Phishing et MFA : comment l'un s'adapte à l'autre

Les services en ligne devraient-ils utiliser un canal de communication distinct* pour l'authentification multifacteur (MFA) ? Un rapport d'étude le suggère. Ses auteurs : trois chercheurs de l'université de Stony Brook (New York) et un de Palo Alto Networks. Son sujet : les *toolkits* de *phishing* « nouvelle génération ».

Qu'entendre par « nouvelle génération » ? Dans les grandes lignes, les outils adaptés au web dynamique et aux mécanismes en temps réel ou proche… dont le MFA. Ils fonctionnent généralement comme des proxys inversés. Cela leur permet de présenter aux victimes les « vraies » versions des sites usurpés. Et d'intercepter le trafic, cookies de session inclus.

Ce genre de mécanisme passe d'autant plus inaperçu qu'il n'interrompt pas la navigation des utilisateurs. Même après interception de données. C'est sans compter les techniques de masquage mises en œuvre au niveau de la couche applicative. Elles permettent de contrer les outils défensifs fondés sur l'analyse du contenu. Et, plus globalement, de faire en sorte que seules les cibles puissent effectivement accéder audit contenu.

Evilginx s'appuie sur une de ces techniques. En l'occurrence, l'usage de paramètres aléatoires dans les URL de *phishing* – seules les requêtes qui incluent ce paramètre aboutissent aux pages demandées. Ce *toolkit*, populaire dans les *red teams*, se configure en ligne de commande. Il embarque son propre serveur DNS, crée automatiquement des certificats TLS grâce à l'API Let's Encrypt et permet d'héberger simultanément plusieurs pages de *phishing*, rattachées à des sous-domaines.

Les chercheurs se sont intéressés à deux autres toolkits. D'une part, Modlishka, publié fin 2018. De l'autre, Muraena, créé en 2019. Ce dernier a la particularité d'automatiser la création des fichiers de configuration (et s'appuie pour cela sur un robot indexeur). Il automatise aussi les actions après extraction des cookies de session, en lançant une instance légère de Chrome par l'intermédiaire du protocole DevTools.

La clé dans la couche réseau

À défaut de beaucoup d'ouvertures sur la couche applicative, allons voir la couche réseau, se sont dit les chercheurs. Et repérons des éléments qui permettent de détecter ces *toolkits*.

Une grosse différence par rapport aux sites qui n'utilisent pas de proxy inversé tient au *timing* des requêtes. En cause, pour résumer, la nécessité de maintenir deux sessions HTTPS distinctes pour gérer les échanges entre la victime et le serveur de destination.

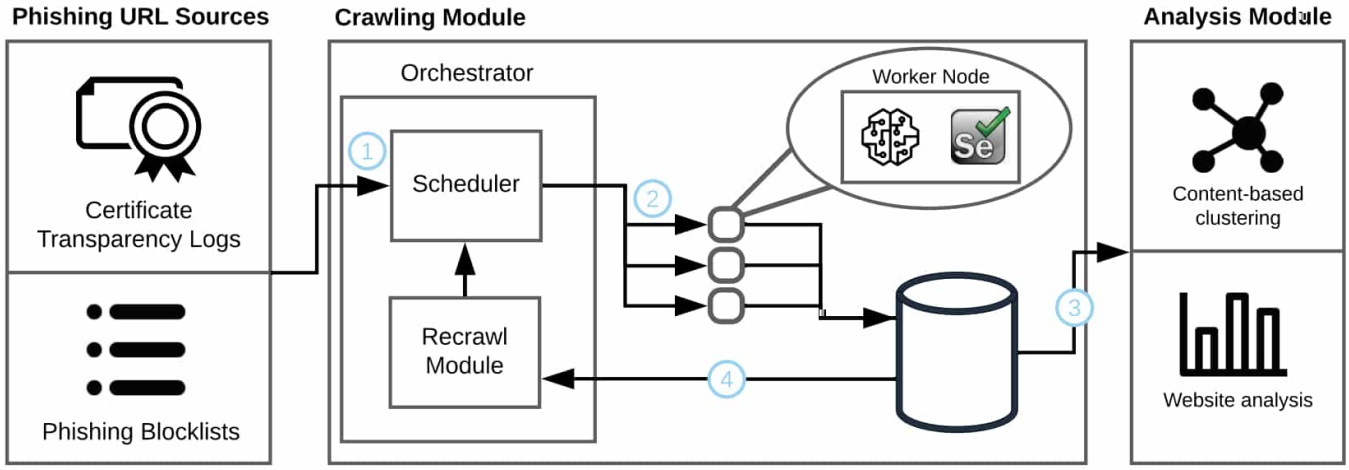
Pour faire la différence avec les sites qui utilisent des infrastructures de type proxy (répartiteur de charge, CDN…), on pourra, entre autres, examiner les caractéristiques des bibliothèques TLS utilisées. C'est la principale méthode qu'ont retenue les chercheurs. Ils l'ont incluse, avec le paramètre *timing*, dans les données d'entraînement d'un modèle d'apprentissage automatique. Son

rôle : détecter les sites derrière lesquels se cachent de tels *toolkits*.

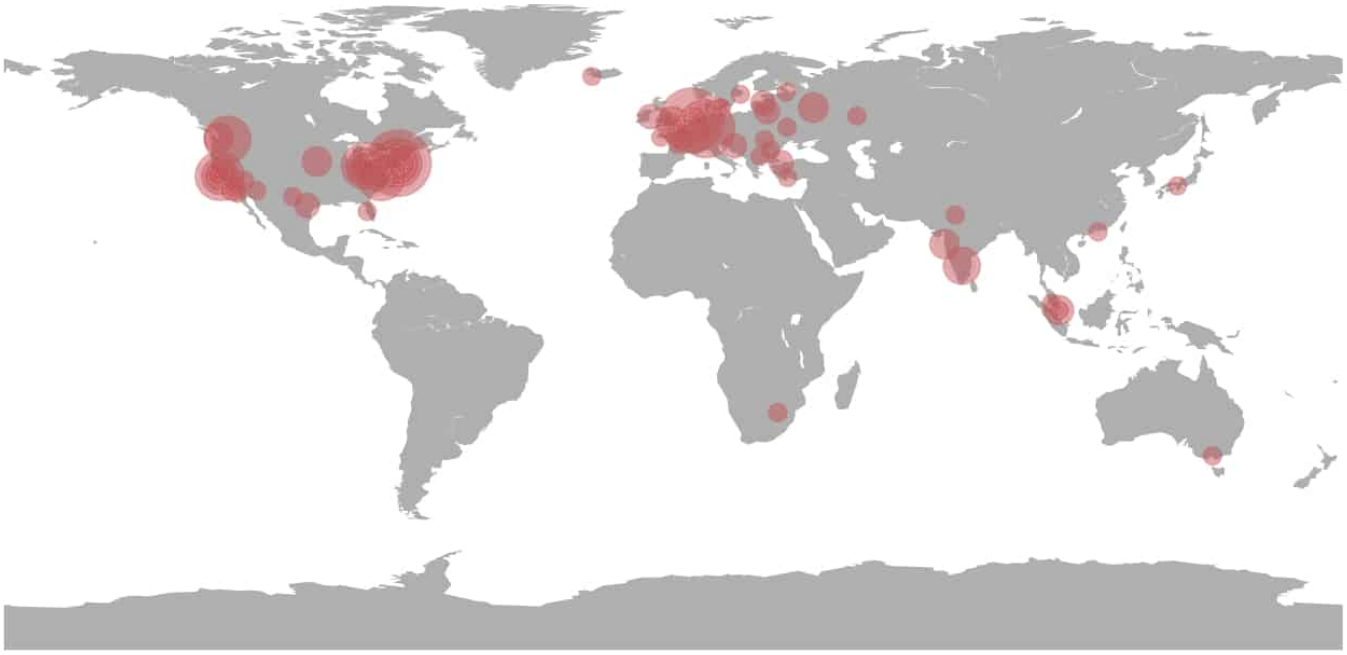
Un phishing plus « résilient » ?

Quatre versions d'Evilginx, sept de Modlishka et deux de Muraena ont servi comme base d'entraînement. Le modèle s'est révélé relativement robuste face aux évolutions des *toolkits*.

Sur ce socle, les chercheurs ont développé PHOCA, outil de détection automatique des sites de *phishing* par proxy inversé. Ils l'ont mis en service pendant un an, à partir de mars 2020.



Une fois supprimés les faux positifs, l'échantillon comporte 1220 sites. Avec une tendance à la hausse de mois en mois. Les deux tiers se concentrent sur cinq marques. Dans l'ordre, Instagram, Google, Facebook, Outlook et PayPal. Avec une quarantaine de domaines hébergés chez OVH.



Le schéma ci-dessous illustre la durée de vie de ces sites. Grâce aux techniques sus-évoquées, elle

est plus longue que pour des sites de *phishing* « classiques » : 40 % durent plus d'un jour ; 15 %, plus de vingt. Sur l'ensemble des URL « positives », moins de la moitié (43,7 %) étaient détectées par au moins un moteur antivirus majeur. Le taux baisse à 18,9 % pour les IP.

À cette démonstration du point de vue du client, les chercheurs en ont associé une du point de vue du serveur. Elle repose sur l'analyse de l'empreinte TLS.

** Par exemple, en faisant en sorte que l'utilisateur renseigne chaque facteur d'authentification sur une page différente.*

Illustration principale © wk1003mike – Shutterstock