De: "CERT-RENATER" <certsvp@renater.fr>
À: renater-cert@listes.renater.fr
Envoyé: Jeudi 8 Juillet 2021 11:45:51
Objet: CERT-Renater : 2021/INFO1 : Information sur les attaques de type Smishing

==========

Message du CERT-RENATER (certsvp@renater.fr)

Note d'information sur les attaques de type Smishing

==========

Bonjour,

Le "Smishing" (contraction de "SMS" et de "Phishing") utilise les mêmes méthodes que les attaques de type phishing mais via l'envoi de SMS. Des SMS sont envoyés dans le but de dérober des données personnelles, professionnelles, mais aussi bancaires des utilisateurs de smartphones.

Un SMS de "Smishing" va utiliser toutes les ficelles du phishing pour pouvoir piéger les utilisateurs, soit en les amenant à donner eux mêmes des informations ou bien en faisant en sorte qu'une application espionne soit installée sur leur téléphone.

Cette méthode d'attaque est très efficace car les utilisateurs ont l'habitude de recevoir des SMS de toutes sortes comme des confirmations d'achat, de livraison, de rendez-vous, d'authentification et autres... Ainsi avec le temps les utilisateurs deviennent assez peu méfiant sur l'envoi de SMS. De plus les attaquants tirent aussi parti de cette pratique pour créer des scénarios d'attaques de plus en plus crédibles.

Un SMS de "Smishing" intègre le plus souvent un lien malveillant qui en cas de validation par simple "clic" va diriger le navigateur internet vers une page Web malveillante.

Comme pour le phishing les émetteurs de "Smishing" vont essayer de se faire passer pour des opérateurs de sites Web légitimes usurpant leur identité et en utilisant un prétexte habilement choisi pour tenter d'obtenir des données frauduleusement.

Techniquement afin d'optimiser cette attaque, les attaquants vont utiliser massivement des raccourcisseurs d'URL comme avec les services bit.ly, ow.ly, bit.do, short.io, tinyurl.com et autres qui produisent des liens du type https://bit.ly/[aléatoire] qui seront repris dans le SMS.

Cette technique qui facilite l'envoie de liens complexes permet aussi de cacher aisément une redirection vers des sites malveillants, que les victimes oublieront ou ne pourront pas vérifier avant d'être infectées.

Details sur les cas de "Smishing" actuellement en cours de diffusion :

Ce type de mécanisme d'attaque est actuellement utilisé pour propager les chevaux de Troie espions "Flubot" et "Teabot".

Ces menaces sont actives en EUROPE depuis plusieurs mois
et ciblent tous les smartphones sous Android.

Une fois installé ce code malveillant subtilisera discrètement des données stockées dans le téléphone et les enverra sur des serveurs contrôlés par les attaquants Il permettra aussi de trouver de nouvelles cibles potentielles en exploitant directement les informations du carnet d'adresses des victimes.

Les liens malveillants utilisés dans ces SMS redirigent essentiellement

vers des pages Web hébergées sur des serveurs préalablement piratés.
Un grand nombre de sites Web ont déjà été compromis afin de
diffuser cette menace (plusieurs centaines par jour).

Pour parachever le tableau ces botnets ont aussi mis en place deux modes
de communication. Un mode de communication vers des serveurs de contrôle
mais aussi le recours à des algorithmes de génération de noms de domaine
(DGA). Ils sont conçus pour permettre aux opérateurs du botnet
d'utiliser des noms de domaine aléatoires supplémentaires afin d'en
conserver le contrôle.

Ce mode de communication est généralement utilisé en complément pour
pallier d'éventuelles coupures avec les serveurs de contrôle. Ces noms
de domaine seront contactés successivement.

Pour en savoir plus sur le mode opératoire qui est utilisé par les
menaces "Flubot et Teabot " voir les pages suivantes :

https://www.proofpoint.com/fr/blog/apercu-de-la-menace/flubot-le-malware-android-se-repand-en-europe
https://www.safeonweb.be/fr/actualite/un-faux-sms-propage-le-virus-flubot-ne-cliquez-pas
https://www.welivesecurity.com/fr/2021/05/18/logiciel-malveillant-flubot/
https://www.undernews.fr/telephonie-phreaking-voip/les-cybercriminels-utilisent-de-fausses-applications-android-pour-diffuser-les-logiciels-malveillants-teabot-et-flubot.html
...

Pour conclure, il est quasiment impossible de se prémunir de ces menaces
qui arriveront sur nos smartphones d'une manière ou d'une autre
(notamment via les réseaux sociaux).

Le "Smishing" devient une menace de plus en plus importante.

Il reste indispensable de signaler ces messages malveillants au numéro
33700. Sur ce numéro il est possible de signaler un spam SMS et le
"Smishing" pour informer les opérateurs.

Lors du signalement au "33700" un deuxième message de validation est
envoyé demandant de transmettre le numéro à l'origine du SMS frauduleux.

Voir la plateforme "33700.fr" pour signaler le SMS en question:

https://www.33700.fr/
https://www.33700.fr/identifier-et-signaler-un-spam-sms/

Autres analyses techniques du code malveillant "Flubot" et
"Teabot/Anatsa" :

https://securityblog.switch.ch/2021/06/19/android-flubot-enters-switzerland/
https://www.prodaft.com/resource/detail/flubot-new-masssive-mobile-malware-ring-targeting-europe
https://github.com/prodaft/malware-ioc/blob/master/FluBot/FluBot.pdf
https://blogs.blackberry.com/en/2021/06/threat-thursday-flubot-android-spam-is-malware-in-disguise
https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
https://www.threatfabric.com/blogs/smishing-campaign-in-nl-spreading-cabassous-and-anatsa.html
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_anatsa_2021_v1.0.pdf
https://www.cleafy.com/documents/teabot
...
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flubot
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anatsa

Listes des IOCs disponibles permettant la détection:

Report Spam TeaBot and FluBot & IOCs
https://otx.alienvault.com/pulse/60be071c1e3cddee8b3156f2

Liste des domaines DGA associés au Botnet Flubot (Juillet 2021):
http://data.netlab360.com/feeds/dga/flubot.txt
https://gist.github.com/sysopfb/78f402f9cf2af120c61a8600c1b49b6d

Liste des sites Web compromis utilisés par le malware "Flubot"
sur le site de équipe "abuse.ch":
https://urlhaus.abuse.ch/browse/tag/Flubot/
https://urlhaus.abuse.ch/browse/tag/Anatsa/

** Autres sites Web de référence:

Site Web de référence de la lutte contre la cyber-malveillance:
https://www.cybermalveillance.gouv.fr/

Comment lutter contre les spams par SMS ou MMS:
https://www.cnil.fr/fr/cnil-direct/question/comment-lutter-contre-les-spams-par-sms-ou-mms

Qu'est-ce que le hameçonnage par SMS et comment vous en protéger ?
https://wwwkaspersky.fr/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Arnaque par SMS, comment déjouer le phishing sur smartphone:
https://www.cnetfrance.fr/news/arnaque-par-sms-comment-dejouer-le-phishing-sur-smartphone-39922573.htm

Information pour ne pas tomber dans le piège des SMS frauduleux:
https://www.frandroid.com/produits-android/smartphone/830036_sms-frauduleux-les-bons-reflexes-a-adopter-pour-ne-pas-se-faire-avoir

Les dangers des raccourcisseurs d'URL:
https://www.it-connect.fr/les-dangers-des-raccourcisseurs-durl/

Démasquez l'URL camouflée derrière un lien raccourci :
https://radiorfa.com/index.php/demasquez-lurl-camouflee-derriere-un-lien-raccourci/

Cordialement,

==========
CERT-RENATER
tel : 01-53-94-20-44
fax : 01-53-94-20-41
23 - 25 Rue Daviel
75013 Paris
email: cert@support.renater.fr
==========