SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°7
Sept. 2019

Phishing
Méfiez vous!

Facebook

Fuite de plus de 400 000 numéros de téléphone.

Retadup

Une belle réussite pour la gendarmerie française.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

ATECYS

Association des Tunisiens à l'Etranger Experts en Cyber Sécurité

ATECYS pour Association des Tunisiens à l'Etranger experts en Cyber Sécurité est, comme son nom l'indique, une association regroupant les compétences tunisiennes œuvrant - de près ou de loin - sur le domaine de la sécurité de l'information.

L'idée du groupe est née en décembre 2017 avec une volonté de rassembler les compatriotes du même domaine - aussi large qu'il soit - dans un but commun; voici les objectifs fixés au lancement d'ATECYS :

- Réunir les compétences tunisiennes expertes et/ou passionnées par la cybersécurité dans un groupe communautaire d'entraide (Accueillir les nouveaux arrivants, Orienter et accompagner les réorientations de carrières, partager l'information, conseiller…) : le but est d'élever le niveau de connaissances global sur les différents volets de la cyber !

- Assurer l'organisation de séminaires, de conférences, de sessions de formation et de rencontres thématiques

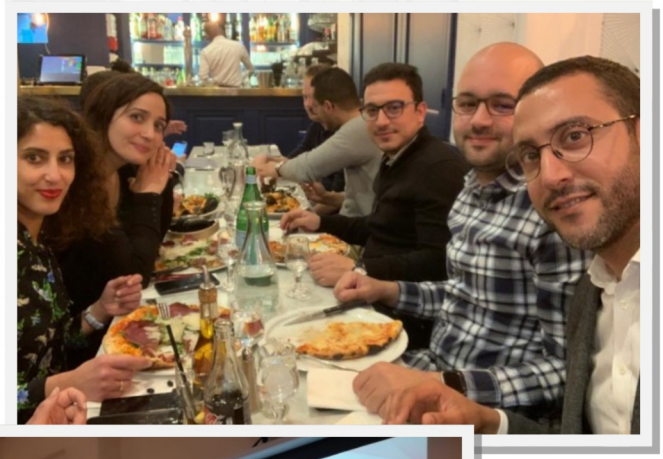
- Mettre en place un trait d'union entre les compétences qualifiées à l'étranger et celles en Tunisie (secteur public: ministères, ANSI, etc. et secteur privé).

- Devenir une référence de qualité et un partenaire actif contribuant au rayonnement global de l'excellence professionnelle Tunisienne à l'étranger dans le domaine de la CyberSécurité

- Apporter un soutien/aide aux autres associations tunisiennes à l'étranger, dans notre domaine de compétence

Depuis, ATECYS s'est bien développée en atteignant environ 90 sympathisants, en organisant - depuis bientôt un an - des workshops mensuels (pendant lesquels des thèmes, qui font l'objet de recherche et préparation par des groupes de travail, sont présentés) et en s'officialisant au mois d'avril 2019 pour compter aujourd'hui 17 adhérents et membres actifs.

Sur la roadmap d'ATECYS, il est prévu de développer les activités des 4 commissions permanentes ATECYS-Hack (démocratiser le hacking, approfondir les connaissances et participer à des challenges au nom d'ATECYS), ATECYSIENNES (promouvoir l'intervention de la femme tunisienne dans le domaine de la cybersec et valoriser sa présence actuelle), ATECYS-DFIR (vulgariser l'activité de réponse à incidents et investigation numérique) et ATECYS-COM (communication sur la cyber sécurité en général avec un focus sur le cyber espace tunisien) .



Facebook: fuite de millions de numéros de téléphone

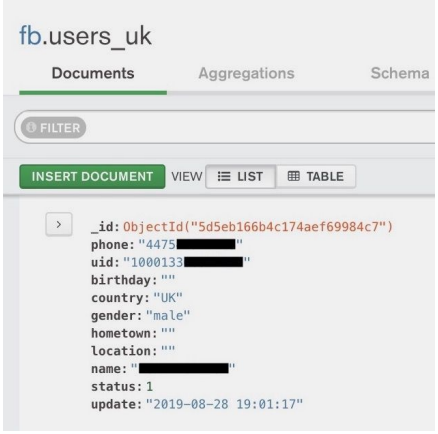
Après une année d'inquiétudes de la part des législateurs et des utilisateurs au sujet des pratiques de sécurité de Facebook, le géant des réseaux sociaux a fait face à un nouveau scandale suite à une base de données découverte en ligne qui aurait contenu des centaines de millions de numéros de téléphone d'utilisateurs.

Le chercheur en sécurité Sanyam Jain a trouvé la base de données en ligne et a partagé la découverte avec TechCrunch. La base de données semble être connectée à un outil qui n'était plus utilisé par Facebook et qui permettait aux utilisateurs de rechercher des amis potentiels en fonction du numéro de téléphone qu'un utilisateur avait volontairement attribué au site.

Un serveur qui n'appartenait pas à Facebook et était accessible au public sans protection par mot de passe hébergeait une base de données des numéros de téléphone. Jain a déclaré à TechCrunch qu'il avait trouvé plusieurs numéros de téléphone de célébrités dans la base de données, qui a été retirée après que le média eut contacté l'hébergeur. Le propriétaire du serveur est toujours inconnu.

Alors que Jain a déclaré que la base de données contenait des enregistrements de plus de 419 millions d'utilisateurs de Facebook, dont 133 millions aux États-Unis et 18 millions au Rayaume uni, l'équipe de relations publiques de Facebook a déclaré aux journalistes que ce chiffre était gonflé et que le serveur contenait "près de la moitié" de 419 millions, selon Gizmodo .
Jay Nancarrow, un porte-parole de Facebook, a déclaré à TechCrunch que les données avaient été effacées avant que Facebook ne restreint l'accès aux numéros de téléphone des utilisateurs en avril 2018.

"L'ensemble de données a été supprimé et nous n'avons trouvé aucune preuve que les comptes de Facebook aient été compromis", a-t-il déclaré.
Néanmoins, les experts en sécurité notent que les données de numéro de téléphone cellulaire, en particulier, sont sensibles aux abus provenant d'appels automatisés ciblés, d'attaques de programmes malveillants, etc.
«Les utilisateurs ne peuvent pas récupérer simplement en changeant leur mot de passe: ils doivent refaire leur compte Facebook ou obtenir un numéro de téléphone différent, ce qui est très peu attrayant», a déclaré Pankaj Parekh, responsable des produits et de la stratégie chez SecurityFirst . "Un autre exemple de données personnelles de personnes exposées par des actions négligentes de la part des personnes de confiance pour les protéger."



Paul Bischoff, défenseur de la protection de la vie privée chez Comparitech, a déclaré que cette exposition pourrait exposer des millions d'utilisateurs de Facebook au spam, au harcèlement et à la fraude par échange de la carte SIM. Les numéros de téléphone étant souvent utilisés pour l'authentification à deux facteurs, des informations pourraient être exploitées par des acteurs malveillants, a-t-il ajouté.
"En transférant un numéro de téléphone existant vers une nouvelle carte SIM, un attaquant recevra le code PIN envoyé par SMS au téléphone de l'utilisateur lors de la connexion," a déclaré Bischoff.

Cette nouvelle faille de sécurité souligne les efforts qui doivent être entrepris par l'entreprise. Le scandale Cambridge Analytica avait remué la planète Facebook, obligeant l'entreprise à se payer des pages d'excuses dans les journaux. L'entreprise a certes depuis pris des mesures afin de tenter de sécuriser au maximum les données de ses utilisateurs, mais il y a encore du travail.

En mai dernier, 49 millions d'utilisateurs Instagram ont vu leurs données s'envoler dans la nature. Le réseau social affirme que les données ne sont plus disponibles, cependant rien ne confirme qu'un acteur malveillant n'y a pas mis la main dessus.
Enfin, l'un des derniers scandales en date pour Facebook a été l'écoute des conversations via Messenger, après qu'Amazon, Microsoft ou encore Apple ont également été accusés d'écouter des conversations sans en informer les utilisateurs.

Sources

https://securitytoday.com/Articles/2019/09/06/Report-Facebook-Database-Found-Online-Exposed-Phone-Numbers-of-Millions.aspx?admgarea=ht.businesscontinuity&Page=3
https://siecledigital.fr/2019/09/05/facebook-fuite-numero-telephone-utilisateurs/

Retadup : Une belle réussite de la gendarmerie Française

Le centre de lutte contre les criminalités numériques (C3N) est parvenu à démenteler le botnet Retadup. Ce dernier compte plus de 960 000 machines infectées.

Détection

Tout a commencé par une alerte reçue par C3N de l'éditeur anti-virus Avast, d'un code malveillant detecté sur un nombre important de machines. La société Avast découvre que le centre de commande et de controle de botnet, baptisé "Retadup", est hébergé en France, plus précisément, chez un hébergeur en Île-de-France ignorant totalement qu'il servait de support technique aux hackers.

Ce redoutable botnet a été créé en 2015. Il s'est répandu dans des ordinateurs fonctionnant sous Windows via onze types de malwares. Au total, ce botnet a touché plus de 960.000 ordinateurs dans 160 pays, principalement en Amérique du Sud (Pérou, Venezuela, Bolivie…) mais aussi en France.

Le code malveillant installé dans les ordinateurs piratés servait aussi à lancer des Dénis Distribués de Service (DDoS).

Contre-attaque

Dès la reception de l'alerte, les gendarmes se sont focalisés sur le serveur C&C des pirates. Ils ont contacté l'hébergeur en questions, et sont parvenus le 2 juillet 2019 à remplacer le serveur commandant "Retadup" par une copie dont ils détenaient les clés de chiffrement, avec pour effet l'autodestruction des instances Retadup connectées. Avec l'appui du FBI

et de la justice américaine pour rediriger des flux informatiques, les cyber enquêteurs de la gendarmerie affirment avoir progressivement neutralisé le botnet.

Source

https://www.zataz.com/retadup-la-gendarmerie-nationale-francaise-met-fin-aux-agissements-dun-groupe-de-pirates-du-moyen-orient/
https://www.europe1.fr/societe/les-gendarmes-neutralisent-le-botnet-geant-retadup-3916344

TOP 6 des attaques de hameçonnage courantes

L'hameçonnage (appelés également « phishing ») est une approche détournée qu'utilisent les cyber-escrocs pour vous pousser à révéler des informations personnelles, comme des mots de passe ou des numéros de carte de crédit, de sécurité sociale ou de compte bancaire. Ils le font en vous envoyant des e-mails contrefaits ou en vous dirigeant sur un site web contrefait.
Le phishing reste l'un des principaux vecteurs de la cybercriminalité

Plusieurs types d'attaques par phishing existent, dans cet articles nous allons dresser uniquement la liste des attaques les plus répandues. L'objectif principal est de sensibiliser les lecteurs à ce genre d'attaque en lui donnant une vue d'ensemble sur le fonctionnement de ces attaques.

1. Usurpation de domaine
Cette méthode d'attaque utilise soit la messagerie électronique, soit des sites Web frauduleux. L'usurpation de domaine survient lorsqu'un cybercriminel «usurpe» une organisation ou un domaine d'entreprise pour:
- donner l'impression que leurs courriels proviennent du
domaine officiel, ou
- Faire en sorte qu'un site Web fictif ressemble à l'original en adoptant le design du site réel et en utilisant soit une URL similaire, soit des caractères Unicode ressemblant à des caractères ASCII.
Comment est-ce possible? Dans le cas d'une attaque par courrier électronique, un cybercriminel forge un nouvel entête de courrier électronique qui donne l'impression que le courrier électronique provient d'une adresse électronique légitime de la société. Dans une falsification de domaine de site Web, le cybercriminel crée un site Web frauduleux avec un domaine qui semble légitime ou qui est proche de celui d'origine (apple.com vs apple.co, par exemple).

2. Clone phishing
Une attaque de phishing par clonage consiste à tirer parti des messages légitimes que la victime a peut-être déjà reçus et à en créer une version malveillante. L'attaque crée une réplique virtuelle d'un message légitime et envoie le message à partir d'une adresse électronique qui semble légitime. Tous les liens ou pièces jointes de l'e-mail d'origine sont remplacés par des logiciels malveillants. Les cybercriminels prétendent souvent qu'ils renvoient le message d'origine en raison d'un problème lié au lien ou à la pièce jointe de l'e-mail précédent afin d'inciter les utilisateurs finaux à cliquer dessus.

3. Mail phishing
L'approche utilisée par les cybercriminels lors de cette attaque consiste à envoyer un courrier électronique contenant uniquement un lien d'apparence légitime dans le corps du message. Il n'y a souvent aucun autre contenu, à l'exception du lien lui-même (qui peut être cliquable ou non actif, qui oblige le destinataire à copier-coller l'URL dans sa barre d'adresse Web. L'attaquant utilise diverses tactiques d'ingénierie sociale pour amener le destinataire du courrier électronique à cliquer sur le lien ou à copier-coller l'URL dans son navigateur Web (ce qui rend ce type de courrier électronique de phishing difficile à détecter par les filtres). Cela inclut l'envoi de messages à partir d'une adresse électronique qui semble légitime, telle que celle du

Exemple de phishing:
Site inscription universitaire

Récemment, l'ANSI a détecté un incident de phishing sur le réseau social Facebook, qui ciblait les étudiants Tunisiens. Le pirate a créé un site clone de l'inscription en ligne et a publié sur Facebook un communiqué falsifié incitant ces derniers à effectuer leur inscriptions sur le lien malicieux.

Son but et de récolter des informations sensibles comme le numéro de la carte d'identité nationale, l'adresse email, les paramètres de la carte de paiement e-dinar, etc..

l'ANSI a publié une alerte concernant cet incident pour éviter sa propagation et son impact. Elle a également profité pour rappeler les régles anti-phishing.


الجمهورية التونسية
وزارة التعليم العالي والبحث العلمي
مكتب الاعلام والاتصال
تونس في 1 سبتمبر 2019
بـــلاغ
تعلم وزارة التعليم العالي والبحث العلمي الطلبة الجدد بأنه وقع انشاء موقع خاص للترسيم والدفع عن بعد
هذا وسيـتم التسجيل عبـر هذا الموقـع
inscription-fac.weebly.com
التسجيل مفتوح ومتاح للجميع انطلاقا من اليوم 1 سبتمبر 2019

chef, du collègue ou du PDG du destinataire.

4. Smishing ou le SMS phishing

Le phishing par SMS, ou «smishing», est une forme de phishing qui tire parti de la dépendance mondiale à la messagerie texte et aux communications instantanées. Le smishing est un moyen pour les cybercriminels d'attirer les utilisateurs vers le téléchargement de charges utiles malveillantes en envoyant des messages texte qui semblent provenir de sources légitimes et contiennent des URL malveillantes sur lesquelles ils peuvent cliquer. Cela pourrait être quelque chose déguisé en code promo - 20% de réduction sur votre prochain achat - ou une offre de gagner des billets gratuits pour un prochain spectacle.

5. Spear Phishing

Une attaque de phishing est une forme ciblée de phishing. Contrairement aux e-mails d'hameçonnage classiques, qui utilisent des tactiques analogues au spam pour envoyer des milliers de personnes dans le cadre de campagnes d'e-mails massives, les e-mails d'hameçonnage ciblent des personnes spécifiques au sein d'une organisation. Ils utilisent des tactiques d'ingénierie sociale pour personnaliser les courriels en fonction des victimes. Ils peuvent utiliser des lignes de sujet qui pourraient intéresser les destinataires pour les inciter à ouvrir le message et à cliquer sur des liens ou des pièces jointes. Le harponnage est très important vu que 91% des cyberattaques commencent par un courrier électronique de phishing . Le but est souvent de voler des données ou d'installer des logiciels malveillants sur l'ordinateur du destinataire pour accéder à son réseau et à ses comptes. Malheureusement, les méthodes de sécurité traditionnelles peuvent ne pas arrêter ces types d'attaques car elles sont tellement personnalisées que de nombreux filtres anti-spam traditionnels risquent de les manquer.

6. Vishing ou voice phishing

Une attaque à distance a lieu lorsqu'un criminel appelle votre téléphone pour vous demander de fournir des informations personnelles ou financières. Ils utilisent souvent des appels automatisés qui redirigent les individus. Ils utilisent également des applications mobiles et d'autres techniques pour usurper leur numéro de téléphone ou pour le masquer complètement. Ces attaquants utilisent fréquemment diverses tactiques d'ingénierie sociale pour vous inciter à fournir ces informations. Ils sont également connus pour prétendre être quelqu'un d'autre - votre banque ou un dirigeant de votre entreprise qui prétend travailler dans une autre succursale. Ils prétendent que vous devez des taxes ou que votre carte de crédit a une activité suspecte et doit être fermée tout de suite. Il vous suffira tout d'abord de «vérifier» vos informations personnelles avant d'entamer la moindre démarche.

RECOMMANDATIONS

- Ayez de bonnes habitudes et ne répondez pas aux liens dans les e-mails non sollicités ou sur Facebook.
- N'ouvrez pas les pièces jointes des e-mails non sollicités.
- Protégez vos mots de passe et ne les révélez à personne.
- Ne donnez pas d'informations sensibles, que ce soit au téléphone, en personne ou par e-mail.
- Vérifiez l'URL (adresse web) des sites web. Dans de nombreux cas d'hameçonnage, l'adresse web peut sembler légitime, mais l'URL peut comporter une faute d'orthographe ou le domaine peut être différent (.com au lieu de .gov).
- Maintenez votre navigateur à jour et appliquez les correctifs de sécurité.
- Ne jamais remplir de formulaires envoyés par courriel dans lequel on demande d'indiquer ses données d'identification.
- Tapez toujours manuellement l'adresse de la page de connexion de l'institut financier.
- Vérifiez la connexion SSL.
- Adressez-vous toujours directement à votre institut financier en cas de doute.

Sources

https://securitytoday.com/articles/2019/09/09/5-common-phishing-attacks-and-how-to-protect-yourself-against-them.aspx?admgarea=ht.businesscontinuity
https://www.thesslstore.com/blog/10-types-of-phishing-attacks-and-phishing-scams/

Le compte de Jack Dorsey, PDG de Twitter, a été piraté

Twitter est l'un des réseaux sociaux les plus utilisés sur la planète avec un nombre d'utilisateurs actifs se portant à environ 330 millions par mois selon des statistiques faites au premier trimestre 2019.Avec ce nombre important d'utilisateurs, twitter propose une multitude d'outils pour préserver la sécurité des comptes d'internautes. Malheureusement, ceci n'empêche pas que le compte Twitter officiel de Jack Dorsey, PDG de twitter, a été piraté vendredi le 30/08/2019 et utilisé pour diffuser des insultes raciales.

Comment est-ce arrivé?
Twitter a déclaré que le numéro de téléphone associé à son compte avait été compromis en raison d'une supervision de la sécurité par le fournisseur de téléphonie mobile. La société affirme que les pirates avaient utilisé une technique connue sous le nom de "simswapping" (ou "simjacking") pour contrôler le compte de M. Dorsey et d'envoyer des tweets par SMS à partir de son numéro de téléphone. Cela peut arriver si un pirate informatique utilise des informations personnelles relatives à une personne et appelle le service clientèle du fournisseur téléphonique de la victime pour transférer son numéro de téléphone vers une autre carte SIM.

Même si on utilisait une authentification à deux facteurs **[1]** pour sécuriser nos comptes, ceci pourrait être peu fiable et cela est prouvé par le cas de M. Dorsey.

Un groupe de pirates, appelé Chuckle Squad a été accusé. Il est fort probable qu'il est aussi à l'origine d'une attaque avant une semaine contre le compte Twitter d'Etika (Daniel Desmond Amofah).

Twitter critiqué pour son manque de réactivité
Twitter a été reproché cette fois aussi. En 2016, les dirigeants de Twitter ont reconnu lors d'une audition de la commission du renseignement du Sénat américain que leur société a réagi trop lentement aux ingérences russes dans la campagne électorale de 2016, en favorisant la candidature de Donald Trump à la Maison Blanche à l'aide de fausses informations. De sa part, Trump dit après cette attaque que "ça ne devrait pas être trop mal" si quelqu'un pirate son compte Twitter parce que "ils ne vont pas trop apprendre".

Source
https://www.theverge.com/2019/8/30/20841288/jack-dorsey-ceo-twitter-account-hacked-chuckle-gang-shane-dawson-james-charles

[1] : Il s'agit d'une fonctionnalité de sécurité qui oblige une personne à prouver son identité en utilisant un mot de passe, ainsi qu'une deuxième information d'identité, comme un code qui lui est envoyé par exemple par SMS.

Newly Registered Domains (NRDs)

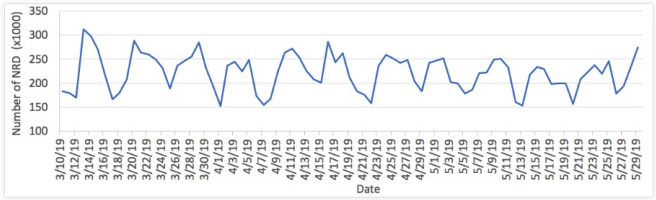
Dernièrement, une étude menée par les chercheurs de l'Unité 42 du réseau Palo Alto a révélé que 70% des domaines nouvellement enregistrés (NRD) sont malveillants, suspects ou dangereux, et conseillent aux entreprises de leur bloquer l'accès à l'aide du filtrage d'URL.

Avant de présenter l'utilisation malveillante et les menaces associées aux NRDs, on va le définir.

C'est quoi Newly Registered Domains ?
Tout domaine est dit «nouvellement enregistré» s'il a été enregistré ou a changé de propriétaire au cours des 32 derniers jours.

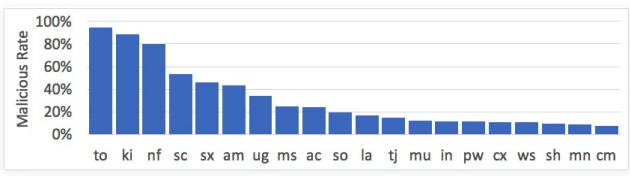
Quoi de nouveau ?
Certains de ces domaines ont une durée de vie courte de quelques heures ou jours. Ils sont désactivés ou supprimés avant même que tout fournisseur de services de sécurité puisse les détecter.
Comme les chercheurs le décrivent, ces NRDs sont malveillants : ils sont configurés pour servir de C & C, distribuer des logiciels malveillants ou publicitaires, héberger des pages d'arnaques et envoyer du spam.

Statistiques
Palo Alto Networks indique que son système identifie en moyenne environ 200 000 DRN chaque jour.



Volume de NRDs quotidien

En plus, les TLD tels que .to, .kl et .nf sont beaucoup plus susceptibles d'héberger du contenu malveillant.



Top 15 TLD avec le taux de NRD malveillant le plus élevé

Utilisation malveillante de NRD
• *Hébergement de l'infrastructure de type attaquant par commande-contrôle (C2)*

Prenons le domaine soroog [.] xyz comme un exemple. Ce

Date	Etat
Le 29 mai 2019	Enregistrement du domaine avec l'adresse IP 51.68.184 .115 et son utilisation par des malwares (Azorult) comme un C2.
Le 24 juin 2019	L'adresse IP est passée à 51.38.101.194
Après le 26 juin 2019	Ce domaine est devenu inexistant.

tableau illustre sa durée de vie :

• *Distribution de logiciels malveillants*

Date	Etat
Le 02 Mai 2019	Le domaine hvkbvmichelfd [.]Info et le domaine halanis21yi84alycia [.]top ont été créés.
Le 06 Mai 2019	Le malware Emotet a utilisé en premier temps le domaine hvkbvmichelfd [.]Info pour télécharger un payload et en deuxième temps le domaine halanis21yi84alycia [.]top pour télécharger le deuxième.

Prenons le malware Emotet comme un exemple:

• *Phishing*
Prenons le domaine canada-neflxt [.] Com comme un exemple. Il tente de voler les informations d'identification des utilisateurs de Netflix ainsi que les informations de fac-

Date	Etat
Le 04 Juillet 2019	Ce domaine a été enregistré.
De 06 Juillet jusqu'à 17 Juillet 2019	Un trafic malveillant a été observé vers ce domaine.

turation.

• *Distribution de logiciels publicitaires*
Prenons le domaine installsvpn [.] com comme un exemple.

Date	Etat
Le 10 mai 2019	Ce domaine a été créé.
Une semaine après	Il a été utilisé pour distribuer un logiciel de publicité destiné aux utilisateurs d'iPhone.

• *Courriel spam*
Un courrier électronique, distribuant des publicités sur l'épargne-retraite, a été détecté comme spam par Gmail au moment de sa réception (le 15 juillet). Il est envoyé via mercinogenitor [.] Com, qui a été enregistré le 4 juillet 2019.

• *Typosquattage*
Le typosquattage (en anglais, typosquatting) est une forme de squattage de domaine se fondant principalement sur les fautes de frappe et d'orthographe commises par l'internaute au moment de saisir une adresse web dans un navigateur.

Les domaines de typosquattage sont largement observés dans les NRDs. Par exemple, le domaine mocrosoft [.] Cf est probablement un domaine de typosquattage destiné à Microsoft. En effet, les lettres «i» et «o» sont côte à côte sur un clavier classique et une faute de frappe est possible. Ce domaine a été enregistré pour la première fois le 3 juin 2019 et un trafic malveillant vers ce domaine a été capturé le même jour. Il a été utilisé dans le but d'un phishing qui tente de dérober les informations de connexion des utilisateurs.

Sources
https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

TUNCERT

Attention à la nouvelle variante du malware « Echobot ».

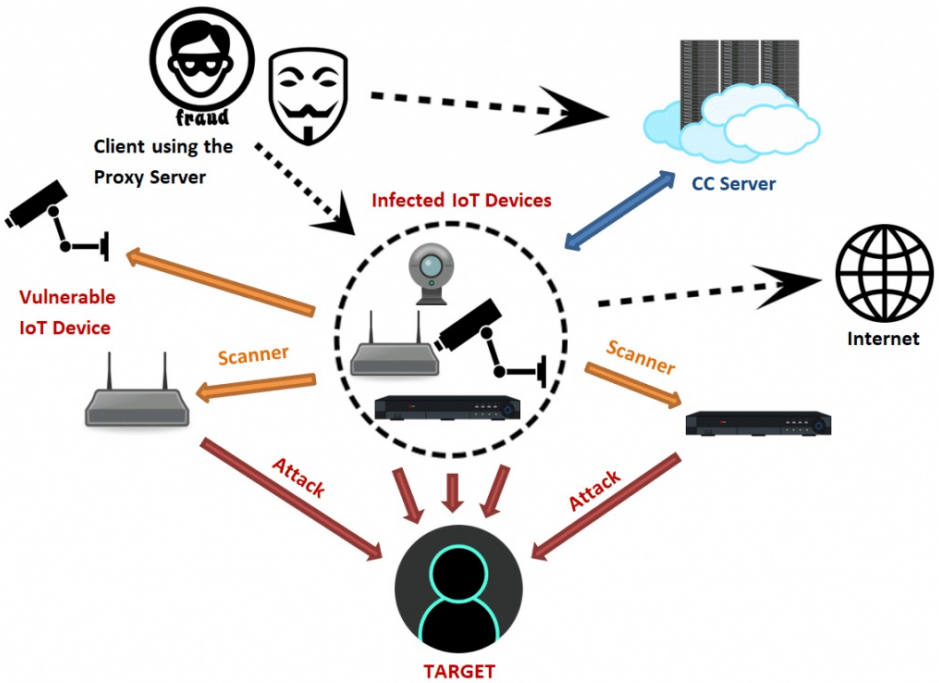
Héritant du fameux botnet « Mirai », une nouvelle variante du malware « Echobot » a été découverte sur le net en utilisant plus que 50 méthodes de propagation via l'exploitation des vulnérabilités présentes dans les périphériques IoT, les routeurs, les caméras, le smart home-hubs, les systèmes de stockage en réseau et les applications d'entreprise.

Pour se protéger face à cette menace, nous vous recommandons d'être vigilant et de suivre les mesures préventives suivantes :

• Scanner votre système d'information et les zones d'hébergement afin de déterminer les failles puis procéder à les corriger en installant les patchs correctifs depuis les sources officielles.

• Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de votre trafic réseau.
• Désactiver immédiatement tous les services que vous n'avez pas besoin.
• Appliquer des règles de filtrage rigoureuses pour sécuriser l'administration de vos serveurs à distance.
• S'assurer de la robustesse des mots de passe des comptes utilisateurs et administrateurs.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=151



Attention aux attaques DDoS exploitant le protocole « WS-Discovery ».

Récemment, des tentatives d'attaques DDoS abusant le protocole « Web Services Dynamic Discovery : WS-Discovery) ont été détectées sur le net. En effet, WS-Discovery est un protocole de multidiffusion (multicast) qui peut être utilisé pour découvrir les périphériques pouvant communiquer via des messages particuliers comme SOAP (Simple Object Access Protocol).

Sur UDP, WS-Discovery est idéal pour réaliser des attaques DDoS avec des adresses IP falsifiées /spoofées et d'entraîner les serveurs non sécurisés à générer plusieurs réponses UDP avec un facteur d'amplification entre 300 et 500 réponses pour une seule requête client ce qui consomme énormément la bande passante des réseaux visés.

Pour s'en protéger, nous vous recommandons d'être vigilant et de suivre les mesures préventives suivantes :

• Contrôler la bande passante de votre trafic réseau et bloquer tout accès non autorisé au port 3702.

• Activer les fonctionnalités qui vous permettent de détecter et d'atténuer les problèmes causés par les adresses IP spoofées au niveau de vos équipements réseaux.

Source

https://tuncert.ansi.tn/publish/content/news.asp?idn=153

Les vulnérabilités signalées par tunCERT durant le mois de Août

Référence	Date découverte	Titre
tunCERT/Vuln.2019-301	29/08/2019	Systèmes Cisco FXOS, NX-OS et UCS
tunCERT/Vuln.2019-300	29/08/2019	Cisco REST API Container pour IOS XE Software
tunCERT/Vuln.2019-299	28/08/2019	Google Chrome
tunCERT/Vuln.2019-298	27/08/2019	Apple iOS
tunCERT/Vuln.2019-297	22/08/2019	Produits Cisco
tunCERT/Vuln.2019-296	21/08/2019	Apache Struts
tunCERT/Vuln.2019-295	20/08/2019	Bluetooth BR/EDR
tunCERT/Vuln.2019-294	19/08/2019	Mozilla Firefox
tunCERT/Vuln.2019-293	19/08/2019	Cisco Firepower Threat Defense
tunCERT/Vuln.2019-292	16/08/2019	Apache Httpd
tunCERT/Vuln.2019-290	15/08/2019	Joomla!
tunCERT/Vuln.2019-289	15/08/2019	HTTP network protocol- HTTP/2-
tunCERT/Vuln.2019-286	14/08/2019	Adobe Photoshop CC
tunCERT/Vuln.2019-285	14/08/2019	Adobe Reader et Acrobat
tunCERT/Vuln.2019-283	14/08/2019	Produits Intel
tunCERT/Vuln.2019-282	14/08/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-281	14/08/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-280	14/08/2019	Microsoft Office
tunCERT/Vuln.2019-279	14/08/2019	Microsoft Edge
tunCERT/Vuln.2019-278	14/08/2019	Internet Explorer
tunCERT/Vuln.2019-277	12/08/2019	F5 BIG-IP
tunCERT/Vuln.2019-276	08/08/2019	Systèmes Cisco IOS XR
tunCERT/Vuln.2019-275	08/08/2019	Cisco Enterprise NFV Infrastructure
tunCERT/Vuln.2019-273	08/08/2019	Cisco Adaptive Security Appliance
tunCERT/Vuln.2019-272	08/08/2019	SWAPGS : Nouvelle variante de Spectre.
tunCERT/Vuln.2019-271	08/08/2019	Cisco Webex Network Recording Player
tunCERT/Vuln.2019-270	08/08/2019	KDE Linux Desktops
tunCERT/Vuln.2019-269	08/08/2019	Google Chrome
tunCERT/Vuln.2019-268	07/08/2019	Cisco Small Business 220 Series Smart Switches
tunCERT/Vuln.2019-267	06/08/2019	Google Android
tunCERT/Vuln.2019-265	03/08/2019	Pilote graphique NVIDIA
tunCERT/Vuln.2019-264	03/08/2019	Produits VMware
tunCERT/Vuln.2019-263	02/08/2019	Cisco Nexus 9000 Series
tunCERT/Vuln.2019-262	01/08/2019	Google Chrome

Source: https://tuncert.ansi.tn/publish/module/listvulnerabilite.asp

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Parce que le partage du savoir est la clé de la réussite dans le domaine de la sécurité_informatique, l'Agence Nationale de la Sécurité Informatique est fière de vous annoncer la parution d'une nouvelle rubrique de son magazine mensuel "**SAHER Magazine**" intitulée "Cyber-agora".

Cyber-agora sera un espace ouvert aux contributions des professionnels, étudiants et académiciens évoluant dans le domaine de la sécurité informatique. À ce titre, une adresse E-mail sera mise à votre disposition pour y envoyer vos articles qui, après leur vérification par les équipes de l'ANSI, seront publiés dans les prochaines éditions de SAHER Magazine.

Il est à noter que le contenu des articles doit être unique sachant qu'une vérification anti-plagiat sera réalisée avant toute publication officielle. Enfin, si l'article est sélectionné, son auteur serait crédité.

Veuillez nous envoyer vos contributions à cette adresse : **sahermag@ansi.tn**

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn
incident@ansi.tn
saher@ansi.tn
cert-tcc@ansi.tn
audit@ansi.tn
sahermag@ansi.tn