Phishing : 5 attaques qui menacent les mobiles en 2020

1 – Les mobiles deviendront le premier vecteur pour les attaques de phishing

Lookout prévoit que les attaques de phishing ciblant les terminaux mobiles dépasseront en nombre les attaques de phishing traditionnelles via email. Les passerelles de sécurité email traditionnelles bloquent les emails de phishing potentiels et les URLs malicieux, ce qui permet de protéger les emails d'entreprise contre des attaques visant à dérober des identifiants d'accès, mais négligent les vecteurs d'attaque mobiles, y compris les emails personnels, les réseaux sociaux, les autres plates-formes de messagerie sur mobile et les SMS/MMS. De plus, les terminaux mobiles sont ciblés non seulement en raison de ces nouveaux vecteurs mais aussi en raison de la nature personnelle du terminal et de son interface utilisateur.

Les entreprises doivent réaliser qu'en matière d'ingénierie sociale dans un monde où les périmètres de sécurité traditionnels n'ont plus cours, les emails d'entreprise ne sont plus le seul, ou même le principal vecteur d'attaque utilisé.

2 – L'authentification à deux facteurs est morte, longue vie au MFA

L'authentification à deux facteurs va progressivement disparaître au profit de l'authentification multifacteur (MFA) utilisant par exemple la biométrie en 2020. La plupart des entreprises ont mis en place des processus d'autorisation à code unique (OTAC) pour fournir une authentification à deux facteurs (2FA), mais Lookout, et d'autres acteurs de l'industrie, ont déjà constaté le ciblage de ces processus par des attaques de phishing avancées.
Pour se protéger contre les vols d'identifiants et garantir leur conformité aux réglementations, les entreprises adoptent de plus en plus l'authentification MFA et la biométrie via des terminaux mobiles. Cette nouvelle approche renforce la sécurité de l'authentification et améliore l'expérience utilisateur, mais il est essentiel que le terminal mobile soit parfaitement protégé.

3 – Les acteurs de menaces vont exploiter

le « machine learning » pour opérer de manière autonome

Un domaine où nous pourrions voir la mise en œuvre du « machine learning » par des attaquants est l'exécution de campagnes de « phishing » Des leurres et des pages d'accueil de phishing seront A/B testés par des algorithmes d'intelligence artificielle pour améliorer les taux de conversion, tandis que de nouveaux domaines seront générés et enregistrés avec de semblables algorithmes.
Ces développements permettront à des attaques de se diffuser plus rapidement, au-delà des capacités de détection de la plupart des solutions existantes.

4 – Les attaques ciblant les élections américaines de 2020 se concentreront sur le mobile

Tout comme les cyber attaques ont évolué pour cibler les terminaux mobiles en raison de leur nature et de leur format, il en sera de même pour les élections présidentielles américaines de 2020. Les campagnes de « spear phishing » (harponnage) vont évoluer au-delà des attaques de « phishing » traditionnelles via email que nous avons vues lors des élections de 2016 vers des attaques plus avancées impliquant des applications de messagerie cryptées, des réseaux sociaux et de faux appels téléphoniques.
Avant le dénouement de la prochaine élection, nous assisterons probablement à des attaques réussies résultant d'actions d'ingénierie sociale ou de « phishing » sur mobile, en particulier en raison du fait que les campagnes présidentielles intègrent les terminaux mobiles dans leurs efforts de démarchage.

5 – Les partenariats s'ajouteront aux acquisitions

La dernière décennie a connu un grand nombre de fusions et d'acquisitions dans l'industrie de la sécurité. Cette tendance va probablement se poursuivre, mais désormais différents acteurs intégreront aussi étroitement leurs solutions pour améliorer la sécurité dans les entreprises.
Alors que nous entrons dans une nouvelle décennie, une nouvelle tendance est en train d'émerger qui verra différents fournisseurs de solutions de sécurité former des alliances – même avec certains de leurs concurrents directs – et collaborant de manière stratégique pour combattre des menaces pour le bien de tous.

Un récent exemple de cette nouvelle tendance est la App Defense Alliance, qui a été lancée à la fin

de 2019 pour combattre des applications malveillantes sur Google Play.
Ces alliances ont également un effet positif sur des solutions d'intelligence artificielle, alors que les algorithmes de « machine learning » doivent ingérer un volume croissant de données.