ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

BULLETIN

Juin 2018

de *Veille Technologique*

SECURITE DES DONNEES :

Android face aux cyberattaques

Comment se prémunir contre le « phising »?

Editorial

La miniaturisation des composants électriques et électroniques entamée dès le début des années 1900 a fortement contribué à la vulgarisation de l'informatique et des télécommunications qui sont indéniablement parmi les plus grandes révolutions que le siècle passé ait connues. En effet, depuis ENIAC le premier calculateur universel électronique mis au point en 1946 jusqu'aux tablettes et smartphones d'aujourd'hui, en passant par les ordinateurs personnels, la tendance à la réduction de la taille et l'optimisation des performances des « machines » est demeurée grandissante. Ceci a suscité une dynamique positive autour du développement des équipements informatiques, en l'occurrence les smartphones et les tablettes, qui sont devenus peu à peu accessibles à toutes les couches socio-économiques et aujourd'hui incontournables que ce soit pour travailler que pour répondre au besoin crucial des populations de communiquer et de rester en contact permanent avec leurs proches.

Les entreprises aussi sont fortement influencées par l'usage des appareils mobiles. Il faut dès lors trouver un juste équilibre entre parc informatique professionnel et appareils personnels des usagers, afin de conserver un environnement de travail propice à la productivité. Le concept « Bring Your Own Device » (BYOD) ou « Apportez Vos Propres Appareils » en français, est devenu une sorte de règle universelle à laquelle les entreprises ont de plus en plus de mal à se départir. Avec l'essor de l'Internet des objets et l'amélioration croissante des capacités de calcul et des performances de ces « machines » mobiles, la dynamique n'est pas prête de s'estomper.

De plus en plus, nos données à caractère personnel et autres données sensibles de nos familles, nos entreprises, etc. sont stockées et traitées sur ces supports de communication mobiles. La frénésie de la mobilité emmenée par les appareils et périphériques de plus en plus intelligents et performants ont vite fait de nous faire perdre de vue l'importance de garder le contrôle de nos données. En effet, l'omniprésence de ces appareils dans nos vies constitue un facteur de risque très important pour la protection de nos vies privées et la santé socio-économique de nos foyers, entreprises. Le nombre colossal d'actes malveillants perpétrés contre les appareils mobiles au cours de ces dernières années, indique clairement que les milieux cybercriminels portent une attention particulière à ce « nouveau marché ».

La donnée a acquis avec l'essor du numérique, une valeur stratégique sans précédent pour devenir le nouvel or noir qui cristallise les tensions entre les différents acteurs de l'écosystème. En effet, les GAFA (Google, Amazon, Facebook, Apple) tirent l'essentiel de leur richesse de l'exploitation « légale » des données des utilisateurs. Moins enclins au respect des dispositions légales, les cybercriminels s'intéressent singulièrement au vol des données personnelles et sensibles qui sont ensuite revendues sur des places de marchés secrets et illicites à des fins malveillantes telles que les intrusions illicites dans les réseaux d'entreprises, l'espionnage industriel, les chantages, la propagande djihadiste, etc. Une chose est certaine, l'avenir appartient à ceux qui sauront exploiter cette nouvelle matière première digitale pour plus d'innovation et de compétitivité ou pour porter atteinte à autrui.

En 2015, la chaine d'information TV5 Monde a été victime d'une cyberattaque géante dont, selon les experts, le point de départ serait l'intrusion dans le réseau de l'entreprise après le piratage d'un compte utilisateur grâce à un « phishing » (ou hameçonnage en français). Les techniques de « phishing », qui consistent à user de stratagèmes pour appâter les utilisateurs, ont fait leur apparition dans la dernière décennie du siècle passée et ont beaucoup évolué pour s'adapter à l'évolution des moyens de communication électronique et des usages. Mais le but des cybercriminels est demeuré le même : obtenir indûment les identifiants et mots de passe des internautes, des données personnelles ou bancaires, etc.

Le renforcement de la sécurité des données et l'accroissement du capital confiance des usagers du numérique passe inévitablement par une meilleure éducation et une sensibilisation du grand public aux règles de sécurité de base. L'ARTCI doit impulser cette dynamique et contribuer au développement d'une forte culture nationale de la sécurité en ligne. C'est l'objectif poursuivi par ce présent bulletin de veille, dans la perspective d'une digitalisation grandissante des activités économiques, sociales, etc.

BILE Diéméléou
Directeur Général de l'ARTCI

Bulletin
de veille technologique -
Juin 2018
ARTCI, Côte d'Ivoire

Directeur de Publication:

M. BILE Diéméléou

Rédacteur en Chef:

M. KOUAKOU Guy-Michel

Equipe de rédaction:

- Service Veille technologique et Normalisation

- Service Cybersécurité et Gouvernance de l'Internet

Contacts

Marcory Anoumanbo, 18 BP 2203 Abidjan 18.

Tél : + 225 20 34 58 80

Fax : + 225 20 34 43 75

...Au lecteur,

Parce que votre avis compte, nous serions heureux de recevoir vos suggestions et remarques, afin d'améliorer nos prochaines publications, à:

veilletechno@artci.ci

Sommaire

Sécurité Android

L'avenir du célèbre système d'exploitation pour mobiles est-il menacé ?

Un système d'exploitation (SE) souvent abrégé (OS) pour Operating System en anglais, est un ensemble de programmes informatiques mis en cohérence, afin de permettre l'utilisation des ressources matérielles d'un équipement (ordinateur, smartphone, montre, etc.). De manière plus simple, le système d'exploitation est le socle qui sert de base au fonctionnement du matériel, des applications et logiciels. L'OS assure le démarrage (appelé Boot) de l'appareil et partant, le démarrage et le fonctionnement de toutes les autres applications.

Chaque OS est spécifique et dispose de ses propres caractéristiques techniques, comme le langage de développement (C++, Java...), les exigences de développement d'applications compatibles, etc.

Sur le marché mondial des OS pour mobiles, cinq (5) acteurs majeurs se partagent près de 99% de parts de marché. Il s'agit de :

- Android (Google);
- iOS (Apple);
- Windows (Microsoft);
- Blackberry OS (Blackberry);
- Symbian OS (Nokia) .

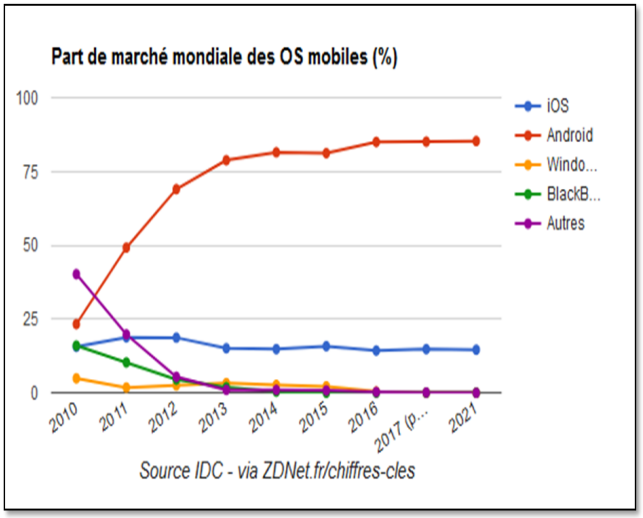
Android, les facteurs du succès spectaculaire et de la notoriété mondiale du système d'exploitation

Créé en 2003 par une startup du même nom (Android-Inc.), Android est un système d'exploitation qui utilise le noyau Linux. Il a été racheté deux ans plus tard (en 2005) par le géant Américain de l'Internet Google et est aujourd'hui le système d'exploitation le plus utilisé dans le monde avec près de 82% de parts de marché sur le secteur des nouveaux smartphones vendus au dernier trimestre 2016, selon IDC/Gartner. Bien que créé en 2003, ce n'est qu'en 2007 que le produit « Android » sous sa forme définitive sera lancé en même temps que la création de l'Open Handset Alliance. En effet, l'idée de la création de cette alliance était de fédérer un ensemble de constructeurs et opérateurs du secteur, afin de créer et standardiser un système d'exploitation pour mobiles interopérable, ouvert, contributif et évolutif, mais également favoriser l'éclosion d'une dynamique de développement du marché des applications mobiles. A sa création, le consortium comptait plus de trente (30) membres parmi les plus influents du marché du mobile.

Android est un logiciel « open-source », c'est-à-dire un logiciel dont le code source est accessible librement au grand public et peut être modifié, adapté à souhait. Cette dernière caractéristique est indiscutablement un facteur clé du succès du système d'exploitation, qui offre une relative facilité de développement et de création d'applications Android. En effet, il apparait bien plus aisé de se lancer dans la programmation et le développement sur des systèmes open-source offrant des API[1]

[1] Application Programming Interface (API): Une API en français « interface de programmation applicative » est un ensemble de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels.

diverses et un accès libre au code source du système d'exploitation.
Le succès d'Android est d'autant plus important qu'il avait été à la base conçu pour être embarqué dans les smartphones et tablettes. Mais aujourd'hui son



utilisation s'est largement généralisée dépassant le simple cadre des tablettes et smartphones pour équiper désormais les télévisions intelligentes (Android TV), les ordinateurs (Android x-86), les montres intelligentes (Android wear), les voitures intelligentes (Android auto), etc.

Meltdown, Spectre, Krack, Stagefright… Android est-il trop faillible ?

Depuis sa création, le système d'exploitation a révélé au cours de son évolution, de nombreuses failles applicatives avec des impacts sur la sécurité des données et des communications des utilisateurs de gravité variable. Difficile d'évaluer l'impact global de ces différentes failles découvertes au fil des recherches et du développement du système d'exploitation, sur la sécurité des utilisateurs.
Une faille de sécurité dans un système d'exploitation est une brèche plus ou moins importante existant dans ledit système et susceptible de donner un accès indu à des données qui y sont stockées ou y transitant. Les failles de sécurité peuvent être dues à des défauts ou des erreurs de conception dans la programmation du logiciel ou naitre suite à l'intégration de nouveaux composants (couches logicielles, matérielles) dans le système dans une dynamique d'amélioration de l'expérience utilisateur par exemple. Par ailleurs, une mauvaise « hygiène informatique »[2] peut créer des failles de sécurité plus ou moins graves sur un système d'exploitation. En somme, tous les logiciels, systèmes d'exploitation y compris, sont susceptibles de présenter des failles de sécurité à un moment ou un autre de leur cycle de vie. Les alertes régulières de chercheurs et autres équipes de sécurité (CERT, CSIRT, etc.) sur les vulnérabilités applicatives confirment que quasiment aucun logiciel n'est épargné par les failles de sécurité. Tous les experts du domaine de la sécurité s'accordent pour dire qu'il n'existe presqu'aucun logiciel à 100% sans erreur ou bug, quel que soit le niveau d'expertise et d'expérience des programmeurs. Au-delà des logiciels, les composants informatiques et électroniques peuvent également contenir des failles de sécurité et affecter la sécurité du système d'exploitation, à l'instar des récentes failles « Meltdown » et « Spectre » découvertes sur des processeurs d'ordinateurs et smartphones.
Dans un tel contexte, la question n'est plus tant de disposer de logiciels 100% sans faille de sécurité, mais plus d'être capable de les identifier et les colmater de manière proactive, afin de limiter les conséquences néfastes que pourraient avoir l'exploitation malveillante de telles brèches de sécurité par des pirates ou autres cybercriminels. En effet, la réactivité et la vitesse de correction des failles de sécurité sont devenues les facteurs clés de la sécurité des logiciels et autres matériels informatiques.
Dans ce domaine, Google (propriétaire et gestionnaire du système Android) fait figure de bon élève, à travers la publication mensuelle de bulletins et correctifs de sécurité relatifs au système d'exploitation. Des équipes entièrement dédiées à la recherche et la correction des vulnérabilités du système d'exploitation mettent régulièrement à disposition des « patchs » de sécurité, disponibles sous forme de mises à jour. La diffusion du bulletin

[2] Hygiène informatique : Une hygène informatique désigne l'ensemble des bonnes pratiques qu'un utilisateur devrait respecter pour garantir la sécurité de son système.

de sécurité se fait en deux temps : le 1er du mois, Google liste les brèches affectant les éléments de son système d'exploitation mobile. Puis, le 5, l'entreprise cite celles qui portent sur les composants fournis par ses partenaires. Par ailleurs, le géant du

Web invite depuis 2010 les chercheurs en sécurité extérieurs et indépendants à lui signaler les vulnérabilités de ses produits, notamment sur Android à travers son programme Bug Bounty. En 2017, ce sont plus de 2,9 millions de dollars USD qui ont été versés à des chercheurs indépendants par Google, pour avoir découvert et signalé des vulnérabilités à la firme américaine.

Une cible de choix pour les logiciels malveillants

Android est devenu le système d'exploitation le plus répandu dans le monde, surpassant même Windows si l'on considère tous les appareils (smartphones et ordinateurs) équipé d'un OS. Par conséquent, le système d'exploitation est devenu la cible préférée des pirates et autres acteurs des marchés cybercriminels, qui prennent la mesure du potentiel gigantesque de l'OS. En effet, la très grande surface de distribution d'Android offre un marché relativement riche pour les vols de données, la distribution de logiciels malveillants (virus, ransomwares, etc.), le spam, etc. On assiste à un véritable acharnement des cybercriminels à découvrir des failles de sécurité dans le système d'exploitation et créer des logiciels malveillants capables de les exploiter et en tirer un profit économique. Selon les chiffres publiés par le cabinet d'analyses G Data en avril 2017, le nombre de malwares Android qui ont été identifiés en 2016 est de plus de 3 millions, soit un nouveau virus toutes les 10 secondes. Cette tendance est malheureusement restée constante et devrait même s'amplifier dans les années à venir à mesure que le système d'exploitation se diversifie et gagne des parts supplémentaires de marché dans l'univers du mobile.

La sécurité à 100% est un rêve inaccessible

Les indicateurs montrent que le système Android a encore de belles heures devant lui, avec l'émergence de l'Internet des objets et la demande croissante d'utilisateurs de plus en plus nomades en matière de systèmes et périphériques mobiles. De plus, la recherche constante de l'amélioration de l'expérience utilisateur et l'ouverture de la plateforme aux développeurs extérieurs indépendants continueront assurément à placer le système d'exploitation au cœur des usages des appareils et périphériques mobiles pendant de nombreuses années encore. Par ailleurs, le système de Bug Bounty et la veille de sécurité soutenue par une large communauté contribueront encore à assurer un niveau de sécurité renforçant la notoriété de l'OS. Les enjeux stratégiques majeurs résident dans la capacité à établir des mécanismes cohérents de défense en profondeur en intégrant le fait que les failles de sécurité sont inhérentes à l'existence du système, afin de définir des outils et procédures qui permettent de limiter l'impact des vulnérabilités dans une approche proactive.

Cependant, il est bien de noter que le plus grand danger de sécurité dans l'utilisation des appareils et périphériques mobiles reste celui qui pianote sur le tactile de son smartphone ou sa tablette, etc. En effet, l'utilisateur reste la première ligne de défense

et la plus grande source de vulnérabilité de ses périphériques, nonobstant les mesures techniques de protection implémentée. Par exemple, un antivirus, n'aurait pas de grande utilité si l'utilisateur le désactive volontairement, afin d'accéder à des contenus potentiellement dangereux. Les quelques règles ci-après énoncées pourraient aider à sécuriser ses équipements mobiles.

- Installer un antivirus
- Effectuer une sauvegarde régulière de ses données personnelles
- Utiliser un VPN (Virtual Private Network) pour la protection de ses données et maitriser la confidentialité des informations échangées
- Adopter une bonne hygiène de mot de passe (Utiliser des mots de passe forts, changer régulièrement son mot de passe, le garder strictement secret, etc.)
- Masquer et/ou chiffrer les données sensibles ou personnelles sur ses équipements
- Désactiver certains services et fonctions lorsqu'ils ne sont pas utilisés (wifi, localisation GPS, etc.)
- Lire, comprendre et refuser, si nécessaire, les permissions allouées aux applications téléchargées, avant l'installation
- Installer régulièrement, voir automatiquement les mises à jour des logiciels
- Verrouiller automatiquement l'écran d'accueil avec un code pin ou un schéma,
- Ne pas télécharger ou installer des applications de sources inconnues ou pas fiables.
- Privilégier les sites web officiels et boutiques officielles de téléchargement (App Store, Play Store, etc.) .

COMMENT ET POURQUOI CHIFFRER SES APPAREILS MOBILES SOUS ANDROID ?

Chiffrer son appareil consiste essentiellement à protéger les données qui y sont stockées grâce à une clé unique, en les rendant illisibles et/ou inaccessibles à toute personne autre que vous, sous la seule condition de garder sous votre contrôle exclusif, la clé sécrète. Le chiffrement n'est pas inviolable, mais offre des garanties suffisantes pour protéger vos données. En effet, si votre appareil est chiffré, les données ne peuvent pas être récupérées en cas de perte de l'appareil ou si quelqu'un connecte votre appareil à son ordinateur à votre insu.

Les versions 6 et plus du système d'exploitation Android sont équipées de la fonction native de chiffrement, mais il faut pour certaines distributions l'activer manuellement. Cette fonctionnalité peut être configuré dans l'onglet paramètre ou réglage de votre appareil sous le champ sécurité.

Si vous désirez aller plus loin dans le chiffrement et la protection de vos appareils, il existe au-delà du chiffrement natif d'Android, un grand nombre d'applications mobiles utiles disponibles sur la plateforme de téléchargement Google, par exemple :

⇒ **Masquer les fichiers** : qui permet de dissimuler et rendre invisible des dossiers ou fichiers sensibles que vous souhaitez dissimuler aux yeux de personnes trop curieuses. L'application fait disparaître de leur emplacement d'origine (la Galerie principalement) les fichiers que vous souhaitez protéger. Vous avez naturellement la possibilité de les restaurer à leurs emplacements respectifs pour y avoir accès comme bon vous semble. Par ailleurs, il est possible de protéger l'accès à l'application par un code secret, pour rajouter une couche de sécurité supplémentaire.

⇒ **Secure (AppLock)** : qui permet de verrouiller l'accès à vos applications. Vous avez le loisir de choisir le mode de déverrouillage parmi les options proposées (mot de passe, schéma, etc.). L'application vous aide à garder le contrôle de l'accès à vos programmes et données sensibles ou personnelles.

Note et références

1. https://source.android.com/security/bulletin/2018-01-01
2. https://security.googleblog.com/2018/02/vulnerability-reward-program-2017-year.html
3. https://www.openhandsetalliance.com/android_overview.html
4. https://www.sstic.org/media/SSTIC2011/SSTIC-actes/Securite_Android/SSTIC2011-Article-Securite_Android-ruff.pdf

Phishing

HISTORIQUE

Le terme « phishing » est un jeu de mot composé des deux termes anglais « phreaking » désignant une technique de fraude perpétrée sur les systèmes de télécommunications, et le terme « fishing » faisant référence à l'activité de pêche. L'attaque de « phishing » était assimilée à l'activité de pêche, car les attaquants utilisaient de véritables appâts, afin de tromper les utilisateurs et collecter en grande quantité les données sensibles des utilisateurs, notamment à travers des milliers d'e-mails.

Les premières réflexions sur le concept de l'attaque de phishing ont été entamées dans le courant de l'année 1987, lors de la conférence « Interex Amérique du Nord » aux Etats unis. Deux scientifiques Jerry Felix et Chris Hauck ont à cette occasion présenté un document intitulé « System Security: A Hacker's Perspective », dans lequel ils dépeignaient des méthodes et scénarii d'attaque permettant à des tiers d'imiter des organisations et services bien connus et de confiance. Selon les archives d'Internet, le terme « phishing » a été utilisé pour la première fois en janvier 1996 dans un groupe de discussion spécialisé de l'entreprise Américaine AOL (America Online). En effet, un groupe de hacker avait mis en place un algorithme malveillant permettant de générer aléatoirement des numéros de cartes de crédit, afin de créer des faux comptes. Les mesures mises en place par AOL ont permis de stopper la fraude sur les faux comptes, conduisant les hackers à inventer un nouveau mode opératoire, en l'occurrence en usurpant les comptes de messagerie instantanée des employés pour obtenir des informations sensibles des utilisateurs. Naissait ainsi ce qui allait devenir l'une des techniques d'attaque les plus insidieuses et usitées de l'ère du numérique.

L'usage de la technique de phishing s'est alors généralisé et s'est développé au sein des équipes et spécialistes de la sécurité à travers la multiplication des usurpations de toute sorte de comptes. Cependant, c'est au cours du mois de Juin 2001 que l'attaque connait une exposition publique, avec deux tentatives d'attaque de phishing contre le célèbre système de monnaie électronique e-Gold[1].

LE PRINCIPE DE L'ATTAQUE DE PHISHING

L'attaque de phishing consiste fondamentalement à user de techniques de manipulation (usurpation d'identité, de qualité, etc.), afin de tromper sa victime et la conduire à communiquer de son propre gré des informations confidentielles et sensibles. Dans la majorité des cas, l'attaque de phishing est réalisée par la manipulation psychologique, communément appelée « social engineering » ou « ingénierie sociale » en français. D'autres méthodes plus élaborées et faisant appel à des procédés

[1] Devise en or numérique créée par l'entreprise Américaine Gold & Silver Reserve Inc., dont l'objectif était de faciliter les paiements en or entre deux titulaires d'un compte e-gold et créer un nouveau moyen de paiement et d'achat de biens et services en ligne.

techniques plus poussés sont également utilisées pour tromper les victimes, notamment l'usurpation de noms de domaines, l'imitation de site web complet, l'injection de faux formulaires sur des pages d'un site internet officiel, etc.

Le succès de l'attaque de phishing repose sur le fait que très peu de compétences techniques sont nécessaires pour réussir à obtenir des données sensibles, confidentielles. En effet, en usant de manipulation psychologique et en s'appuyant sur la force de persuasion, l'attaquant usurpe l'identité ou la qualité d'une organisation ou d'une personne reconnue, afin de se faire communiquer les informations convoitées.

De manière concrète, l'un des exemples de phishing les plus courants est le phishing de comptes e-mails ou de réseaux sociaux. En effet, l'attaquant envoie un e-mail à ses potentielles victimes – pas choisies à l'avance – en prétextant être le l'équipe technique de gestion de la sécurité du service (Facebook, Twitter, Yahoo, Gmail, etc.). L'utilisation des éléments d'identification de l'entreprise légitime (logo, couleurs, etc.) sert à renforcer la crédibilité de l'usurpateur d'identité. Dans la plupart des cas, le message contient des énoncés du type : « En raison de problèmes de sécurité sur votre compte, vous êtes invités à modifier vos informations personnelles, afin de ne pas voir votre compte suspendu ou fermé. A cet effet, vous êtes priés de communiquer votre login et mot de passe ». L'aspect manipulation psychologique intervient dans la mesure où l'utilisateur a une totale confiance au fournisseur légitime du service dans ses efforts de protection du consommateur et l'usager souhaite évidemment conserver la propriété et l'usage de son compte. Le caractère incisif, urgent et directif du contenu du message ont malheureusement un effet psychologique très fort sur la capacité de jugement des victimes peu averties sur les questions de sécurité en ligne.

Dans les cas de phishing un peu plus avancés techniquement, l'attaquant envoie un lien hypertexte dans le corps de l'e-mail et invite la victime à cliquer sur le lien, afin de mettre à jour ses informations d'identification ou son numéro de carte bancaire, toujours sous des prétextes identiques à ceux cités précédemment. Dans ce cas de figure, lorsque l'utilisateur clique sur le lien, il est redirigé vers une vraie « fausse page » du service en question. En effet, l'attaquant prend le soin de reproduire de manière pratiquement identique la page, ou le site internet ; afin de crédibiliser la supercherie. En croyant répondre à une requête légitime des services techniques du fournisseur de service, l'utilisateur qui saisit ses informations dans les formulaires présents sur cette page frauduleuse, transmet l'ensemble de ses informations vers un serveur contrôlé par le pirate. Le pirate peut les récupérer et prendre totalement le contrôle des comptes (e-mail, réseaux sociaux, bancaire, etc.) de sa victime, afin de réaliser diverses actions malveillantes, allant de l'intrusion dans les systèmes de l'entreprise, au vol ou la suppression des données personnelles, voire la commission d'infractions plus graves sous l'identité de sa victime.

Dans certains cas, l'attaquant peut utiliser les données de sa victime pour avoir accès à ses comptes et installer frauduleusement des logiciels espions et autres codes malveillants, qui lui donneront un accès et un contrôle total aux appareils (ordinateurs, smartphones, etc.).

UNE ATTAQUE AUX VECTEURS ET FORMES MULTIPLES

Les vecteurs de l'attaque se sont multipliés et diversifiés avec l'évolution des moyens de communication numérique. Les attaquants malveillants réinventent quotidiennement les méthodes et outils de phishing. En effet, outre la méthode classique et la plus courante de l'e-mail, des attaques de phishing sont réalisées par le biais de :

- ### SMS : ON PARLE DE SMISHING

Le smishing est un phishing qui est réalisé par le biais d'un SMS. Dans la majorité des cas, cette forme de phishing est matérialisée par du texte envoyé par SMS depuis un numéro de téléphone usurpé (personne physique ou morale ou service automatisé). La collecte des informations est réalisée

à partir du moment où l'utilisateur clique sur le lien frauduleux. Le smishing est une forme de phishing particulièrement redoutable, car la plupart des utilisateurs ont plutôt tendance à faire confiance à un SMS qu'à un e-mail. En effet, quand bien même les utilisateurs sont sensibilisés à la sécurité en ligne, cliquer sur un lien contenu dans un SMS, parait malheureusement moins dangereux que cliquer sur un lien contenu dans un e-mail.

Comme pour les phishing classiques, les escrocs incitent les usagers à cliquer sur les liens malveillants, avec des messages du type : « en application des dispositions réglementaires, vous serez facturés sur une base journalière pour l'utilisation du service Y. Si vous souhaitez vous désabonner, veuillez cliquer sur le lien ci-dessous » ou « pour ne pas voir votre compte suspendu ou clôturé, veuillez mettre à jour vos informations, en cliquant sur le lien ».

- ### La voix sur IP (VoIP) : on parle de Vishing

Le Vishing est un phishing réalisée par VoIP. Il consiste à utiliser un ou plusieurs serveurs afin de composer aléatoirement des numéros de téléphone en utilisant la technologie voix sur IP. Les personnes contactées sont incitées à communiquer des informations sensibles ou confidentielles, soit par le biais d'un serveur vocal ou de codes USSD, etc. La victime est invitée à saisir son numéro de carte bancaire, code PIN ou toutes autres informations utiles qui pourraient être utilisées à des fins malveillantes par les attaquants.

- ### Des liens transmis sur les réseaux sociaux

De nombreux cas de phishing sont réalisés par l'envoi de message via les services de messageries instantanées. En raison du grand nombre de données personnelles produites par les usagers sur les réseaux sociaux, les attaquants utilisent ce vecteur pour prendre le contrôle des comptes de réseaux sociaux, mais aussi et surtout pour réaliser des vols d'identité. En effet, les utilisateurs peu sensibilisés aux risques de sécurité, communiquent très aisément un nombre très important de données personnelles, permettant de créer une vraie fausse identité d'eux. Ces données sont dans la majeure partie des cas revendues sur le « darknet », à des fins criminelles (faux papiers, fausses identités, etc.).

- ### Le hacking d'un site pour qu'il redirige vers un site frauduleux

Les attaques de phishing réalisées par le pirate de site internet, requièrent un niveau de technicité relativement élevé, mais peuvent avoir un impact absolument catastrophique. En effet, les pirates étudient, découvrent et exploitent les failles du site internet d'un organisme reconnu et proposant des services. Les établissements bancaires et de commerce en ligne sont les plus visés par ce type d'attaque. Dans la pratique, l'attaquant pirate une ou plusieurs pages contenant les formulaires d'identification du site internet (login, mot de passe, numéro de carte bancaire, etc.), ensuite il redirige les informations saisies vers un serveur qui est sous contrôle. Bien que le lien renvoie au site légitime de votre banque, les informations confidentielles sont détournées vers un centre de collecte contrôlé par le pirate.

- ### L'usurpation de nom de domaine

Dans ce cas de figure, l'attaquant recrée un site internet copie conforme d'un site légitime, afin de tromper ses victimes et obtenir d'elles la communication d'informations sensibles. La subtilité apportée par cette technique est que l'attaquant crée également un nom de domaine qui est à un détail près, identique au nom de domaine de l'entreprise légitime, étant donné que techniquement il ne peut y avoir deux noms de domaines identiques. En vérité, l'attaquant crée un nom de domaine qui se rapproche le plus du nom de domaine du site ciblé, par exemple pour le site internet www.cybersecurite.ci, l'attaquant crée un domaine www.cyberscurite.ci, en modifiant subtilement l'orthographe du nom de domaine. A vu d'œil, les deux domaines sont identiques, mais il manque un « e » au second. Des utilisateurs, même avertis,

auraient bien du mal à détecter du premier regard, la supercherie.

UN PHÉNOMÈNE MONDIAL AUX PROPORTIONS INQUIÉTANTES

En mai 2017, le géant Google a mis en garde ses utilisateurs contre une tentative massive de phishing. En effet, des utilisateurs, pour la plupart basés aux Etats-Unis et en Europe, ont reçu un mail provenant prétendument d'un de leurs contacts, les invitant à cliquer sur un lien, afin de modifier un document Google Doc. Après avoir cliqué, sur les liens et renseignés les formulaires d'identification, les utilisateurs donnaient accès à leurs contacts et leurs messages à des cybercriminels. L'attaque avait pris de telles proportions que Google invitait ses utilisateurs à ne plus cliquer sur aucun lien pendant cette période et à signaler tous messages comme spam et a réussi à stopper la propagation de cette attaque, qui selon la firme américaine n'avait touché que 0,1% de ses utilisateurs.

En février 2018, une campagne de phishing très évoluée et sophistiquée a visé les clients d'Air France. Les attaquants promettaient des billets gratuits en renvoyant comme dans la plupart des phishing, vers un site web malveillant, imitant presque à la perfection le site légitime de l'organisme. L'URL renvoyant au site malveillant utilisait un caractère issu de l'alphabet phonétique rendant l'escroquerie presque indécelable. Dans l'actualité du 85ème anniversaire d'Air France, le lien malveillant a été largement diffusé par des SMS envoyés par milliers et promettant à leurs destinataires des billets gratuits en guise soit disant de cadeau.

L'URL utilisait des caractères de type non latin, en l'occurrence le « a » avec un point en dessous dans « france ».

Selon les données d'une étude réalisée par l'entreprise de sécurité Webroot en 2017, en moyenne, 1.385.000 sites uniques de phishing sont créés chaque mois, avec un record de 2,3 millions de site de phishing enregistrés en Mai 2017.

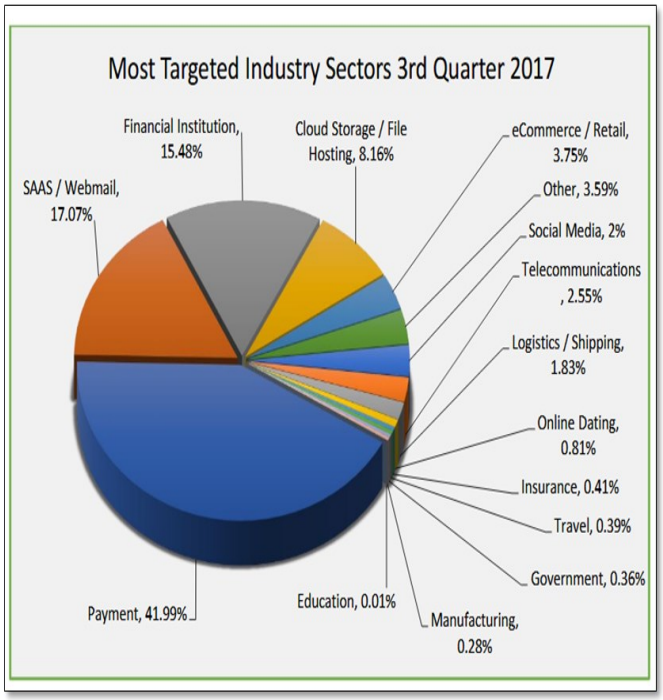
Les attaques de phishing sont la principale cause des violations et infractions numériques et constituent une menace croissante pour les organisations du monde entier. Selon les données communiquées par le FBI, les attaques de phishing ont coûté aux entreprises américaines près de 500 millions de dollars par année sur une période de trois ans entre octobre 2013 et décembre 2016.

En 2017, au cours d'une enquête réalisée par le SANS (SysAdmin, Audit, Network, Security) Institute, auprès de professionnels de l'informatique et de la sécurité du monde entier sur les menaces qui pèsent aujourd'hui sur leurs entreprises, 72% ont affirmé que le phishing est l'une des menaces les plus fréquentes. 40 % des personnes interrogées ont déclaré avoir été victimes d'attaques de phishing, notamment le « spear phishing » (phishing ciblé) et « whaling » (phishing ciblant en priorité les cadres dirigeants des organisations).

A QUEL AVENIR LE PHISHING EST-IL DESTINÉ ?

Le profil et les méthodes du « phisheur » classique ont drastiquement changé avec les années. De nos jours, les auteurs de phishing se professionnalisent indéniablement. De nombreuses campagnes de phishing sont organisées de manière professionnelle en utilisant de plus en plus des kits prêts à l'emploi comprenant l'ensemble des outils dont ils ont besoin pour réaliser des larges campagnes de phishing.

Les attaques de phishing traditionnelles appartiennent désormais au passé, car les campagnes de phishing actuelles sont constituées de groupes ou d'individus bien organisés ciblant les entreprises, les personnalités et motivés par l'appât du gain. Dans une autre mesure, les attaques de phishing sont des armes toujours redoutables utilisées comme point de départ par les hackers, dans les campagnes d'espionnage industriel, politique et voire des campagnes propagandistes, à l'instar de l'attaque de TV5 Monde.



COMMENT S'EN PRÉMUNIR ?

Réduire le risque d'être victime des attaques de phishing relève de prime abord du bon sens et de la capacité à reconnaitre les signes trahissant une tentative de phishing. Certains outils techniques fournissent des alertes sur des tentatives de phishing, mais rien ne remplace l'œil et la vigilance de l'homme. Les indices suivant devraient vous mettre la puce à l'oreille de l'existence d'une tentative de phishing :

s'il y a présence de fautes d'orthographe inhabituelles ou une faible qualité rédactionnelle dans un e-mail de la part d'un organisme de confiance ;

si l'on vous demande de communiquer des informations confidentielles ou sensibles, telles que mot de passe, code PIN, etc. (un organisme de confiance ne le fera jamais !) ;

si l'orthographe du nom de domaine du site est différente du nom de l'organisme ;

si l'on vous incite à effectuer une action avec une forme quelconque de pression (urgence, menaces, etc.).

Si reconnaitre les signes annonciateurs d'une tentative de phishing est essentiel, adopter des bonnes pratiques et mettre en œuvre les règles de sécurité suivantes, peuvent aider à éviter d'en être victime :

Utiliser une extension pour navigateur (sorte d'application supplémentaire installée dans les navigateurs), sécurisant la navigation web (par exemple, WOT: Web Of Trust) ;

Installer une extension ou une barre d'outils anti-phishing dans votre navigateur;

Utiliser un anti-virus permettant de détecter des logiciels espions éventuellement téléchargés ;

Ne jamais communiquer son mot de passe en réponse à un appel ou à un email, quelles qu'en soient les raisons évoquées ;

Ne jamais cliquer sur un lien contenu dans un email ou un SMS, si vous devez saisir des informations sensibles dans un formulaire (mot de passe, code PIN, numéro de carte de bancaire, etc.). Copiez plutôt le lien et coller le dans la barre d'adresse ;

Effectuer un survol avec le pointeur de votre souris sur le lien et faire attention à l'URL qui s'affiche dans la bulle d'information pour vérifier qu'elle est identique à l'adresse du lien ;

Mettre régulièrement à jour son navigateur web ;

Réfléchir avant de cliquer sur des liens et ne pas hésiter de confirmer par un appel téléphonique auprès des personnes concernées (banque,

collègue, parents, etc.), toute demande ou requête douteuse ;

S'assurer de la présence de la mention « https:// » dans l'URL des sites sur lesquels vous devez renseigner des données sensibles. La présence du petit cadenas et du https:// indiquent que le site utilise une connexion sécurisée. Même si cela ne garantit pas à 100% que le site n'est pas faillible à une attaque de phishing, c'est une garantie suffisante de confiance ;

Ne pas hésiter à contacter des spécialistes de la sécurité en cas de doute, avant ou après avoir reçu des messages présentant les signes d'un phishing

Note et références

1. https://www.linformaticien.com/actualites/id/48348/bug-bounty-google-a-verse-2-9-millions-de-dollars-en-2017.aspx
2. https://en.wikipedia.org/wiki/E-gold
3. https://www.lemondeinformatique.fr/actualites/lire-une-vicieuse-attaque-de-phishing-usurpe-air-france-70915.html
4. https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf
5. https://www.ic3.gov/media/2017/170504.aspx#fn3
6. http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf
7. https://www.cybrary.it/2017/03/history-phishing-now/
8. https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf
9. http://www.merriam-webster.com/dictionary/phishing
10. http://www.allspammedup.com/2009/02/history-of-phishing/

Le service Veille Technologique rattaché à la Direction de l'Economie et marchés, de la Prospective et des Statistiques (DEPS) de l'ARTCI scrute le paysage des TIC afin de déterminer de nouveaux sujets d'informations. Ces sujets permettent d'analyser l'actualité du secteur, de mieux comprendre les enjeux de la régulation et l'impact des TIC dans la vie de tous les jours.

ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

Juin 2018
Abidjan, Côte d'Ivoire