Le Mémo - Épisode 8

Cyberguerre : le phishing peut-il faire tomber de gros poissons ? (1/3)

– Germain :

Jeanne est fan de Star Wars. Comme tous les accros du sabre laser, elle attend avec impatience décembre 2019… date de la sortie du dernier épisode de sa saga préférée. Alors, quand on lui propose sur Twitter de regarder avant tout le monde le film tant attendu... Elle n'hésite pas...

Elle arrive sur un site qui ressemble comme deux gouttes d'eau à une plateforme de streaming. En plein écran, un player avec une image du film. À peine le chargement commencé, on lui demande de renseigner les données de sa carte bleue.

A ce moment-là, Jeanne réfléchit, l'url du site est quand même étrange et pourquoi aurait-elle cette chance alors que tout le monde fait la queue au cinéma ? Elle ferme la fenêtre et retourne sur son fil d'actualité.

Sans vraiment s'en rendre compte, Jeanne vient de passer au travers d'une série d'attaques malveillantes... on trouve tous les détails dans un article de Tech Republic. Sa courte expérience est une des 285 103 tentatives pour infecter des utilisateurs ou collecter des données personnelles... et encore, je ne parle que des attaques basées sur la saga Star Wars en 2019.

[Identité sonore]

— Germain :

Bonjour Marine

– Marine :

Bonjour Germain.

– Germain :

Bienvenue à tous dans le Mémo, le podcast qui décrypte pour vous l'actualité du numérique. Aujourd'hui, on entame une série de trois épisodes sur la Cyber-guerre. La cyber guerre, ce sont des combats sans coups de feu, sans explosion mais des affrontements bien réels même s'ils se déroulent sur la toile. Marine, pour comprendre le lien avec l'attaque qu'a évité jeanne il faut d'abord définir ce qu'est le phishing ?

– Marine :

Et l'étymologie de ce mot valise est très utile pour le comprendre ! C'est ce que je lis dans un article du Journal du Net. Phishing. C'est la contraction des mots « phreaking » avec un P pour le piratage de lignes téléphoniques et « fishing » qui veut dire pêcher. La métaphore est très parlante… On la retrouve d'ailleurs dans « Hameçonnage », la traduction française.

Pour faire court, le phishing est une pratique en ligne malveillante et illégale qui consiste à récupérer les informations personnelles d'un internaute par le biais d'une tromperie.

Je ne suis sans doute pas la première à vous en parler : ce sont les attaques les plus rependues en ligne… tout le monde a déjà reçu des mails étranges demandant de cliquer sur un lien pour aider un ami ou se faire rembourser des sommes astronomiques…

– Germain :

En effet, rien de nouveau là-dedans, ma boite de spams en est remplie… Mais pourquoi on continue d'en entendre parler ?

– Marine :

Eh bien parce que ces attaques évoluent ! Oui, le mail peut paraître parfois ringard. Mais maintenant, il en existe des formes très sophistiquées. Regardez l'exemple de notre fan de Star Wars, l'hameçon est apparu sur son fil Twitter. Sans doute via un hashtag Star Wars ou autre. Elle aurait pu également tomber dessus en recherchant « Star Wars en ligne » sur Google… La méthode derrière ces attaques ? C'est ce que les experts de Kaspersky appellent le Dark SEO, la capacité à optimiser le contenu de ses appâts pour qu'ils remontent naturellement dans les fils d'actualité ou les recherches. Et ça marche particulièrement avec les sujets tendances, comme Star Wars, qui touchent beaucoup de monde…

– Germain :

Et il y a d'autres techniques ?

– Marine :

Oui ! Elles figurent d'ailleurs en cinquième position des prédictions sur la cybersécurité du CEO de Centrify, une entreprise de sécurité informatique. Sur le site Forbes, il annonce qu'« en 2020 le phishing va continuer d'évoluer vers d'autres canaux que les mails, vers les SMS et les vidéos ». Et il décrit aussi comment l'intelligence artificielle pourrait permettre à des hackers de changer de visage lors d'un appel vidéo. Le but étant bien sûr de se faire passer pour un tiers de confiance et de convaincre un dirigeant par exemple de donner des informations clés… Le cas est extrême, mais comme le rapporte Le Parisien, on a connu en France un cas d'arnaque où les malfaiteurs portaient un masque en silicone d'un ministre pour extorquer des fonds à des personnalités…

– Germain :

En fin de compte, les formes de phishing évoluent avec les avancées de la technologie. Mais Marine il y a tout de même un point commun à toutes ces attaques… Leur but : soutirer à la victime une information ou lui faire faire quelque chose…

– Marine :

… oui. La première manière d'y parvenir c'est de multiplier les canaux pour toucher le maximum de personnes, on vient d'en parler. Mais il faut aussi

convaincre l’internaute de donner ces informations. Et les hackers sont devenus experts en la matière. Daniela Oliveira, professeure associée à l'Université de Floride explique même que « nous sommes tous susceptibles d'être victimes d'hameçonnage parce que le phishing influence la manière dont notre cerveau prend ses décisions ».

– Germain :

C’est-à-dire ?

– Marine :

La MIT Technology Review a recensé plusieurs exemples dans un article intitulé « Comment les attaques phishing se jouent de notre cerveau ? ». Pour commencer, l’humeur joue un rôle important. Une personne heureuse qui n’est pas stressée sera moins en mesure de détecter la tromperie. Autre levier, l’autorité. Les hameçonneurs sont particulièrement bons quand il s’agit de construire un message qui reprend les codes graphiques d’une administration ou d’un site populaire comme Amazon. D’autres messages jouent sur la corde sensible et font appel à nos émotions pour nous amener à suspendre notre méfiance... Dans ces conditions, même de simples mails deviennent difficiles à détecter.

– Germain :

Et… donc ça marche ?

– Marine :

De mieux en mieux… Un article de ZDNet qui s’intéresse au phishing en entreprise rapporte une expérience menée par le cabinet de conseil en sécurité Coalfire. Ils ont envoyé des mails d’hameçonnage à 525 entreprises. Et ils ont récolté des informations de 71% d’entre elles… La raison ? 20% des employés de ces entreprises étaient tombés dans le piège et avaient partagé leurs accès et mots de passes internes… L’année précédente, ils étaient seulement 10%. On comprend alors ce qui rend le phishing si efficace : il suffit d’un employé trompé pour récolter des informations qui permettent de mener des actions de plus grande ampleur.

– Germain :

Mais alors, comment y faire face ?

– Marine :

Pour commencer, il est essentiel d’être informé que de telles pratiques existent et sous quelles formes… Selon Daniela Oliveira, 45% des utilisateurs d’Internet ne savent pas ce qu’est le phishing…

Pour y faire face, de nombreuses actions ont été mises en place. Orange par exemple a lancé une fausse campagne l’été dernier qui proposait la 6G en illimité. Pour cela, il fallait cliquer sur un lien… qui redirigeait vers une page de sensibilisation au hameçonnage. Autre exemple, Google a lancé un quiz très

pédagogique pour tester sa capacité à détecter les tentatives de phishing. Le lien est dans la description si vous voulez tester. Attention, c'est difficile…

– Germain :

Oui... en faisant ce test je me suis fait avoir deux fois…

– Marine :

C'est dire... Même le patron d'Amazon peut être piégé ! On a récemment entendu parler du téléphone de Jeff Bezos, hacké par l'Arabie Saoudite. Le cas est une forme raffinée de phishing. Dans un article de Wired sorti en janvier, on découvre que la source du hack provenait de deux messages envoyés en novembre 2018 par Mohammed bin Salman, le prince héritier d'Arabie saoudite. L'un contenait une vidéo et l'autre une photo d'une femme qui ressemblait à Lauren Sanchez avec qui Bezos avait une relation cachée. Dans les deux fichiers… un malware qui a infecté l'appareil.

– Germain :

Ce n'est pas exactement la même chose...

– Marine :

Non en effet, ce qui diffère ici, c'est que l'attaque est très personnalisée. Bezos connaissait Mohammed bin Salman, il lui avait même donné son numéro en personne quelques mois plus tôt. Mais le principe est le même : on utilise la confiance de sa victime pour extorquer une information ou pour exploiter une faille…

– Germain :

C'est ce qu'on appelle le Spear Phishing…

– Marine :

Harponnage en français. Là où le phishing consiste à lancer un filet sur le net, le spear phishing touche une cible précise. Concrètement, on ajoute de l'ingénierie sociale à la méthode que l'on vous a décrite.
Qui vous envoie des mails couramment ? Qui est votre chef ? Qui est votre expert-comptable… Plus j'obtiens d'informations sur vous (via d'autres campagnes de phishing par exemple) plus je pourrai concevoir LE bon message pour vous conduire à donner une information confidentielle.

– Germain :

Une technique particulièrement efficace dans le cadre d'une cyber-attaque ou de cyber espionnage …

– Marine :

Exactement. Un exemple que je lis dans un article de ZDNet est particulièrement éloquent. Alors que l'escalade sur le plan diplomatique atteignait des sommets après qu'un drone américain a abattu Qassem Soleimani, un puissant général iranien, des fonctionnaires fédéraux américains ont commencé à recevoir des e-

mails imitant des questionnaires de Westat. Westat c'est un organisme qui a travaillé avec plus de 80 agences fédérales depuis au moins 16 ans… Derrière ces mails, deux groupes de cyber espionnage liés à l'Iran… Et en copie… dans de faux documents Excel… deux malwares. L'un destiné à s'introduire dans les systèmes informatiques, l'autre pour dérober des mots de passe.

– Germain :

Et pour savoir ce qu'il est possible de faire avec de telles informations, il faudra attendre le prochain épisode de notre série sur la cyberguerre… Merci beaucoup Marine et merci à vous de nous avoir écoutés. Promis : pas de mauvaises surprises dans la description, mais que des liens vers les articles cités dans cet épisode. A très bientôt pour un prochain numéro du Mémo.

Sources :

- Phishers prey on fans of 'Star Wars: The Rise of Skywalker' film (Tech Republic)
- Phishing : définition, traduction (Journal du net)
- Six Cybersecurity Predictions For 2020 (Forbes)
- L'audacieuse arnaque au «faux Jean-Yves Le Drian» arrive devant la justice (Le Parisien)
- How phishing attacks trick our brains (MIT Technology Review)
- Les courriels de phishing en entreprise ça marche encore, voici pourquoi (ZDNet)
- Phishing Quiz (Google)
- Everything We Know About the Jeff Bezos Phone Hack (Wired)
- Iranian hackers target US government workers in new campaign (ZDNet)
- De la 6G illimitée pendant 100 ans ? La fausse pub d'Orange pour alerter contre le phishing (Le Parisien)