontés à des logiciels malveillants

19 % ont été confrontés à des attaques par scans

14 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

7 % ont été confrontés à un réseau malveillant connu

5 % ont été confrontés à un site web malveillant

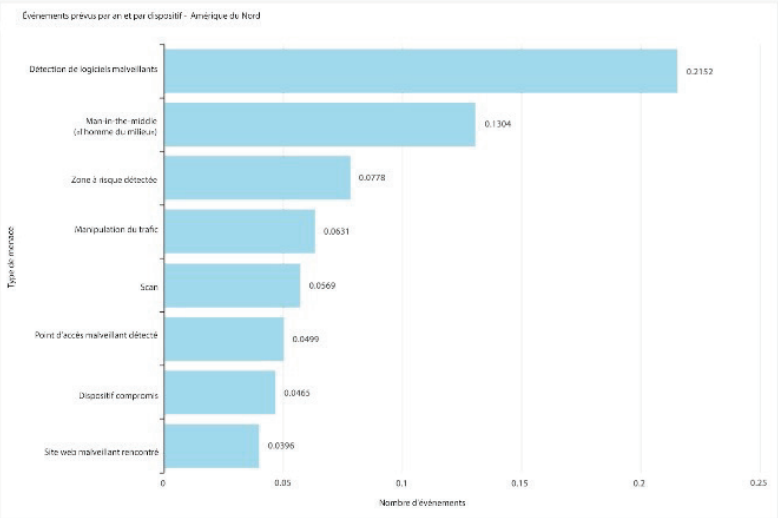
2 % de dispositifs compromis

1 % ont été confrontés à une manipulation du trafic

1 % nt été confrontés à un point d'accès malveillant

Expected Events per Year Per Device | North America

North American Mobile Threat Breakdown



22 % ont été confrontés à des logiciels malveillants

13 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

8 % ont été confrontés à un réseau malveillant connu

6 % ont été confrontés à une manipulation du trafic

6 % ont été confrontés à des attaques par scans

5 % ont été confrontés à un point d'accès malveillant

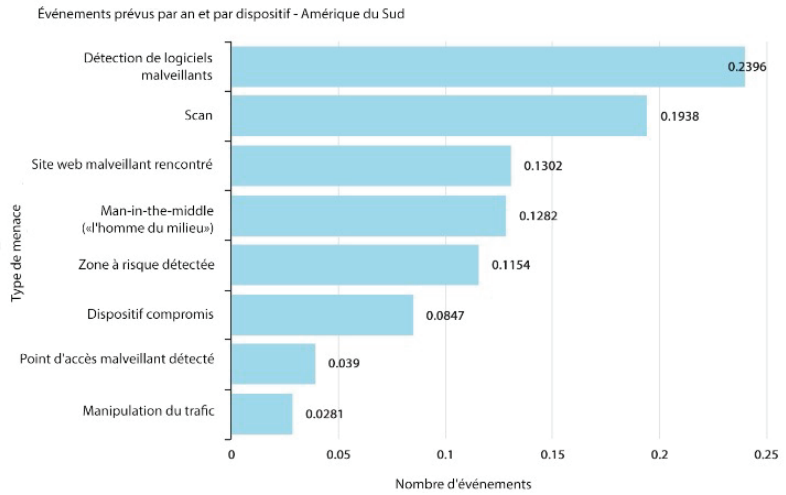
5 % de dispositifs compromis

4 % ont été confrontés à un site web malveillant

Amérique du Nord - 1 dispositif mobile professionnel sur 5 a été victime d'un logiciel malveillant en Amérique du Nord, ce qui met les dispositifs et les données en danger, tant pour l'utilisateur final que pour l'entreprise. Les attaques de type « Man in The Middle » (MiTM) étaient également omniprésentes contre les téléphones et les tablettes, représentant 13 % des tentatives d'interception des communications. Bien qu'ils ne soient pas aussi constatées comme les deux autres types de menaces, les risques connus de réseaux malveillants et de manipulation du trafic mettent en évidence la falsification des données comme étant un risque d'entreprise résultant de réseaux mal sécurisés.

Expected Events per Year Per Device | South America

South America Mobile Threat Breakdown



24 % ont été confrontés à des logiciels malveillants

19 % ont été confrontés à des attaques par scans

13 % ont été confrontés à un site web malveillant

13 % ont été confrontés à des attaques du type « Man in The Middle » (MiTM)

12 % ont été confrontés à un réseau malveillant connu

8 % de dispositifs compromis

4 % ont été confrontés à un point d'accès malveillant

3 % ont été confrontés à une manipulation du trafic

Amérique du Sud - 1 point d'extrémité mobile sur 4, soit 24 % de ceux d'Amérique du Sud, a rencontré des logiciels malveillants mobiles en 2021. Ces logiciels sont généralement téléchargés directement depuis des magasins d'applications ou téléchargés en mode « sideload » afin de contourner les restrictions régionales. 1 dispositif mobile sur 5 a fait l'objet d'une analyse du réseau, ce qui a mis en danger les données critiques sur le dispositif. En Amérique du Sud, 13 % des dispositifs, soit un peu plus de 1 sur 10, ont également été victimes d'attaques par phishing et d'attaques de type « Man in The Middle » (MiTM), ce qui expose les données critiques à des risque de surveillance des communications ou encore de vol d'informations d'identification.

Les données indiquent la diversité des risques, des menaces et des attaques qui visent les terminaux mobiles à l'échelle mondiale. Les logiciels malveillants mobiles continuent de dominer le paysage des menaces, car ils représentent la méthode la plus simple et efficace pour attaquer, compromettre et voler les terminaux mobiles. Les attaques qui se basent sur le réseau sont également efficaces et très célèbres, elles s'appuient sur un élément distinctif très important du téléphone mobile, à savoir la possibilité de rechercher en permanence une connectivité. Avec la montée du nombre de travailleurs et de clients distants et décentralisés, les entreprises doivent se préparer et se protéger contre un paysage de menaces en constante évolution, en selon l'emplacement dans lequel se trouvent leurs employés, leurs applications et leurs données dans le monde. La surface d'attaque moderne s'est agrandie, et les attaques qui menacent les entreprises continuent d'être répandues et efficaces contre les dispositifs non sécurisés.

Répartition des vulnérabilités les plus fréquemment exploitées en 2021

« L'augmentation des plateformes mobiles a provoqué une augmentation du nombre de produits dont des organismes veulent tirer profit ».

- Maddie Stone et Clément Lecigne, Groupe d'analyse des menaces de Google, 2021.[45]

2021 était « l'année de l'exploitation » par excellence. Les équipes chargées de sécurité ont lutté contre la montée en flèche des vulnérabilités exploitées de type « zero-day » ou encore inédites, sur tous les systèmes d'extrémité, y compris les systèmes mobiles Android et iOS. **La recours de plus en plus fréquents aux technologies mobiles et la croissance du marché de celles-ci ont présenté des perspectives viables pour les acteurs malveillants d'exploiter des systèmes généralement non sécurisés, avec plus de 30 % des vulnérabilités zero-day connues découvertes en 2021 et qui ciblent les dispositifs mobiles.**[44] **Cette tendance représente la plus forte augmentation des exploits de type « zero-day » dans l'histoire des smartphones et des tablettes.** Même le projet Zero de Google a abordé cette question lors de la récente divulgation de multiples attaques de type « zero-day ».

Qu'il soit connu ou non, chaque exploit présente une lacune potentielle dans la gestion de la surface d'attaque d'un dispositif mobile. Dans l'univers du concept BYOD, la surface d'attaque des dispositifs mobiles ne représente plus une menace réservée aux consommateurs. Chacune d'entre elles représente un risque accru pour la sécurité de l'entreprise. Chaque type d'exploit, si jamais il se trouve entre les mains du bon attaquant, peut représenter un outil très efficace dans une attaque ciblant un terminal mobile, que ce dernier soit géré ou pas, ceci aide donc l'attaquant à mettre le pied dans les systèmes et réseaux d'entreprise.

Ignorées et non corrigées, ces vulnérabilités CVE (Common Vulnerabilities and Exposures) connues mettent les entreprises en danger en laissant des failles dans les systèmes. Pour compliquer encore la situation, chaque fabricants gère son cycle de diffusion de mises à jours de sécurité à sa propre façon. En attendant, plusieurs téléphones, plus anciens, ne reçoivent pas les mises à jour récentes, ce qui les expose donc à des vulnérabilités plus anciennes et connues et les rend des cibles plus faciles pour les acteurs malveillants.

Depuis quelques années, la recherche de vulnérabilités de type « zero-day » sur les dispositifs mobiles est devenue un marché de plus en plus lucratif. Dans cet esprit, les chercheurs sont de plus en plus nombreux à rechercher activement des exploits. Pour remédier à cette situation, les entreprises doivent atténuer ces nouvelles menaces à la sécurité de leurs systèmes et réseaux.

Plusieurs exploits de type « zero-day » ont été découverts et signalés car ils sont devenus de plus en plus rentables pour de nombreux experts en sécurité. Les primes aux bogues officielles et officieuses se multiplient, avec des gains importants pour les découvertes encore plus poussées, du moins par rapport aux exploits concernant les points finaux classiques. Pour les exploits mobiles qui n'ont pas encore été découverts, Zerodium, une plateforme de chasse de vulnérabilités de type « zero-day » et leader en recherche avancée en cybersécurité, propose actuellement des récompenses pouvant aller jusqu'à 2 500 000 dollars.[46] Les récompenses pour les dispositifs mobiles peuvent permettre aux experts de gagner plus que le double de gain, il s'agit donc d'une recherche de grande valeur.

Ci-après un résumé des vulnérabilités d'Android et d'iOS en 2021, mettant en évidence les surfaces d'attaque complexes de ces deux écosystèmes mobiles. Vous y trouverez un historique des vulnérabilités de type « zero day », utilisées dans des attaques réelles contre des dispositifs mobiles, pendant toute l'histoire des terminaux mobiles.

Traceur des CVE Android (Android CVE Tracker)[47]

D'après le suivi des vulnérabilités, le système d'exploitation Android a enregistré une baisse du nombre de vulnérabilités en 2021, avec 574 CVE suivies. En 2020, on a relevé 859 cas. Les principales vulnérabilités concernaient l'injection de code arbitraire, le bypass et le débordement ou le dépassement de tampon.

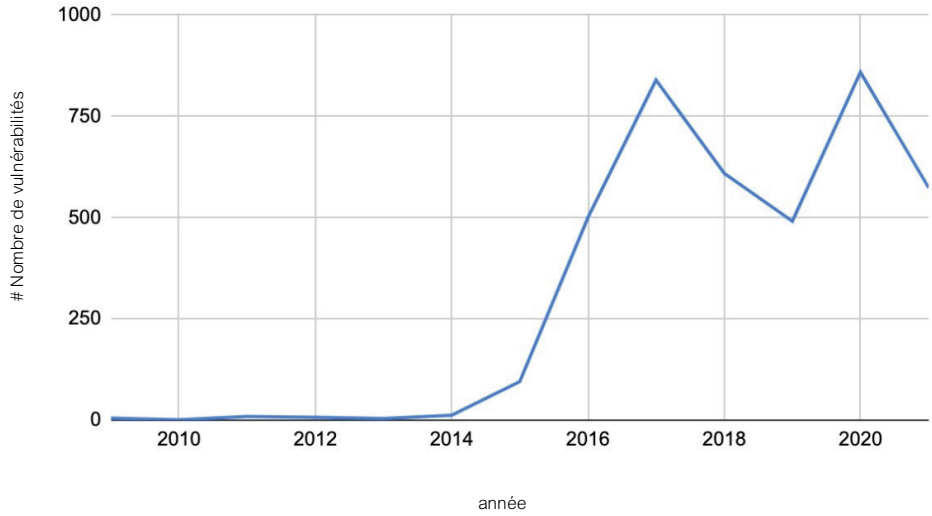
Parmi les vulnérabilités signalées et suivies :

21 % sont classées dans la catégorie des attaques de complexité moyenne.

79 % sont classées dans la catégorie des attaques peu complexes.

135 vulnérabilités CVE **(soit 23 %)** suivies ont enregistré un score CVSS de **7,2** ou plus, **18** d'entre elles figurant dans la catégorie critique. Cela représente une diminution par rapport à l'année précédente, avec **62** vulnérabilités critiques découvertes et signalées en **2020**.

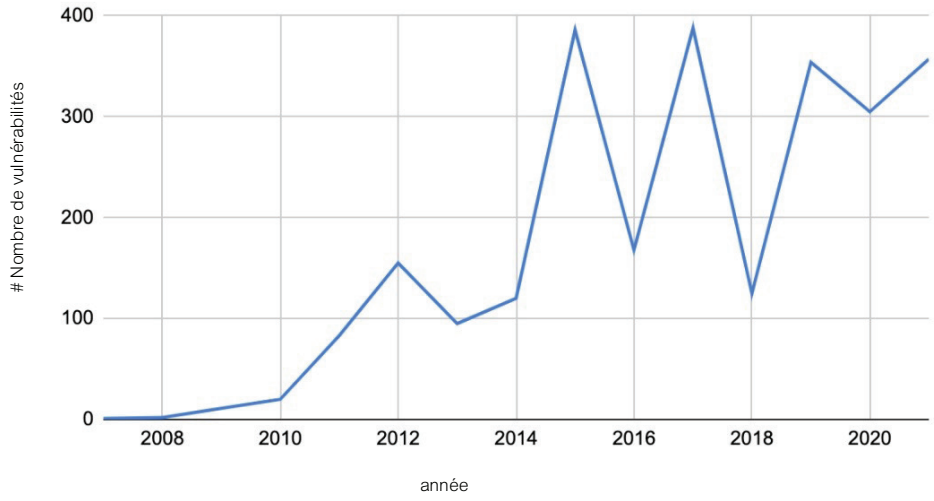
Nombre de vulnérabilités par année



Traceur des CVE pour iOS[48]

Dans le cadre du suivi des vulnérabilités, 357 vulnérabilités CVE ont été attribuées à Apple iOS en 2021. Cela représente une augmentation par rapport aux 305 cas découverts et signalés en 2020. Les principales vulnérabilités étaient l'injection de code arbitraire suivie par le débordement ou le dépassement de tampon.

Nombre de vulnérabilités par année



Parmi les vulnérabilités signalées et suivies :

24 % sont classées dans la catégorie des attaques peu complexes.

2 % sont classées dans la catégorie des attaques très complexes.

74 % sont classées dans la catégorie des attaques de complexité moyenne.

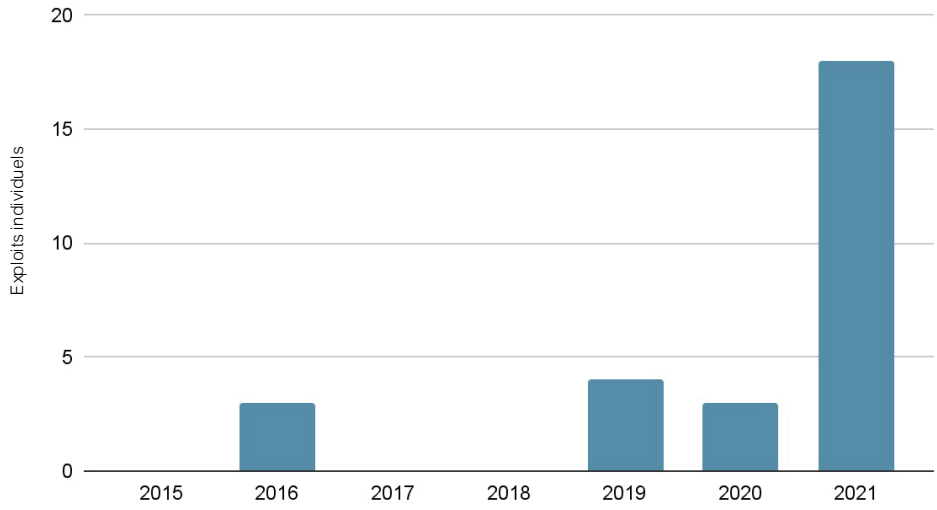
63 vulnérabilités CVE **(soit 17 %)** ont enregistré un score CVSS de **7,2** ou plus, **45** d'entre elles figurant dans la catégorie critique. En **2020**, **67** vulnérabilités critiques ont été identifiées et signalées.

Exploits en libre circulation de type « zero day » découverts en 2021[49]

Les exploits de vulnérabilités de type « zero day » en libre circulation sont des vulnérabilités détectées lors d'attaques réelles contre des utilisateurs, alors que ni le public ni le fournisseur n'en étaient au courant. Cela signifie qu'aucun correctif n'était disponible au moment de la survenue de l'attaque.

Le suivi des tendances représente un aperçu de l'évolution du paysage des vulnérabilités zero-day des dipsositifs mobiles :

Exploitation mobile de type « zero day » en circulation libre



Le suivi des tendances représente un aperçu de l'évolution du paysage des vulnérabilités zero-day des dipsositifs mobiles :

En 2021, on a constaté une augmentation de 466 % des vulnérabilités zero-day exploitées et utilisées dans des attaques actives contre les terminaux mobiles.

- **2021 :** 58 vulnérabilités de type « zero-day » au total, dont 31 % (17) concernent les dispositifs mobiles
- **2020 :** 26 vulnérabilités de type « zero-day » au total, dont 11 % (3) concernent les dispositifs mobiles
- **2019 :** 21 vulnérabilités de type « zero-day » au total, dont 19 % (4) concernent les dispositifs mobiles

Malgré la grande popularité des dispositifs mobiles au cours de la dernière décennie, les vulnérabilités de type « zero-day » qui ciblent les terminaux mobiles - comme les téléphones et les tablettes - ont gagné en importance plus que jamais au cours des trois dernières années.

En 2021, les vulnérabilités iOS représentaient 64 % des attaques zero-days qui ciblent spécifiquement les dispositifs mobiles.

Selon l'équipe de recherche zLabs, cette hausse est due à l'augmentation du nombre de systèmes de données personnelles, privées et sensibles connectés à des terminaux mobiles. Lorsque les chasseurs de failles informatiques cherchent de nouvelles opportunités exploitables, ils cherchent des dispositifs qui permettent d'accéder aux données et représentent une faible couverture de sécurité. Les terminaux mobiles constituent des cibles de grande valeur qui, une fois exploitées, deviennent les clés du royaume des données.

La montée en puissance du phishing mobile

Les références au attaques par phishing remontent à 1995, mais malheureusement, au lieu de s'éloigner de plus en plus dans l'histoire, elles constituent un élément essentiel de l'arsenal des cyber-attaquants. À un niveau plus élevé, voici comment fonctionne le phishing :

- Les cybercriminels créent des sites Web qui se font passer pour des tiers de confiance et tentent ensuite de persuader les utilisateurs à visiter ces sites.
- Dès qu'un utilisateur communique ses identifiants ou des informations confidentielles sur le site, l'attaquant les exploite pour contrôler le compte ou mener d'autres actions frauduleuses.
- Puisque de nombreux utilisateurs utilisent le même mot de passe sur plusieurs sites, une seule attaque réussie peut souvent menacer plusieurs services et comptes.
- Cette attaque s'appuie sur l'ingénierie sociale afin d'exploiter la confiance et la curiosité des victimes à travers des communications qui semblent officielles.

Les cyber-attaquants ciblent généralement les victimes via des canaux électroniques, comme les e-mails, le détournement se sites Web (d'adresses IP) et les SMS. Toutefois, les cyber-attaquants peuvent aussi utiliser les communications téléphoniques afin de leurrer une victime. Au fil des années, différentes sous-catégories ont vu le jour :

- **Le spear phishing (ou hameçonnage ciblé).** L'attaquant cible une organisation ou une personne bien déterminée.
- **Le whaling (ou la chasse à la baleine).** Il s'agit d'une attaque qui vise des victimes spécifiques de haut niveau au sein d'une entreprise.

Phishing continues to be employed because, quite simply, **it works.**

Prévalence du phishing

La pratique du phishing persiste parce qu'elle est tout simplement très efficace. Selon un rapport, le phishing était présent dans 36 % des attaques, et cette pratique a connu une croissance de 10 % entre 2020 et 2021.[50] Par ailleurs, des recherches ont montré que les e-mails de phishing étaient le principal moyen de diffusion des ransomwares, soit environ 54 % de ces attaques.[51]

Pendant notre étude, les participants ont été interrogés sur les risques qui les préoccupent le plus. « L'exploitation par phishing » fut la réponse la plus souvent citée (55 %). De plus, 61 % des personnes interrogées ont déclaré avoir constaté un pic d'attaques de phishing pendant la pandémie de COVID-19. En plus, les attaques de phishing sont devenues des escroqueries très en vogue : des outils et des kits de phishing permettent désormais aux utilisateurs, même novices, de créer des sites frauduleux en quelques clics.

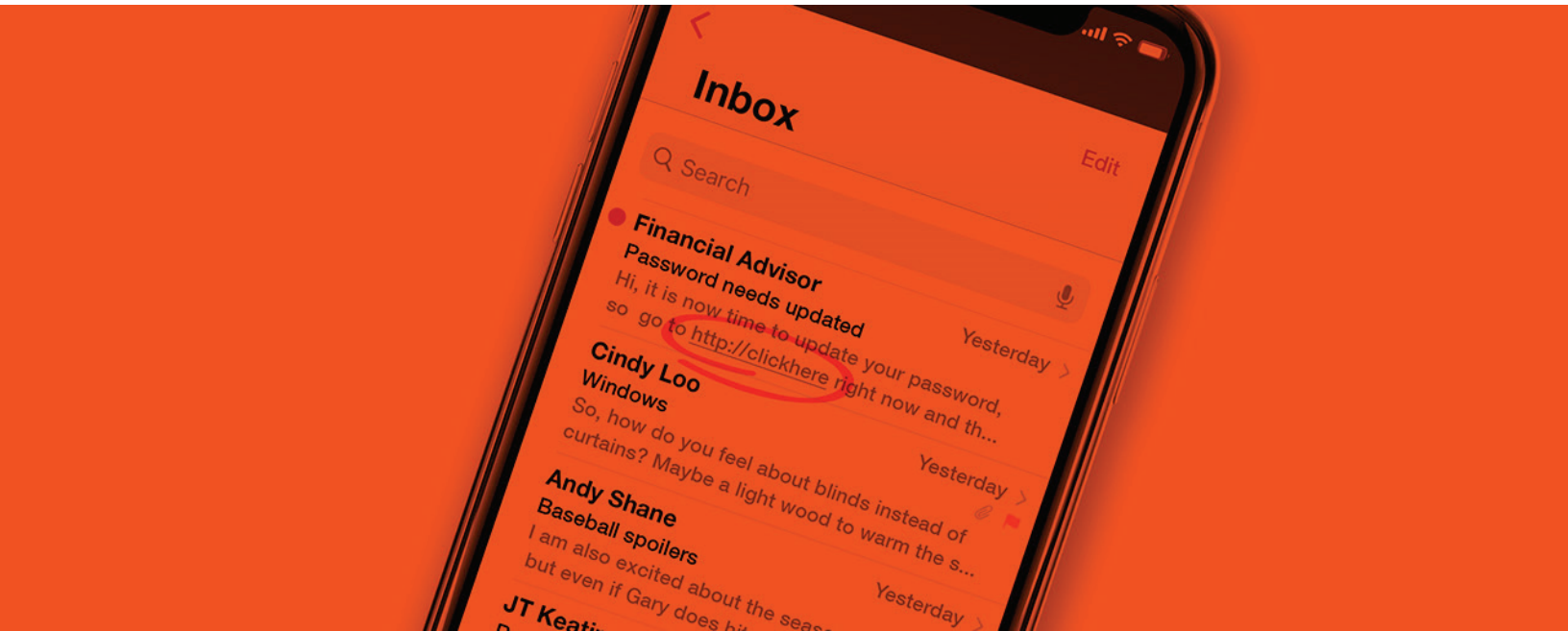
61 %

des personnes interrogées ont déclaré avoir constaté un pic d'attaques de phishing pendant la pandémie de COVID-19.

Au fil des ans, nous sommes devenus de plus en plus dépendants de nos téléphones mobiles, tant dans notre vie personnelle que professionnelle. Si cette tendance s'observe depuis un certain temps, la pandémie de COVID-19 a bien accéléré la transition. Cette dépendance accrue envers les smartphones au travail signifie que les utilisateurs accèdent régulièrement aux données et aux applications de l'entreprise. En plus, ces dispositifs ne bénéficient pas du même niveau de sécurité que les ordinateurs classiques portables et de bureau, ce qui encourage les cyber-attaquants potentiels à miser sur les dispositifs mobiles.

Généralement, les terminaux mobiles ne sont pas sécurisés ou, le cas échéant, les systèmes de sécurité ne sont pas aussi performants que ceux des terminaux classiques. En essayant d'appliquer les outils de sécurité classiques aux dispositifs mobiles, les équipes techniques sont souvent confrontées à plusieurs obstacles. Par exemple, les contraintes de traitement peuvent limiter les capacités d'analyse potentielles. Sur les dispositifs mobiles, les outils de sandboxing ne fournissent pas toutes les informations essentielles à la détection avancée des menaces.

En plus, les dispositifs mobiles présentent de façon inhérente des difficultés supplémentaires. Les écrans plus réduits des dispositifs mobiles peuvent cacher des indices pouvant avertir un utilisateur en cas d'un site malveillant, car la taille de l'écran peut masquer le drapeau rouge. Les dispositifs mobiles sont utilisés pour plusieurs vecteurs de communication, notamment les e-mails, le chat, la messagerie in-app, la messagerie instantanée, etc. Ces différents canaux offrent un nombre de plus en plus important de surfaces d'attaque que les cybercriminels peuvent exploiter.



Cette insécurité des dispositifs mobiles, à laquelle s'ajoute le fait que ces dispositifs deviennent désormais des passerelles vers des données personnelles et professionnelles très sensibles, il n'est pas surprenant que ces dispositifs soient de plus en plus la cible des cyber-attaquants.

Alors que le phishing était, de par sa nature, indépendant des dispositifs, Zimperium a détecté une augmentation du nombre de sites de phishing dédiés aux mobiles. Nous avons effectué une analyse de nos propres données et de celles librement accessibles sur une période de 2 ans et demi. Dans cette analyse, nous avons pu analyser plus de 500 000 sites. **Au cours de cette période, le nombre de sites de phishing spécifiques aux mobiles a augmenté de 50 %. En outre, au cours de l'année 2021, 75 % des sites de phishing analysés ciblaient spécifiquement les dispositifs mobiles et délivraient un contenu adapté au format mobile.**

Les sites de phishing exploitant les dispositifs mobiles entre 2019 et 2021

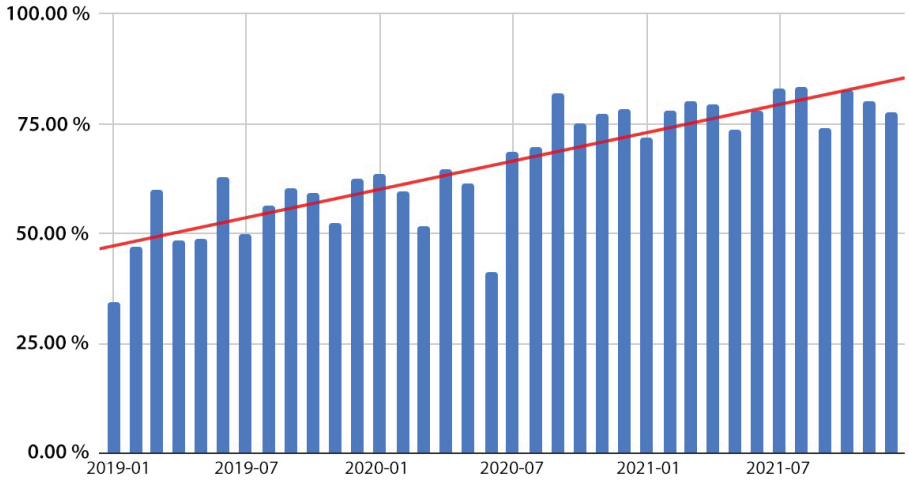


Figure # : Le nombre de sites de phishing qui ciblent spécifiquement les dispositifs mobiles a connu une croissance très rapide, et les sites qui ciblent les dispositifs mobiles représentent désormais plus de 3/4 de l'ensemble des sites analysés.

En outre, les attaques suivies deviennent de plus en plus compliquées. **Ainsi, entre 2019 et 2021, le pourcentage de sites de phishing qui utilisent des communications sécurisées (communément appelées HTTPS) n'a cessé d'augmenter, ce qui rend de plus en plus difficile pour les utilisateurs de distinguer ces sites de ceux qui sont sécurisés.**

Les sites de phishing utilisant https entre 2019- et 2021

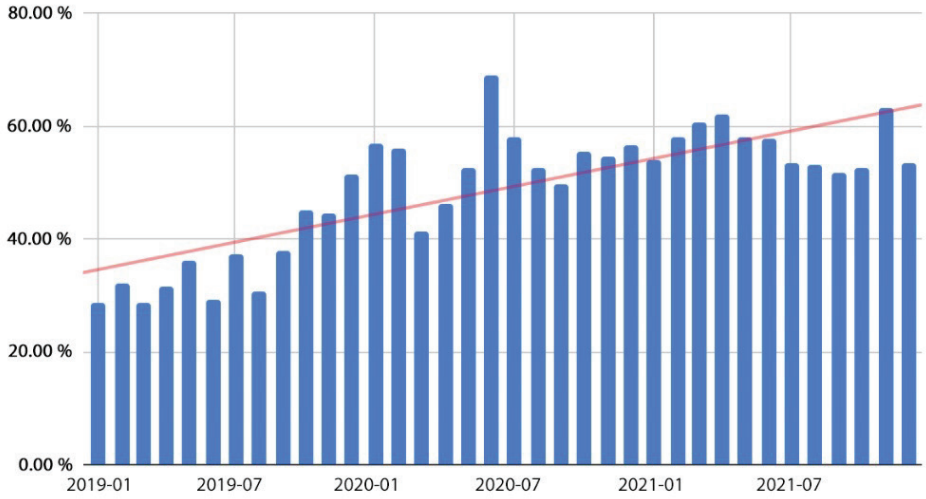


Figure # : Le pourcentage de sites de phishing qui utilisent le protocole HTTPS a connu une croissance constante.

Figure # : Si un utilisateur naviguant sur le site malveillant avec un ordinateur portable recevra un message d'erreur 404, l'utilisateur d'un appareil mobile verra un site de phishing qui imite une page de connexion au compte PayPal.

Comment les hackers ciblent les dispositifs mobiles

Pour cibler des dispositifs mobiles, les cybercriminels utilisent des techniques adaptatives ou réactives. Vous trouverez ci-dessous un résumé de certaines de ces approches.

Sites web dits « adaptatifs »

Sur les sites web adaptatifs, il est possible de charger un contenu complètement différent et rediriger vers d'autres sites, selon le dispositif utilisé. Les cybercriminels adaptent le contenu en fonction de l'utilisateur du terminal mobile. Grâce à cette approche, un hacker peut cibler exclusivement les dispositifs mobiles. Par exemple, si un ordinateur de bureau est détecté, le hacker peut empêcher le chargement de la page. Ainsi, il est capable d'éviter d'être détectés par les ordinateurs de bureau équipés d'outils de détection des menaces.

Sites web réactifs

Les sites web réactifs visent à adapter l'emplacement et la taille des objets selon la dimension de l'écran du terminal utilisé et affichent les interfaces de dialogue appropriées. Même si cette réactivité offre aux développeurs d'applications légitimes la possibilité de garantir une meilleure expérience utilisateur, ces mêmes capacités peuvent offrir aux cybercriminels un avantage en matière de phishing.

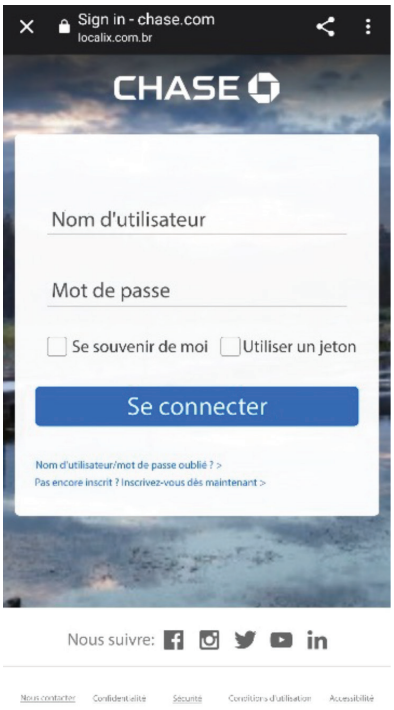


Figure # : Exemple de ce que voit un utilisateur du dispositif mobile du même site de phishing.

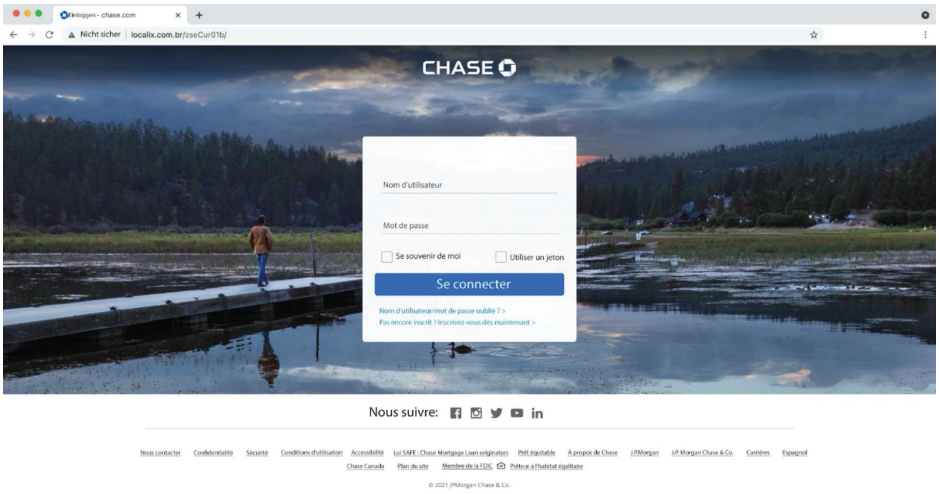


Figure # : Exemple de site de phishing réactif ciblant les utilisateurs de Chase. C'est l'aperçu que verrait l'utilisateur d'un ordinateur de bureau.

Les marques les plus attaquées à l'échelle mondiale

Lorsqu'ils lancent des attaques par phishing, les cybercriminels cherchent à faire croire à leurs victimes qu'elles ont affaire à une organisation à laquelle elles font confiance. Il n'est donc pas étonnant qu'il existe une corrélation claire entre la popularité d'une marque et la probabilité qu'elle soit ciblée. **Les commerces au détail, les réseaux sociaux, les technologies et les services financiers les plus connues et les plus proches des consommateurs monopolisent la catégorie du phishing. Les phishers espèrent que la confiance d'un consommateur dans une marque bien déterminée le poussera à communiquer ses informations d'identification.** Voici les résultats par région en termes de marques les plus utilisées par les phichers.

L'Amérique du Nord

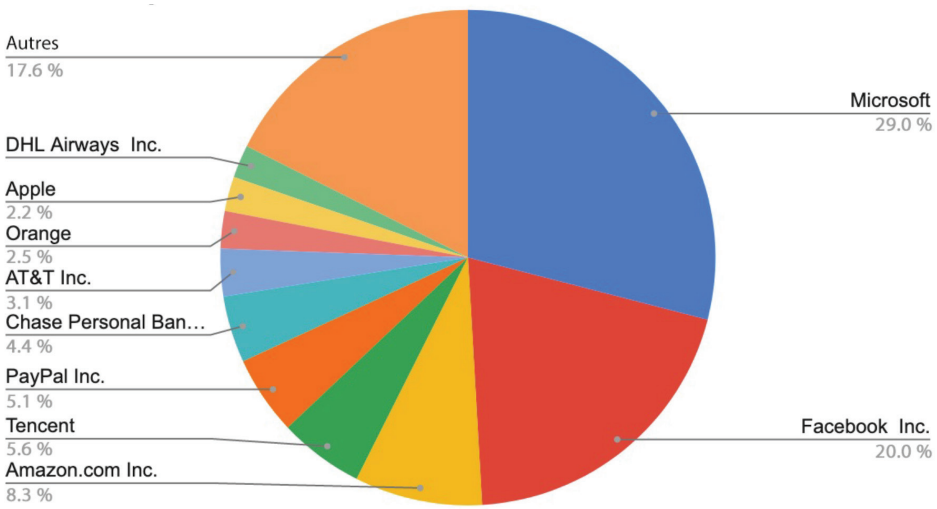


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs en Amérique du Nord.

En Amérique du Nord, près d'un tiers (29 %) des attaques de phishing menées par des entreprises sont censées provenir de Microsoft. Les sites de phishing qui imittent Facebook et Microsoft (20 %) représentaient environ la moitié de toutes les attaques menées. Amazon arrive au troisième rang, avec un peu plus de 8,3 %. Les autres sites comprenaient également des institutions de services financiers (PayPal et Chase combinés représentant 9,5 %), des opérateurs de télécommunications (AT&T représentant 3,1 % et Orange 2,5 %) et une société de transport (DHL Airways avec 2,2 %).

Amérique centrale / Amérique latine

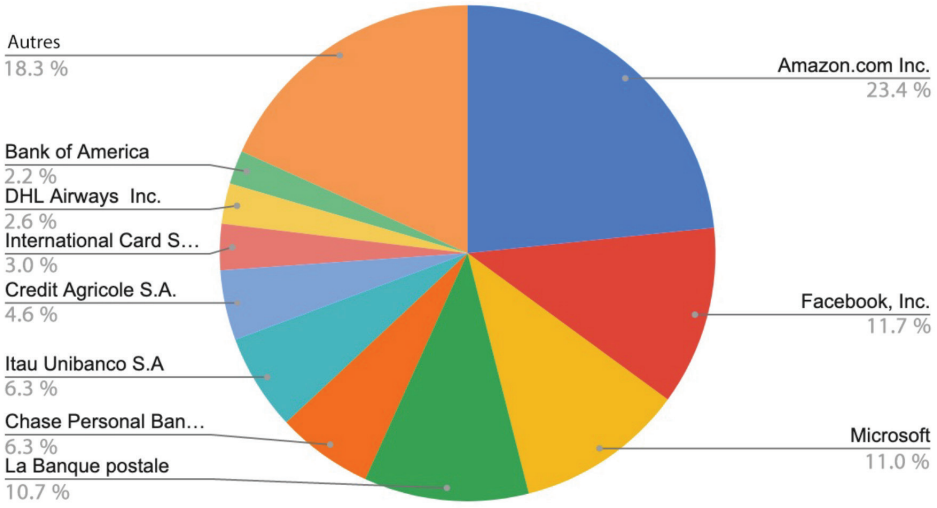


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs en Amérique centrale et en Amérique du Sud.

En Amérique centrale et du Sud, Microsoft et Facebook, respectivement premier et second rang en Amérique du Nord, ont été remplacées par Amazon, qui figure dans environ le quart (23,4 %) de tous les sites de phishing. Facebook et Microsoft sont respectivement deuxième et troisième. À l'exception de DHL Airways (2,6 %), les autres marques phishing les plus importantes étaient toutes des sociétés de services financiers, La Banque Postale figure dans environ 10,7 % des attaques.

Europe / Moyen-Orient

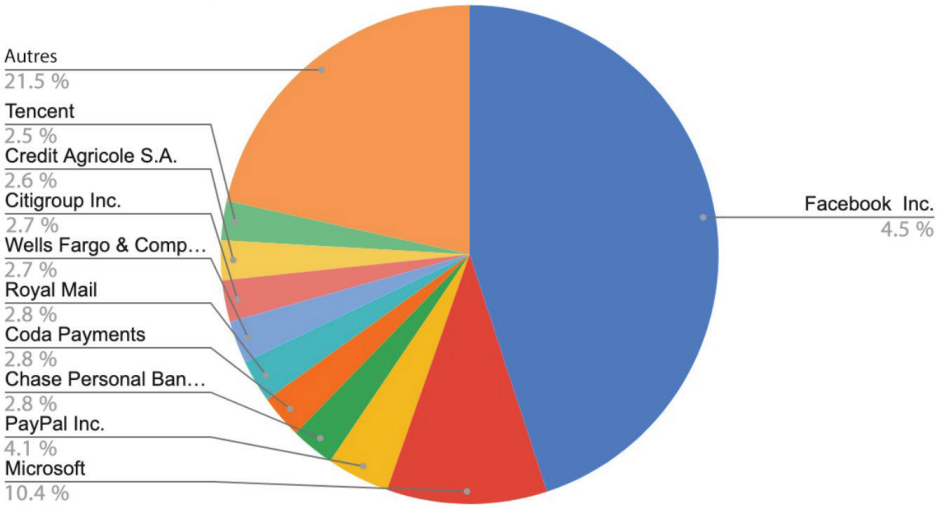


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs en Europe et au Moyen-Orient.

En Europe et au Moyen-Orient, Facebook est de loin le site le plus ciblé par les attaques de phishing. Ce réseau social représentait 45 % des cibles. Microsoft arrive en deuxième place avec 10,4 %. Six parmi ces neufs marques les plus ciblées sont des sociétés de services financiers.

Afrique

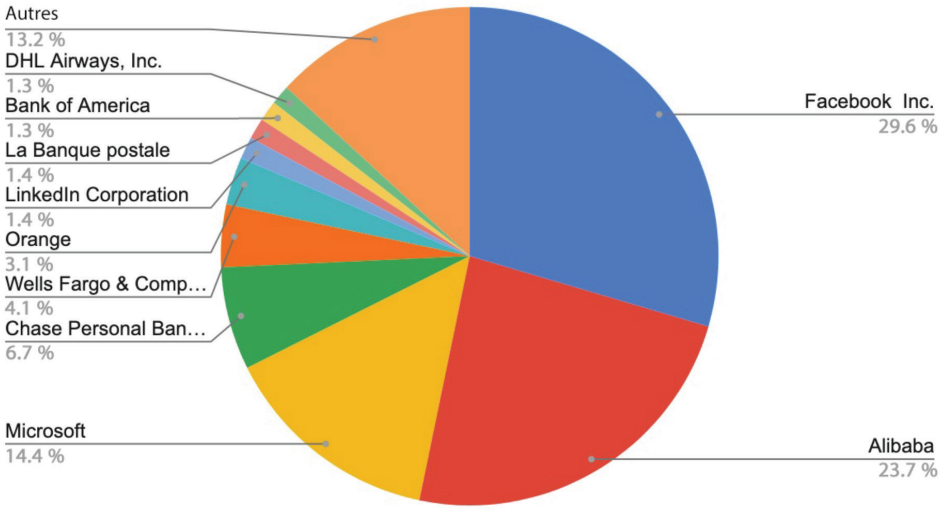


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs en Afrique.

En Afrique, comme en Europe et au Moyen-Orient, Facebook a été la cible privilégiée des cyber-attaquants, figurant dans 29,6 % des sites de phishing. La plus grande part du marché africain revient à Alibaba, avec 23,7 % des attaques. Microsoft arrive en troisième position (14,4 %), suivi de Chase (6,7 %) et de Wells Fargo (4,1 %).

Australie

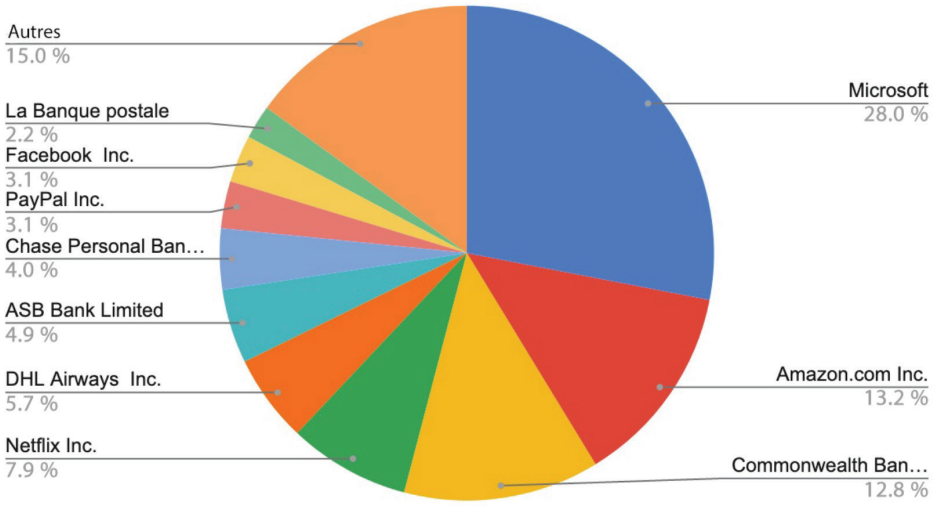


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs en Australie.

En Australie, comme en Amérique du Nord, Microsoft est la marque la plus ciblée, figurant dans 28 % des sites de phishing. Amazon (13,2 %) et Commonwealth Bank (12,8 %) suivis de Netflix (7,9 %), qui n'est pas aussi présent dans les autres régions. En plus du Commonwealth, plusieurs entreprises de services financiers figuraient dans le top 10, notamment ASB Bank (4,9 %), Chase (4,0 %), PayPal (3,1 %) et La Banque Postale (2,2 %).

Asie / Pacifique

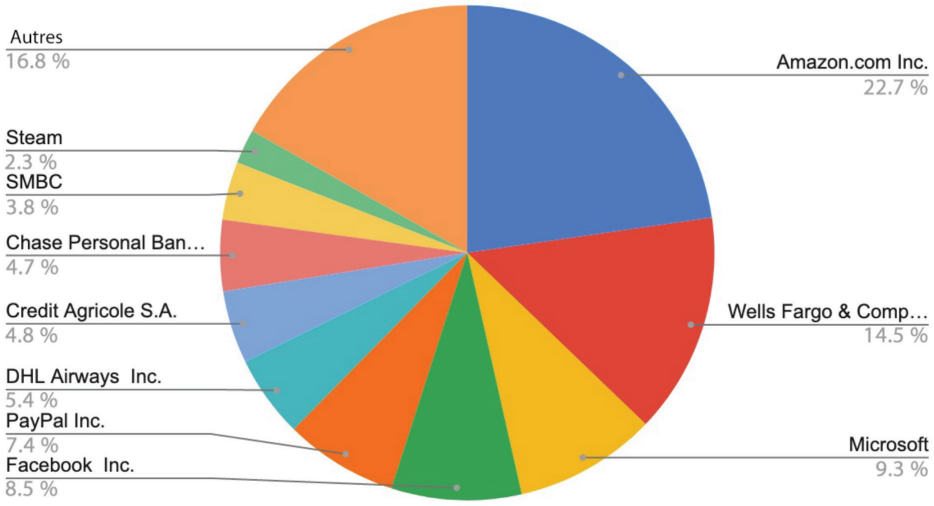


Figure # : Le pourcentage des marques imitées par des sites de phishing ciblant les utilisateurs dans la région Asie-Pacifique.

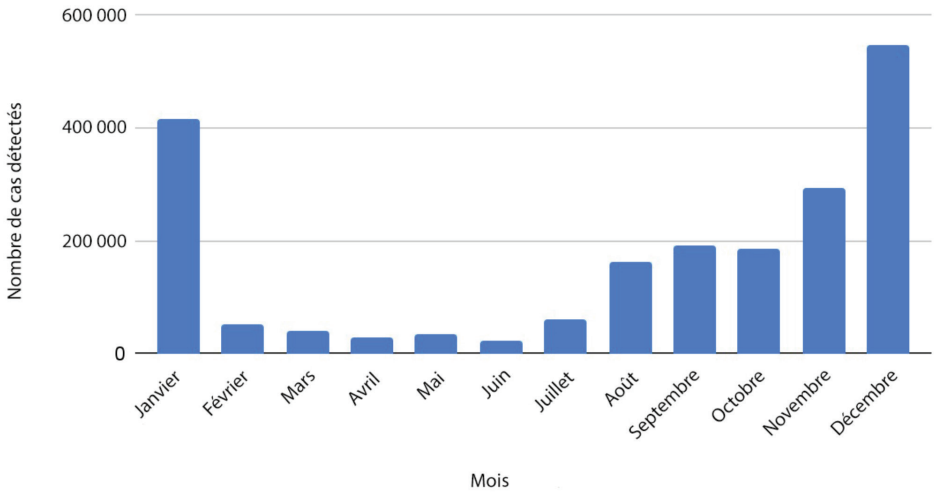
Dans la région Asie-Pacifique, Amazon est le site le plus sollicité par les phishers (22,7 %). Bien que présente dans plusieurs régions, Wells Fargo est plus active ici que partout ailleurs, avec 14,5 %. Malgré sa forte présence sur le marché dans ce domaine, Steam n'est apparu que dans 2,3 % des attaques.

Risques et attaques : Logiciels malveillants, bogues et profils mobiles

Les logiciels malveillants font partie de l'arsenal de tous les cyber-attaquants, car ils sont faciles à accéder et à déployer, ce qui leur permet de causer des effets très dévastateurs. Il existe des millions de différentes souches de logiciels malveillants, avec des milliers de nouveaux programmes créés et publiés chaque jour. Les logiciels malveillants sont devenus la première source de profit des hackers, et c'est pour cette raison qu'ils constituent une cible mouvante.

En 2021, l'analyse de la sécurité mobile de Zimperium a permis de détecter 2 034 217 nouveaux échantillons de logiciels malveillants en libre circulation. En moyenne, cela représente près de 36 000 nouvelles souches de logiciels malveillants par semaine et plus de 5 000 par jour.

Nouveaux logiciels malveillants sur Android - 2021



Même si le pourcentage de nouveaux logiciels malveillants a diminué de 50 % par rapport à l'année précédente, nos études indiquent que ce changement est dû à la genèse de familles de logiciels malveillants recyclés. Les experts ont également constaté que les cyber-attaquants ont investi massivement dans des frameworks très complexes, comme Flutter, Cordova ou Unity, par rapport au code classiques des années passées.

En 2020, les hackers ont profité du confinement dû à la pandémie qui a obligé les entreprises du monde entier à adopter le télétravail.

En 2020, les hackers ont profité du confinement dû à la pandémie qui a obligé les entreprises du monde entier à adopter le télétravail. Ces circonstances exceptionnelles représentent une surface d'attaque beaucoup plus importante, car les employés utilisent souvent des dispositifs fournis par l'entreprise et d'autres personnels, comme les dispositifs mobiles, afin de soutenir leur productivité. Éventuellement, cette situation a contribué à l'augmentation des logiciels malveillants, des ransomware et des exploits dans les entreprises.

En 2021, nos statistiques ont révélé une augmentation des nouvelles variantes de logiciels malveillants mobiles à partir d'octobre et un pic en décembre. Cette montée en flèche n'était pas une surprise. Les cyber-attaquants tirent profit des promos et remises accordées par les entreprises en ligne, promus par des liens dans les courriels et les SMS pendant les périodes de fêtes, en espérant que les utilisateurs téléchargeront des logiciels malveillants sur leurs dispositifs mobiles.

Les logiciels malveillants mobiles sont uniques car leur surface d'attaque est différente. Certaines variantes de logiciels malveillants mobiles agissent en tant que des attaques traditionnelles de points de terminaison, comme les logiciels espions et les chevaux de Troie. D'autres logiciels malveillants peuvent avoir un impact sur les utilisateurs, chose que les logiciels malveillants classiques ne peuvent pas faire, par exemple :

- Vol de code 2FA
- Réalisation d'attaques par superposition
- Attaque d'autres applications mobiles
- Localisation des utilisateurs
- Enregistrement des audios personnels
- Accès aux photos privées et aux données personnelles
- Suivi des données du capteur

Les techniques d'évasion (ou de bypass) et d'exploitation évoluent pour contourner les mécanismes de détection et éviter de « tuer la poule aux œufs d'or », comme en témoigne le nombre de nouveaux échantillons de logiciels malveillants mobiles que nous voyons chaque jour. La détection des logiciels malveillants mobiles n'est pas seulement compliquée, mais les dispositifs mobiles collectent des données de grande valeur. Cela crée une véritable catastrophe pour les cyber-attaquants qui cherchent à mener une attaque rapide et très rentable.

Augmentation de la surface d'attaque d'Apple iOS

En 2021, Apple a révélé une fonctionnalité populaire d'iOS qui permettait aux entreprises d'installer des applis en dehors de l'app store et a augmenté accidentellement le vecteur d'attaque des appareils iOS, avec peu de moyens d'arrêter cette exploitation.

Ces profils de configuration iOS offrent aux entreprises un niveau de contrôle granulaire sur les appareils iOS sans avoir à se soumettre à l'examen de l'App Store d'Apple. Une fois l'approbation obtenue, Apple fournit un certificat signé que l'entreprise peut appliquer à l'appareil, ce qui lui permet d'y installer toute application qu'elle a produite en interne. Sauf que cette fonctionnalité a également offert aux utilisateurs finaux la possibilité de charger des applications non approuvées et souvent non sécurisées, sans les protections établies par les OEM, ce qui augmente le risque de vol et d'exploitation des données sur l'appareil.

Selon un rapport d'Apple publié en octobre 2021, les cyber-attaquants abusent de ce programme depuis des années. Ils s'y appuient afin de distribuer des logiciels malveillants, des logiciels espions et d'autres applications malveillantes sur les dispositifs, ciblant ainsi les utilisateurs et les entreprises du monde entier.

« Malgré les contrôles stricts et l'envergure limitée du programme, les cyber-attaquants ont réussi à trouver des moyens illégaux d'y accéder, par exemple en achetant des certificats d'entreprise sur le marché noir... Apple a déployé des efforts considérables afin de renforcer les contrôles du programme et d'ajouter des protections pour les utilisateurs, mais la violation n'a pas cessé ».[52]

« Malgré les contrôles stricts et l'envergure limitée du programme, les cyber-attaquants ont réussi à trouver des moyens illégaux d'y accéder, par exemple en achetant des certificats d'entreprise sur le marché noir... Apple a déployé des efforts considérables afin de renforcer les contrôles du programme et d'ajouter des protections pour les utilisateurs, mais la violation n'a pas cessé ».[52]

Un certificat compromis permet d'activer les paramètres du système et d'installer des certificats signés supplémentaires ou d'autres applications. Des entreprises géantes de médias sociaux à la distribution de logiciels malveillants, les exemples d'abus de ce certificat sont nombreux. Malheureusement, les entreprises ne se rendent compte de ces violations que lorsque le certificat est révoqué. Le fait que cette option soit activée par l'utilisateur représente un risque considérable pour les entreprises.

Pour prendre effet, ces certificats apportent des modifications à la configuration du système, mais les attaques précédentes ont montré combien de données peuvent être consultées, partagées et modifiées en raison de cette violation. Un certificat compromis permettrait d'activer des paramètres à l'échelle du système et d'installer d'autres certificats signés pour d'autres applications non autorisées. Que ce soit des VPN gratuits, des configurations de proxy, des magasins d'applications tiers ou encore des certificats racine, les données peuvent être réacheminées et partagées en clair, ou des données telles que les contacts et les identifiants de messagerie peuvent être partagées avec des parties malveillantes. Rien ne permet de savoir où sont envoyées les données d'un dispositif compromis ni quelles données sont déchiffrées après le chargement d'un profil malveillant.

Les exploits « zero-day » contre les appareils Apple iOS ont augmenté en 2021, avec 11 vulnérabilités exploitées zero-day dans le domaine public. Bien que les logiciels malveillants utilisés contre les appareils iOS ne fassent pas autant parler d'eux, les bogues et les vulnérabilités font l'objet d'une attention particulière en raison de leur impact et de leur base client.

En 2021, 11 vulnérabilités du type « zero-day » ont été révélées, ciblant Apple iOS et Apple WebKit, représentant 19 % de tous les exploits « zero-day » de l'année.

L'éditeur de solutions de sécurité ZecOps a également publié des recherches menées sur WiFiDemon, une vulnérabilité de Wi-Fi à proximité de type « zero-click » sur iOS 14 à iOS 14.4, sans CVE attribué.[53] L'équipe de recherche de ZecOps a révélé que le problème de panne de réseau était en fait une vulnérabilité de type « zero-day » non corrigée. Cette vulnérabilité permettait aux attaquants d'exécuter un code à distance sur le téléphone ou la tablette de la victime sans aucune interaction ni notification à l'utilisateur final. Si la composante « zero-click » de la vulnérabilité a été corrigée avec iOS 14.4, les versions plus récentes du système d'exploitation mobile n'ont pas reçu le correctif avant la publication d'iOS 14.7.

Plus d'applications signifient plus de données à risque

Pour les créateurs d'applications mobiles, avoir une idée incroyable et unique d'application mobile est une chose. Mais qu'en est-il de la sécurité ? La sécurité d'une application mobile est indispensable, surtout que les attaques contre les dispositifs mobiles continuent d'évoluer et de se développer. Les téléphones et les applications mobiles constituent une cible vulnérable, chose dont les cyber-attaquants sont parfaitement conscients.

Pendant le premier trimestre de 2021, près de 3,5 millions d'applications sont disponibles sur le Google Play Store et 2,2 millions d'applications sur l'App Store d'Apple.[54]

Zimperium analyse les vulnérabilités, les logiciels malveillants et le risque général pour des millions d'applications. **Nous avons pu établir que 41 % des applications iOS ne disposent pas d'une protection des données efficace, tandis que 26 % des applications Android sont confrontées au même problème.** Adopter un cryptage ne suffit pas, car de mauvaises mises en œuvre et pratiques de gestion des clés de chiffrement peuvent mettre les données confidentielles et cryptographiques entre les mains de cyber-attaquants.

Nous avons constaté que 40 % des applications Android et 52 % de la population iOS utilisent au moins un algorithme de chiffrement vulnérable. En outre, 81 % des applications Android n'étaient pas suffisamment protégées, contre 72 % pour iOS.

La sécurisation d'une application ne s'arrête pas à sa simple publication. Grâce à des stratégies de rétro-ingénierie, les cyber-attaquants peuvent localiser des failles dans le code de l'application. Il est donc très important de procéder à des tests de pénétration des applications sur une base continue. Cependant, seules 49 % des personnes interrogées réclament effectuer ces tests sur leurs applications mobiles.[55]

Les résultats de Zimperium ont également révélé que **75 % des applications iOS ne répondent pas aux exigences de rétro-ingénierie de l'Open Web Application Security Project (OWASP) Mobile 10-M9 contre 24 % des applications Android.** Lorsque nous les avons interrogées à propos de ce qui représentait le risque le plus important pour les applications mobiles, 49 % des personnes interrogées ont répondu que leurs applications faisaient l'objet d'une rétro-ingénierie.[56]

La confidentialité et la sécurité représentent la première priorité pour les consommateurs et les entreprises. Il est donc primordial que les développeurs renforcent leurs applications mobiles. Pourquoi est-ce essentiel pour les entreprises ? Supposons que 51 % des personnes interrogées réclament avoir installé entre 4 et 8 applications professionnelles sur leurs dispositifs mobiles, tandis que 31 % en ont installé au moins une.[57]

Si ces applis mobiles ne sont pas contrôlées, leurs vulnérabilités peuvent avoir des conséquences tragiques sur les revenus, l'image de la marque et l'activité en général. Le paysage des menaces mobiles évolue constamment au fur et à mesure que de nouvelles vulnérabilités et techniques sont découvertes. Cela exige que les solutions de sécurité soient non seulement complètes, mais aussi rapides et faciles à mettre à jour.

En revanche, selon une enquête récente, 49 % des personnes interrogées affirment que lorsqu'un nouveau risque est découvert, elles ne mettent à jour leurs applications qu'au moment de la prochaine version prévue.[58] En plus, même si une nouvelle version est publiée, les clients peuvent ne pas déployer immédiatement ces mises à jour. Pour les entreprises qui disposent d'un grand nombre d'applications, cela peut signifier que les applications et les données restent exposées pendant 12 à 18 mois, le temps que toute la base des applis soit mise à niveau.

	d'Android	d'iOS
Les applications ne protègent pas les données	26 %	41 %
Un cryptage vulnérable	40 %	52 %
Les applications ne sont pas protégées par un code	81 %	72 %

Risques liés aux applications mobiles par secteur d'activité

Comme indiqué, une vulnérabilité courante est l'exposition des données des utilisateurs finaux. Comme les cyber-attaquants continuent d'exploiter les applications mobiles, des facteurs de conformité et de réglementation entrent en jeu dans plusieurs secteurs :

- **Santé.** Si des données relatives à la santé tombent entre de mauvaises mains, les acteurs de la santé sont soumis à des amendes et à des sanctions dans le cadre de la loi américaine sur l'assurance maladie (Health Insurance Portability and Accountability Act - HIPAA).
- **Services financiers.** Les établissements financiers sont passibles d'amendes en cas de violation de données et de manquement à la conformité. En outre, les violations ont explosé depuis l'apparition de la pandémie COVID-19.[59]
- **Vente au détail.** De mauvaises pratiques de sécurité peuvent exposer les détaillants à des amendes pour violation de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Ces entreprises pourraient également être confrontées à des frais de justice et à des pénalités si les consommateurs font objet d'une cyberattaque.

Des entreprises des industries du monde entier doivent se conformer aux réglementations régionales pertinentes en matière de protection de la vie privée, notamment le règlement général sur la protection des données (RGPD) de l'Union européenne et la loi californienne sur la protection de la vie privée des consommateurs (CCPA). Ces lois offrent aux consommateurs un cadre juridique bien déterminé en matière de gestion et d'utilisation de leurs données. En outre, elles s'appliquent à toutes les entreprises qui gèrent des informations personnelles identifiables (PII) appartenant à des personnes dans des régions régies par ces lois. Ces règles s'appliquent donc aux applications financières, de vente au détail, de soins de santé et de l'art de vivre. En cas de non-conformité, une entreprise peut se voir infliger des amendes et faire l'objet de recours collectifs. Cela comprend les cas où les données des clients font l'objet d'une violation ou d'une cyberattaque à cause de l'absence de mesures de sécurité adéquates.

	d'Android	iOS
Applications financières		
Manquements à la protection des données	**49.9 %**	**41.2 %**
Utiliser un chiffrement vulnérable Algorithmes	**79.8 %**	**42.3 %**
Manquements à la protection du code	**64.4 %**	**71.9 %**
Applications de soins de santé		
Manquements à la protection des données	**45.4 %**	**36.6 %**
Utiliser un chiffrement vulnérable Algorithmes	**72.4 %**	**41.4 %**
Manquements à la protection du code	**82.4 %**	**72.2 %**
Applications pour le commerce de détail		
Manquements à la protection des données	**61.1 %**	**48.0 %**
Utiliser un chiffrement vulnérable Algorithmes	**80.4 %**	**54.0 %**
Manquements à la protection du code	**69.7 %**	**82.34 %**
Applications sur l'art de vivre		
Manquements à la protection des données	**54.6 %**	**44.5 %**
Utiliser un chiffrement vulnérable Algorithmes	**77.4 %**	**49.0 %**
Manquements à la protection du code	**74.8 %**	**74.0 %**

Ressources :

1. Pew Research. (2021). Fiches techniques des téléphones mobiles. Pew Research Center. https://www.pewresearch.org/internet/fact-sheet/mobile/

Les risques posés par un stockage Cloud défectueux.

Plusieurs applications s'appuient sur le stockage Cloud afin de remplir leurs fonctions. Les développeurs peuvent utiliser le cloud pour stocker des fichiers de configuration, des fichiers multimédias et d'autres ressources. Configurer le stockage Cloud sur une application est un jeu d'enfant. Toutefois, mettre en place les configurations de sécurité nécessaires n'est souvent pas considérée comme une priorité ou est complètement négligée. Cela constitue un risque considérable : En analysant les applications, les cyber-attaquants peuvent déterminer si une application utilise le stockage Cloud et, surtout, si des mesures de sécurité protègent ce stockage.

Il convient de noter que dans certains cas, les développeurs peuvent travailler avec des exemples de code ou des bibliothèques qui accèdent au stockage Cloud et ne pas être conscients de ces corrélations. Ainsi, ils peuvent ne pas connaître les risques potentiels, et encore moins y remédier.

En accédant au stockage Cloud, un cyberattaquant peut extraire des informations sensibles, telles que des informations sur la santé, des fichiers de configuration, des informations personnelles identifiables (PII), et bien plus encore. Dans au moins un des cas, un pirate a pu prendre le contrôle de toute l'infrastructure Cloud d'un développeur d'applications.

	d'Android	iOS
Manquements à la protection des données	**18.85 %**	**8.19 %**
Nombre total d'applications analysées (depuis janvier 2020)	**232760**	**325200**
Nombre total d'applications avec une configuration Cloud défectueuse.	**43892**	**26639**

Pourquoi MTD est important pour XDR (SentinelOne)

Rick Bosworth, directeur du marketing produit, SentinelOne

7 sur 10

organisations déclarent que les dispositifs mobiles sont indispensables pour leur activité

1 sur 3

de type « zero-day » visait les appareils iOS et Android

Les dispositifs mobiles sont désormais une catégorie d'actifs à protéger en urgence. Le télétravail et les politiques de BYOD sont désormais la règle, et non plus l'exception. En effet, **7 sur 10 organisations déclarent que les dispositifs mobiles sont indispensables pour leur activité.**[60] Ce même pourcentage d'employés utilise ses dispositifs mobiles personnels pour accéder aux ressources de l'entreprise : listes de clients, stratégies de compte, modèles financiers, etc. Paradoxalement, les dispositifs mobiles représentent le principal moyen (c'est-à-dire via une application 2FA) de vérifier l'identité et la confiance lors de l'accès à ces ressources. Cela en fait une cible de choix dans la surface d'attaque de votre entreprise, ce qui explique pourquoi la lutte contre **les menaces mobiles est un élément essentiel d'une pile de sécurité XDR.**

Il existe une idée aussi fausse que répandue qui veut que les systèmes d'exploitation mobiles sont sécurisés de par leur conception. Alors que les experts de la sécurité sont conscients que cela est faux, ils doivent encore convaincre une hiérarchie sceptique - vous savez, ceux qui tiennent les cordons de la bourse - de la nécessité d'agir. Les exploits de type « zero-day », les applications malveillantes, les comportements à risque des utilisateurs et les attaques de phishing sont des menaces bien réelles pour l'entreprise mobile. L'équipe Project Zero de Google indique qu'en 2021, **1 attaque sur 3 de type « zero-day » visait les appareils iOS et Android ;** par rapport à 1 sur 10 l'année précédente. Des applications malveillantes sont téléchargées dans les magasins d'applications et échappent aux responsables de la sécurité des systèmes informatiques. Une application 2FA malveillante a été supprimée du Google Play Store en février 2022, après avoir été téléchargée 10 000 fois.[61] Les utilisateurs débrident leurs dispositifs et chargent des applications en parallèle. Un point d'accès non autorisé positionné dans des zones très fréquentées comme les cafés intercepte le trafic. Et puis, bien sûr, il existe le spectre omniprésent des attaques par phishing (hameçonnage par e-mail) et smishing (hameçonnage par SMS).

La défense contre les menaces mobiles (MTD) est particulièrement dédiée à la prévention, la détection et la réponse aux menaces pour les dispositifs mobiles fonctionnant sur iOS, Android et même Chrome OS. La plupart des entreprises ont déjà implémenté un système de gestion des appareils mobiles (MDM), mais un MDM n'est pas synonyme de sécurité. Il s'agit d'une simple gestion : administration et contrôle basique. Considérer un MDM en tant qu'une solution de sécurité, c'est comme dire qu'un bricoleur est un plombier : certes, ils se chevauchent un peu, mais vous savez qui appeler lorsqu'un gel fait éclater vos tuyaux. Un MDM est parfait pour la gestion : suivre un portable, le verrouiller, le supprimer. Par contre, le MTD protège toute entreprise contre les attaques de phishing, les logiciels malveillants et les exploits de réseau tels que les attaques de type « man-in-the-middle » (MITM). Un MTD et un MDM sont des solutions complémentaires, qui se complètent mutuellement.

La sécurisation des dispositifs mobiles reste une étape essentielle dans n'importe quelle stratégie XDR

Les dispositifs mobiles ne constituent qu'une des nombreuses surfaces d'attaque comme les points d'extrémité d'utilisateur, les charges applicatives Cloud, IoT, les e-mails, identité, etc. Le XDR est un processus en 3 étapes, à la vitesse de la machine : (1) charger les données qui proviennent de ces multiples surfaces d'attaque, (2) automatiser leur analyse et leur corrélation, en recherchant des informations, et (3) prescrire et potentiellement automatiser une action de réponse sur la base des informations collectées. Il existe de bonnes raisons d'intégrer une solution MTD dans votre système de sécurité. **La simple détection d'une attaque sur un utilisateur de dispositif mobile, même si elle est bloquée par une solution MTD, peut constituer une information puissante et exploitable pour un SOC.**

Prenons l'exemple d'une cible de grande valeur, peut-être une PDG, qui se fait conduire à l'aéroport. Elle reçoit des appels et consulte ses e-mails, dont l'un provient du directeur général divisionnaire avec un lien vers les informations dont elle doit disposer. Bien sûr, il s'agit d'une attaque de type spear phishing minutieusement conçue. Avec la solution MTD, l'attaque sur son téléphone mobile est immédiatement détectée grâce à une analyse comportementale, bloquée, et le SOC est alerté. Grâce à sa visibilité complète croisée, l'attaque est immédiatement identifiée en tant que phishing réussi de l'e-mail du directeur général de la division. Dans un environnement XDR, cette confirmation déclenche automatiquement une réinitialisation de leurs identifiants de messagerie. Le SOC appelle donc la PDG pour lui assurer que non seulement elle est en sécurité, mais aussi qu'il a identifié la cause du problème et que la situation est maîtrisée, tout cela en 2 minutes... voire moins. Globalement, le SOC est alerté d'une campagne active visant des profils du top management.

Conscients qu'un dispositif mobile contient des logiciels malveillants, nous pouvons en interdire l'accès, mais aussi renseigner le SOC sur les compétences des utilisateurs en matière de sécurité.

Un modèle XDR adéquat affectera automatiquement un profil plus risqué à cet utilisateur, et pourra même utiliser un outil de gestion de droits afin de limiter l'accès autant que possible, atténuant ainsi le risque pour l'organisation. Il peut également forcer l'utilisateur à utiliser plus fréquemment le système 2FA jusqu'à ce que le risque diminue, par exemple en supprimant l'application malveillante.

Le fonctionnement de l'entreprise a changé radicalement, accéléré par les événements de ces deux dernières années. **Avec un nombre considérable d'employés qui se développent en dehors du périmètre de l'entreprise, nos stratégies de sécurité changent constamment pour relever le défi de garder nos actifs à la fois disponibles et confidentiels. La lutte contre les menaces liées aux mobiles est indispensable au succès de notre sécurité XDR uniforme et multiplateforme.**

Établir la confiance zéro des dispositifs mobiles dans les architectures de sécurité

Loren Russon, vice-président de la gestion des produits, Ping Identity

L'évolution des employés vers des environnements de travail plus virtuels et mobiles, à cause de la pandémie, a poussé les grandes entreprises à s'éloigner des approches de sécurité conventionnelles, statiques et basées sur le périmètre. Ce changement a renforcé chez les entreprises l'urgence d'investir dans des capacités de sécurité basées sur l'identité, dans le cadre d'une stratégie visant à implémenter des modèles de sécurité de type « zero trust » pour leur personnel décentralisé.

Le concept de sécurité « zero trust » – souvent résumé par l'injonction ***« Never Trust ; Always Verify »*** (ne jamais faire confiance, toujours vérifier) – considère tout le monde comme une menace potentielle et empêche l'accès aux données et aux ressources jusqu'à ce qu'il soit vérifié. Une transformation de type « zero trust » promet de relever de nouveaux défis afin de mieux protéger les employés, les clients et les opérations contre des cyber-menaces en constante évolution, tout en améliorant la conformité et la productivité des employés. L'objectif étant d'offrir une expérience en ligne de qualité supérieure aux employés et aux clients, quel que soit l'endroit dans lequel le travail est effectué.

Mais avec la prolifération rapide des dispositifs mobiles qui accèdent aux actifs de l'entreprise, les responsables de la sécurité ont besoin de meilleurs moyens pour établir des relations de confiance avec les dispositifs présents sur le réseau. Afin d'assurer aux employés un accès sécurisé aux données dont ils ont besoin sur les dispositifs qu'ils utilisent fréquemment, la solution « zero trust » doit s'accompagner d'une défense avancée contre les menaces mobiles.

C'est à ce niveau que le partenariat entre Ping Identity et Zimperium se distingue. Nos deux entreprises travaillent en étroite collaboration afin d'améliorer les modèles de sécurité « zero trust » en fournissant des données de stratégie de risques mobiles. La solution de sécurité Ping Identity/Zimperium permet aux grandes entreprises d'établir des relations plus fiables avec tous les composants du réseau : utilisateurs, dispositifs, applications, transactions, API, etc.

Créer des relations de confiance

en se basant sur l'identité reste la première étape cruciale vers la construction d'une architecture « zero trust », car on ne peut pas faire confiance à ce que l'on ne peut pas identifier. La sécurité basée sur l'identité repose sur l'idée que tous les utilisateurs et dispositifs doivent être authentifiés avant de pouvoir accéder à des ressources ou des données sensibles. Actuellement, cela peut sembler évident, mais il s'agit d'un changement de mentalité par rapport aux anciennes approches de sécurité, où l'on faisait confiance aux utilisateurs une fois qu'ils étaient sur le réseau de l'entreprise.

Ping Identity fournit une plateforme basée sur l'identité et une suite sous-jacente de prestations qui aident les équipes de sécurité à implémenter des contrôles et des politiques de sécurité plus robustes sur pratiquement tout utilisateur, appareil ou autre élément du réseau, que ces éléments fonctionnent sur le cloud, que ce dernier soit hybride ou sur site.

Les utilisateurs, par exemple, doivent être authentifiés de manière intelligente. Ils doivent prouver leur identité à l'aide de plusieurs moyens, ce que l'on appelle également l'authentification multifactorielle (multi-factor authentication ou MFA). Cet ensemble de facteurs se décline souvent en indices que l'utilisateur connaît, comme un mot de passe, un dispositif qu'il possède, comme un smartphone, voire un facteur biométrique comme la reconnaissance faciale ou encore l'empreinte digitale. Les différents niveaux d'activités et de risques de sécurité peuvent nécessiter l'utilisation de différents niveaux d'authentification multifactorielle.

La seule authentification des utilisateurs n'est pas suffisante pour atteindre le niveau « zero trust ». Même les utilisateurs authentifiés correctement peuvent être victimes de problèmes liés à l'utilisation de dispositifs mobiles piratés. L'authentification de ces terminaux est indispensable pour établir des mécanismes de protection efficaces contre les menaces liées aux dispositifs mobiles, car les appareils compromis peuvent être exploités par des menaces comme les ransomware, les logiciels espions et les chevaux de Troie.

Mais la sécurité des dispositifs mobiles reste souvent négligée au détriment de la commodité. Dès lors, ces terminaux mobiles sont exposés à un plusieurs vecteurs d'attaque sur lesquels les entreprises n'ont aucune visibilité, et encore moins les moyens de les prévenir, ce qui crée des failles dans leur architecture « zero trust ». Par ailleurs, même s'il a été prouvé qu'un dispositif mobile n'a pas été manipulé, il peut manquer un correctif de sécurité qui risque de compromettre la stratégie de la sécurité de l'entreprise.

Zimperium et Ping Identity collaborent ensemble afin d'améliorer la gestion des identités des dispositifs mobiles et les contrôles d'accès, en intégrant tous les terminaux mobiles dans un périmètre de sécurité. Zimperium fournit une protection en temps réel, sur le dispositif, basée sur l'intelligence artificielle, contre les menaces liées à Android, iOS et Chromebooks. Cette intelligence en temps réel, à son tour, améliore la plate-forme de Ping Identity avec une plus grande visibilité de la sécurité, du contrôle d'accès et de la sécurité des dispositifs requis dans le but de sécuriser les terminaux mobiles qui appartiennent à l'entreprise. Les équipes chargées de la sécurité peuvent mieux comprendre leur stratégie de risque et renforcer leur sécurité mobile contre les attaques qui ciblent leurs dispositifs ou leur réseau, de type phishing ou applications malveillantes.

Cette technologie surveille constamment les dispositifs et diffuse des alertes précises et exploitables qui indiquent aux équipes de sécurité comment résoudre les problèmes de sécurité ou de conformité. Grâce à la détection, à la notification et à la réponse aux menaces mobiles en temps réel proposées par Zimperium, les équipes de sécurité qui utilisent la plateforme Ping Identity peuvent s'assurer que la couverture des terminaux mobiles fait partie intégrante de leur stratégie de sécurité « zero trust ».

L'identité est le nouveau périmètre que les entreprises doivent sécuriser, et la meilleure façon de procéder efficacement est d'utiliser une approche de type « zero trust » qui unifie la résistance aux menaces mobiles avec la puissance d'authentification.

L'intégration de la plateforme IAM de Ping Identity avec Zimperium simplifiera l'implémentation de la stratégie « zero trust » pour les équipes de sécurité afin de fournir une expérience utilisateur plus transparente et plus sécurisée.

Une plus grande surface d'attaque pour les smartphones

Julian Durand, vice-président de la gestion des produits, Intertrust

Le nombre de smartphones mobiles connectés à l'internet a progressé à un rythme rapide. À mesure qu'ils deviennent indispensables à notre vie personnelle et professionnelle, leur technologie et leurs applications sont devenues plus complexes et plus connectées et, par conséquent, constituent davantage une cible de choix pour les cyber-attaquants. Mais afin de mieux se préparer aux attaques actuelles et futures, nous devons comprendre la surface d'attaque des smartphones mobiles et explorer les trois niveaux principaux de maturité que sont la détection, la protection et la défense afin d'atténuer les risques liés à la surface d'attaque.

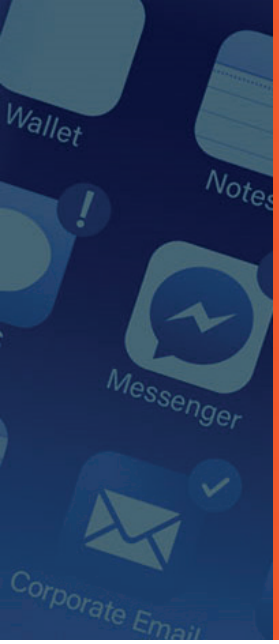
Les expéditions annuelles de smartphones à travers le monde sont passées de 173,5 millions en 2009 à 1,43 milliard en 2022, avec un taux de croissance annuel de plus de 10 % sur 23 ans.[62] Ce taux aurait été encore plus élevé si l'approvisionnement en semi-conducteurs n'avait pas été affectée par la pandémie.

De nos jours, le nombre de téléphones mobiles connectés à Internet dépasse légèrement la population mondiale de 7,6 milliards d'habitants.

Même si la densité varie des Maldives (246 connexions mobiles pour 100 habitants) à des pays où elle reste très minime, comme Cuba et la Corée du Nord (12 connexions pour 100 habitants), la vérité est que les téléphones mobiles sont devenus omniprésents .[63]

Afin de mieux comprendre les menaces de cybersécurité qui pèsent sur ces dispositifs omniprésents, le National Institute of Standards and Technology (NIST) des États-Unis propose une liste des menaces liées aux dispositifs mobiles.[64] Il s'agit d'un cadre utile pour recenser la croissance de la surface d'attaque de ces systèmes, notamment lorsqu'elle est considérée sous l'angle de l'identification et de l'atténuation des cyber-risques de l'entreprise. Nous verrons plus bas que la surface d'attaque a augmenté de façon non linéaire, voire exponentielle, en raison de la croissance spectaculaire de chaque élément de complexité, du nombre de connexions et du caractère central de ces dispositifs dans nos vies. Pris ensemble, ces éléments représentent une croissance composée, chacun d'entre eux aggravant le niveau de menace suivant et élargissant davantage la surface d'attaque globale associée à la mobilité des entreprises.

De nos jours, la pile technique d'un smartphone commence par les puces qui fournissent les performances des applications et des communications. Par exemple, le flagship Snapdragon 8 Gen1 de Qualcomm nous donne une idée des caractéristiques des smartphones de 2022. On trouve notamment un processeur multicœur de 3 GHz, un moteur d'IA haute performance, un modem 5G avec un débit de 10 Gbps, un moteur de jeu de classe console, un module de localisation avancé prenant en charge 6 systèmes de satellites GNSS (système global de navigation par satellite) multi-constellations distincts, des modules avancés de traitement de la caméra, de la vidéo et des capteurs, ainsi que des modems Wi-Fi, Bluetooth et NFC de dernier cri, le tout étant construit sur un nœud de processus de 4 nm .[65]



Tout ce matériel requiert un micrologiciel pour accéder à l'autotest de mise sous tension (POST), au chargeur de démarrage initial, ainsi qu'aux pilotes pour chacun de ces noyaux technologiques.

Un système d'exploitation mobile comme iOS ou Android s'appuie sur le micrologiciel. Android, le système d'exploitation pour téléphones mobiles le plus répandu au monde en termes de volume, a récemment publié sa 11e version. La mise à jour d'un smartphone nécessite un téléchargement d'environ 2 Go.[66] Cela représente plusieurs logiciels avec un grand nombre de nouvelles fonctionnalités, chacune représentant un niveau élevé de complexité et des opportunités potentielles pour de multiples nouvelles menaces. La dimension du système d'exploitation, elle seule, contribue de manière significative à l'augmentation rapide de la surface d'attaque liée aux dispositifs mobiles.

Et que serait un smartphone aujourd'hui sans les téléchargements d'applications ?

Les applications constituent une source de menaces encore plus vaste et plus hétérogène, car ces dernières peuvent contenir des logiciels malveillants, des vulnérabilités ou souvent les deux.

Un smartphone moderne offre aujourd'hui plusieurs procédés de connexion, chacune d'entre elles pouvant offrir à un cyber-attaquant un moyen d'attaque direct. Il s'agit notamment de :

- Un modem cellulaire qui se connecte automatiquement à une antenne-relais de téléphonie mobile afin d'offrir un meilleur signal. Les stations indésirables peuvent être réglées et centrées sur un dispositif cible afin de donner l'impression qu'il s'agit de la station à laquelle le téléphone doit se connecter.
- Le Bluetooth a été largement critiqué pour ses failles en matière de sécurité. Les attaques liées au Bluetooth incluent :
  - Bluejacking - envoi de messages malveillants non sollicités sur le téléphone d'un individu
  - Bluesnarfing - vol d'informations
  - Bluebugging - exécution de code à distance et prise de contrôle du dispositif
- Le Wi-Fi dispose de plusieurs protocoles de sécurité, la mais la plupart sont défaillants et inefficaces. Même si la couche réseau est sécurisée, un smartphone se connectera souvent à des points d'accès dont la fiabilité est douteuse dans des lieux publics tels que les cafés, les hôtels et les aéroports. Même si la liaison est protégée, il semble presque banal pour un point d'accès contrôlé par un cyberattaquant d'espionner, d'intercepter et de modifier les communications.

L'architecture du réseau « Zero Trust » (ZTNA) est une approche, indépendante de l'état de la sécurité du réseau, qui vise a assurer l'intégrité et la confidentialité des communications. Intertrust propose une solution basée sur ZTNA qui apporte une architecture de bout en bout, de l'appareil mobile au cloud, sur laquelle les entreprises peuvent s'appuyer afin de mieux protéger les données sensibles.

Les smartphones sont de petits ordinateurs mobiles polyvalents qui sont personnalisés grâce à des applications. Ces applications sont téléchargées à partir de magasins d'applications, et donc si vous faites confiance au magasin d'applications, vous pouvez généralement faire confiance aux applications qu'il distribue.

Cela peut être poussé à l'extrême. La guerre actuelle entre le plus grand fabricant de jeux vidéo du monde et l'une des premières compagnes technologiques du monde en est un exemple. Epic Games a déposé une plainte contre Apple pour son abus de position dominante de l'écosystème des smartphones Apple, empêchant ses utilisateurs de recourir à un magasin d'applications concurrent. Epic Games a intenté un procès parce qu'elle estime que la commission de 30 % exigée par Apple pour les applications rend excessivement chers les jeux freemium comme Fortnite. Apple prétend que le problème est lié à la cyber-sécurité, alors que le problème est bien plus complexe. Mais elle souligne la nécessité d'examiner les applications et de procéder à leur signature cryptographique pour en garantir l'intégrité et l'authenticité.

- Les entreprises développent de plus en plus leurs propres applications qu'elles vérifient elles-mêmes et signent de manière cryptographique afin de garantir leur intégrité et leur authenticité. Si c'est bien fait, c'est un moyen sûr d'ajouter des fonctionnalités aux employés d'une entreprise. Le cas échéant, ceci constituera un autre vecteur d'attaques.

- Quoi qu'il en soit, les applications développées par les entreprises constituent un autre élément de la surface d'attaque mobile dans l'entreprise en croissance rapide.

Smartphone en tant que hub IoT

Étant omniprésents et dotés d'importantes fonctionnalités matérielles de cybersécurité, les smartphones sont souvent utilisés pour gérer les appareils et réseaux IoT. Même les voitures peuvent être démarrées et arrêtées par votre téléphone.

Ce confort est apprécié tant par les clients que par les entreprises. Mais ceci augmente considérablement la surface d'attaque disponible car plusieurs appareils et réseaux IoT, notamment ceux utilisés par les clients, ne disposent pas des mêmes fonctionnalités de cyber-sécurité sophistiquées que celles utilisées sur les smartphones modernes. Par conséquent, les cyber-attaquants peuvent contrôler des dispositifs, des hubs et des passerelles et attendre que les dispositifs vulnérables se connectent. Ainsi, les logiciels malveillants qui ont propagé le botnet Mozi se sont répandus si rapidement dans le monde.[67]

Les logiciels malveillants comme Mozi peuvent attendre. Lorsqu'un smartphone présentant une vulnérabilité se connecte à un hub IoT compromis, ils lancent une attaque. Si le smartphone n'a pas été mis à jour ou n'a pas utilisé d'autres moyens de défense, il pourrait être infecté.

Atténuation des menaces - les trois phases de la maturité de la sécurité

1. Détecter une menace

- Contrôler un smartphone
- Les algorithmes de détection par apprentissage automatique sont indispensables car les capacités de code polymorphe utilisées par de nombreux concepteurs de logiciels malveillants échappent aux contrôles de signatures III. Envoyer des alertes lorsqu'on soupçonne qu'un appareil est attaqué ou contient des vulnérabilités connues.

2. Protéger le smartphone

- En sus de ses capacités de détection des menaces, le dispositif doit disposer de plus de fonctionnalités automatisées de cybersécurité, comme le téléchargement et l'application automatiques des derniers correctifs de cyber-sécurité authentifiés
- Protection contre les messages de phishing grâce aux techniques de sandboxing « bac à sable »
- Les fonctionnalités VPN sur demande pour protéger les données contre les passerelles et (surtout) les routeurs Wi-Fi non fiables.
- Contrôles d'accès pour cloisonner les informations et processus sensibles
- Pour les entreprises, il est surtout important de renforcer l'application des politiques de sécurité afin de s'assurer que les risques de cyber-sécurité sont correctement adressés

3. Défense

- Outre la détection et la protection, le système de défense consiste à intensifier les actions défensives de l'entreprise.
- Ce système comprend des mécanismes de cyber-sécurité d'exigence très particulière, une sécurité web centralisée pour les appareils et les serveurs, en plus des solutions de gestion unifiée des identités et des accès (IAM), de prévention des pertes de données (DLP) et de courtier de sécurité d'accès au cloud (CASB).

Cybersécurité des données de bout en bout

De plus, l'utilisation d'une architecture « zero trust » dans le réseau reste primordiale, notamment pour les entreprises et les cas d'utilisation liés à l'IdO, en raison de l'existence de nombreuses techniques d'attaque très performantes axées sur le réseau. Utiliser un service « device-to-cloud » (appareil-à-cloud) afin d'assurer la sécurité des données lorsqu'elles traversent les réseaux, qu'elles soient de confiance ou non. Cela permettra de renforcer la défense, puisque le service comprend l'authentification du dispositif, ce qui contribue à prévenir les attaques.

La montée en puissance de l'informatique mobile hyperconnectée a offert à la population mondiale un accès sans précédent à des communications peu coûteuses, à la connaissance et à des puissances de calcul de plus en plus sophistiqués. La grande portée et le caractère sophistiqué de ces plateformes de téléphonie mobile nous ont également mis en danger, en particulier dans les entreprises qui gèrent des données sensibles. La reconnaissance de ce paysage de menaces est la première étape, tandis que la mise au point de processus de détection, de protection et de défense est encore plus importante que jamais. Heureusement, nous disposons des outils et de l'expertise nécessaires pour réduire les surfaces d'attaque et minimiser l'exposition aux risques. Mais cela implique un engagement, des outils et un effort concerté qui doit être mené par la direction générale.

Les risques accrus des outils mobiles de productivité pour les entreprises

JT Keating, vice-président de la stratégie produit, Zimperium

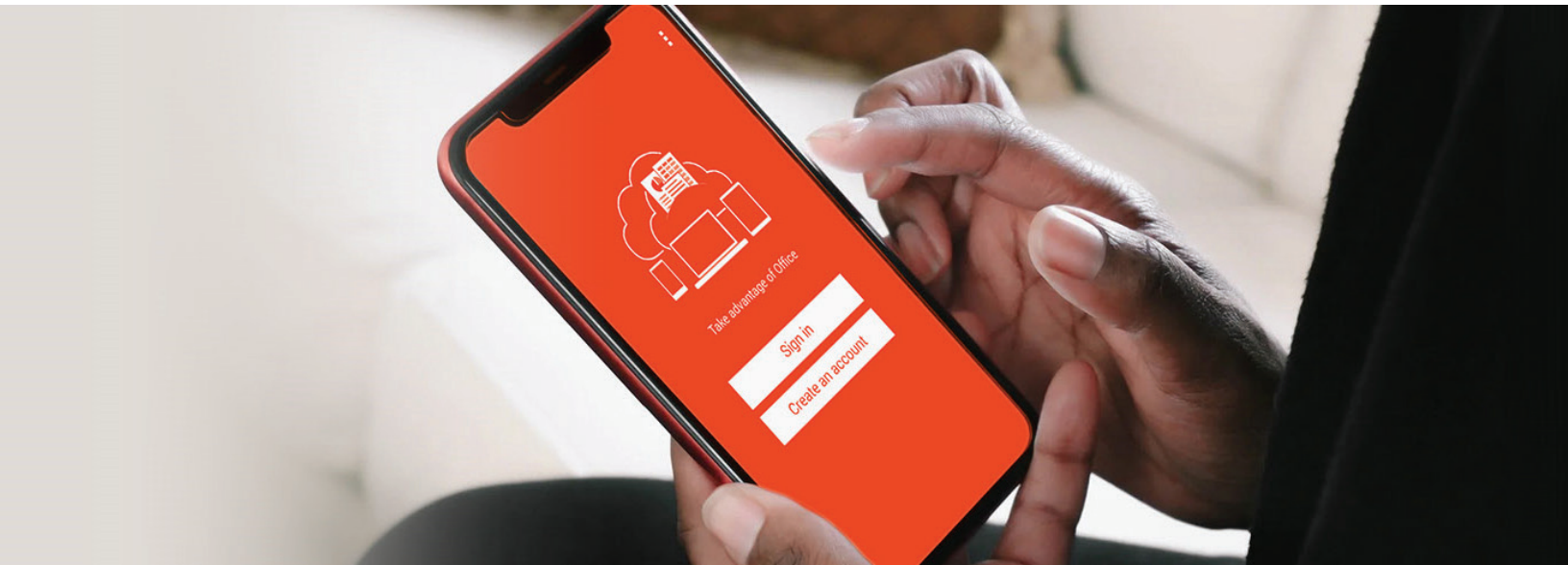
La pandémie de COVID-19 a soulevé chez les employés une tendance au télétravail, ce qui a considérablement modifié la façon dont les entreprises exercent leurs activités dans ce que l'on appelle désormais « le milieu de travail d'aujourd'hui ». Au début du confinement, les employés ont rapidement rangé leurs ordinateurs portables, leurs écrans et leurs autres dispositifs pour commencer leur nouvelle aventure de télétravail. Alors que le télétravail était considéré comme un avantage supplémentaire avant 2020, il fait désormais partie du mode de vie de la plupart des gens. Parallèlement, les dispositifs BYOD ont considérablement augmenté, les employeurs permettant l'utilisation d'outils de productivité sur des dispositifs mobiles personnels afin de s'assurer que leurs employés décentralisés disposent des outils et de la connectivité nécessaires pour être tout aussi, voire plus, productifs dans leur nouvel espace de travail.

Depuis lors, les dispositifs mobiles sont devenus des outils de productivité indispensables dans le milieu de travail moderne, offrant à leurs utilisateurs le même niveau d'accès aux applications et aux données que les anciens terminaux classiques. En fait, 84 % des experts en sécurité ayant répondu à un récent sondage mené par Zimperium ont déclaré avoir activé Microsoft Office 365 sur les appareils mobiles. [68]

84 % des experts en sécurité ayant répondu à un récent sondage mené par Zimperium ont déclaré avoir activé Microsoft Office 365 sur les appareils mobiles

En permettant l'utilisation d'outils de productivité comme Office 365, autorisant les dispositifs approuvés par une entreprise à accéder au contenu d'Office 365, comme les e-mails, les messages de Teams, les documents, et plus encore, améliorant ainsi les communications et la collaboration entre les équipes. Ces applications Cloud de productivité permettent aux télétravailleurs de se détacher éventuellement de leur bureau et d'être productifs à distance. Si les administrateurs informatiques utilisent la gestion des appareils mobiles (MDM) pour avoir un niveau de contrôle plus élevé sur les dispositifs qui accèdent à des applications comme Word, Excel, PowerPoint, Outlook et le contenu de OneDrive, ce niveau d'accès n'est pas sans risque.

Si l'année 2020 a prouvé quelque chose, c'est que les cybercriminels ont profité de la pandémie de COVID-19, en plus de l'expansion des télétravailleurs. Nous ne sommes pas surpris que les vulnérabilités mobiles aient augmenté de 50 % depuis la pandémie. Les experts en sécurité s'accordent sur une vulnérabilité courante : depuis l'apogée de la pandémie, les dispositifs BYOD ont multiplié la surface d'attaque des entreprises de toutes tailles. Alors que les équipes se précipitent pour mettre en place des équipes de télétravailleurs, certaines ont dû prioriser la mise en place d'une équipe distribuée plutôt que la sécurisation de tous les dispositifs de la stratégie BYOD, notamment leurs propres points terminaux.



36 % des personnes interrogées de Zimperium ont déclaré avoir terminé l'implémentation des solutions de sécurité pour protéger Office 365 sur les dispositifs mobiles, alors que 38 % sont encore en train de les implémenter.[69] Commentant ce fossé, Eric Green, ancien responsable mondial de la sécurité mobile chez HSBC, a déclaré : **« Étant donné que Office 365 sur mobile donne le même accès qui n'était autrefois fourni aux utilisateurs que sur des ordinateurs de bureau ou portables entièrement sécurisés, il serait donc irresponsable de ne pas sécuriser les données sur les dispositifs mobiles également ».**

Dans le contexte actuel marqué par de multiples menaces, les dispositifs mobiles doivent être très bien équipés afin de se prémunir contre l'ensemble des risques et des attaques qui ciblent les dispositifs et les réseaux, comme le phishing et les applications malveillantes.

La protection de l'entreprise contre les attaques qui ciblent les dispositifs mobiles dépasse de loin les simples contrôles de conformité MDM ou la restriction de l'appareil, empêchant les employés de télécharger certaines applications. Par conséquent, la restriction excessive des dispositifs par l'intermédiaire des politiques de gestion supplémentaires peut être l'opposé de l'amélioration de la productivité.

Afin de sécuriser l'accès mobile à Office 365 et améliorer l'expérience de l'utilisateur final, les entreprises doivent réduire les restrictions de sécurité grâce à une solution de défense contre les menaces liées aux mobiles. Les MTD peuvent détecter les menaces, prévenir les intrusions, et fournir les fonctionnalités essentielles d'attestation de risque et de notation des dispositifs, indispensables pour les modèles Zero Trust et les stratégies d'accès conditionnel.

Même si elles doivent choisir entre un MDM et un MTD, les entreprises peuvent tirer parti des deux pour combler les failles en matière de couverture, de données et de sécurité. La confidentialité est un maillon principal de la sécurisation des dispositifs BYOD, elle contribue à une adoption plus faible que prévue de la sécurité mobile, mais l'utilisation des stratégies MDM et MTD permet à l'entreprise d'assouplir les restrictions. Les travailleurs sont réticents à accorder un accès total à leurs dispositifs BYOD pour des raisons de fiabilité et pour éviter que les équipes informatiques des entreprises n'aient accès à leurs données personnelles comme les photos, le répertoire et les messages.

Il semblerait prudent de veiller à ce que ces dispositifs mobiles ne puissent être facilement compromis. En cas de violation, la réaction à l'incident et les efforts de récupération qui en résultent peuvent être coûteux et entraîner des sanctions réglementaires sévères si des informations personnelles identifiables sont exposées.

Rares sont ceux qui contesteront. De nos jours, il existe un large consensus au sein de l'industrie quant à la sécurisation des dispositifs mobiles. Toutefois, l'efficacité de ces systèmes de défense contre les menaces mobiles reste à déterminer. Ils seront étudiés et testés par les cybercriminels qui perçoivent correctement les dispositifs mobiles comme étant le maillon faible de la chaîne de sécurité.

Conclusion

En 2021, la surface d'attaque des mobiles a fait l'objet d'attaques et d'exploitations complexes, entretenues par des cybercriminels qui explorent une plus grande surface d'attaque et davantage d'opportunités offertes par les terminaux mobiles. Nous avons été témoins des attaques informatiques contre les dispositifs utilisés par les élites politiques et administratives, les chefs d'entreprise, les journalistes, etc. Des applications très répandues dans le monde ont également été exploitées par des cyber-attaquants, exposant les données sensibles des clients et des investisseurs, etc. À l'horizon de 2022, ces exploitations et attaques mobiles continueront de se produire, car la dépendance aux dispositifs mobiles ne cesse d'augmenter.

Par le passé, l'accès aux données mobiles a souvent jeté une ombre sur le besoin de mesures de sécurité avancées, mais l'arrivée de 2021 a prouvé que les risques de sécurité mobile pour les entreprises, les gouvernements et les personnes sont plus élevés que jamais. Les techniques et les capacités des cyber-attaquants sont affinées en permanence, ce qui lève le voile sur la confiance dans les appareils mobiles. Leurs objectifs vont du crime financier à l'exfiltration de données, en passant par l'exploitation de la faible sécurité des systèmes mobiles. Avec chaque découverte de nouvelle vulnérabilité, les cyber-attaquants continueront à menacer davantage d'entreprises et de systèmes critiques par l'intermédiaire de ces exploits.

Il est essentiel pour les entreprises de ne pas oublier l'importance stratégique de la sécurité mobile, entourant les dispositifs et les applications connectés à leurs systèmes essentiels. Le monde mobile devient de plus en plus complexe, avec de nouvelles applications, fonctions et capacités introduites chaque année. Il est important de comprendre que la sécurité, comme les dispositifs, est une cible en constante évolution. Il faut comprendre les risques encourus et leur impact potentiel, et prendre une décision réfléchie avec les bons outils et ressources en place.

Le moment est venu pour que les terminaux et les applications mobiles fassent l'objet des mêmes attentes en matière de sécurité que leurs homologues classiques. Comme les écosystèmes

Alors que la menace mobile ne cesse d'évoluer et de s'amplifier, les outils et les capacités de sécurité de Zimperium, leader de l'industrie, permettent de répondre aux attentes des utilisateurs.

It is essential for enterprises not to lose sight of the strategic importance of comprehensive mobile security surrounding the devices and applications connected to their critical systems.

5.2

Sources

Remerciements

Rédacteurs de Zimperium
Adam Wosotowsky
Asaf Peleg
Esteban Pellegrino
Jon Paterson
JT Keating
Kern Smith
Krishna Vishnubholta
Monique Becenti
Nico Chiaraviglio
Richard Melick
Santiago Rodriguez
Shridhar Mittal
Jessica Vose

Rédacteurs partenaires
Julian Durand, vice-président de la gestion des produits, Intertrust
Loren Russon, vice-président de la gestion des produits, Ping Identity
Rick Bosworth, directeur du marketing produit, SentinelOne

Un remerciement particulier à
Malcolm Harkins
TK Kellerman

Rédacteurs
Eric Block
Jennifer VanAntwerp
Jessica Vose
Karen Walsh
Randy Budde
Richard Melick

Présentation et mise en page
Tom Green

À propos de Zimperium / Mentions légales

Partant de l'idée que la sécurité mobile nécessite une approche entièrement nouvelle, Zimperium sécurise à la fois les dispositifs et les applications mobiles dans le but de pouvoir accéder aux données en toute sécurité. Une seule et unique plateforme protège les terminaux et sécurise l'ensemble du cycle de développement des applications grâce au seul moteur basé sur l'apprentissage automatique installé sur le dispositif. Zimperium offre une visibilité et une protection accrues contre les cyber-menaces et les attaques connues ou encore de type « zero-day » qui ciblent les dispositifs Android, iOS et ChromeOS ou encore le réseau, comme le phishing et les applications malveillantes. Basée à Dallas, au Texas, Zimperium est soutenue par Warburg Pincus, SoftBank, Samsung, Sierra Ventures et Telstra Ventures.

Pour plus d'informations ou pour nous contacter, rendez-vous sur zimperium.com.

ZIMPERIUM®