Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 25 janvier 2016
N° CERTFR-2016-ACT-004

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-004

1 - La fraude aux faux ordres de virements internationaux (première partie)

Le contexte de la fraude au niveau national

Une vague d'escroqueries, apparue depuis 2010, a touché les entreprises françaises (source : Office Centrale de Répression de la Grande Délinquance Financière - OCRGDF). Ce type d'escroqueries, plus connu sous le nom d'escroquerie aux `faux ordres de virement` international (FOVI) ou `escroquerie au Président`, a connu une forte recrudescence depuis plus d'un an, avec un mode opératoire en constante évolution. Les cibles font généralement partie du service comptable ou de la trésorerie de l'entreprise victime.

La fraude peut prendre de multiples formes :

- un individu se fait passer pour le PDG et demande un virement financier vers un compte bancaire illégitime ;
- les escrocs se font passer pour des informaticiens de la banque et, sous le prétexte de tester la comptabilité de l'entreprise avec le protocole SEPA, demande à effectuer un virement bancaire soi-disant de test. Les individus peuvent même aider la victime en effectuant eux-mêmes la transaction financière via un logiciel de prise en main à distance ;
- les escrocs se font passer pour un fournisseur et demandent le paiement d'une facture sur un nouveau compte bancaire. On remarque une bonne connaissance de la relation client/ fournisseur de la part des escrocs ;
- l'action directe par les escrocs auprès de la banque détentrice des comptes ;
- l'utilisation d'un virus envoyé par message électronique (cheval de Troie permettant la prise en main de la machine de la victime ou du vol de ces mots de passe).

Les victimes ont subi de lourds préjudices pouvant se chiffrer à plusieurs millions d'euros. 55% des entreprises françaises auraient déjà subi ce type d'attaque. Le préjudice financier est important, mais il ne faut pas négliger les impacts humains au sein des entreprises victimes (e.g. licenciements, dépôt de bilan et perte d'emploi, suicides, ...).

La technique des escrocs est basée sur l'ingénierie sociale (ou `social engineering`), méthode qui a pour but d'extirper des Informations à des personnes sans qu'elles s'en rendent compte. La clé étant la force de persuasion.

Le contexte de la fraude au niveau international

Les réseaux d'escrocs ont dans un premier temps opéré en France mais leurs modes opératoires se sont exportés dans les pays francophones puis dans le monde entier (source FBI). Le développement de cette menace est ralenti par la nécessité pour les escrocs de maîtriser la langue locale, les procédures financières du pays concerné par l'attaque.

Aux Etats-Unis, on retrouve cette malveillance sous le nom de `business email compromise scams` ou `bogus boss`. Depuis deux ans, l'entité `Internet Crime Complaint Center` du FBI estime que 7000 sociétés américaines seraient impactées. Le coût total évalué durant cette période sur le territoire américain

serait de 740 millions de dollars. Dans ce contexte, les escrocs augmentent significativement l'intensité de leurs attaques en bénéficiant de complicités locales. Etant donné les gains, les acteurs historiques du scam 4.1.9 ou de l'arnaque nigérienne peuvent être tentés par ce mode opératoire.

Le mode opératoire de la fraude au faux ordre de virement

L'escroquerie aux faux ordres de virement est réalisée par l'utilisation des courriels et du téléphone. Aujourd'hui, beaucoup d'entreprises sont informées sur ce sujet, c'est pourquoi les escrocs ont tendance à abandonner le scénario du faux `président` au profit de celui du changement de RIB. Les bailleurs sociaux gérants des grands parcs immobiliers constituent une cible importante, sans être exclusive.

La préparation de l'attaque

Les escrocs vont réaliser durant plusieurs mois une démarche `d'ingénierie sociale`, permettant de collecter un maximum d'informations en source ouverte sur l'environnement économique et humain de l'entreprise cible. Les escrocs vont se renseigner en détail et s'imprégner de l'entreprise à partir d'internet et de moteurs de recherche en consultant :

- le registre du commerce, les statuts, l'état d'endettement de l'extrait K-bis ;
- les comptes rendus des comités d'entreprises ;
- les procès-verbaux d'assemblée générale ;
- les sites Internet de l'entreprise ;
- les sites Internet avec des vidéos du type : `Le mot du directeur` ;
- la presse économique ;
- les comptes Facebook et Twitter ;
- les sites Linkedin, viadeo et `les copains d'avant`.

Les escrocs utiliseront aussi la technique `Google Hacking` et des Google Dorks qui permettent d'utiliser le moteur de recherche Google (ou un autre moteur de recherche d'ailleurs) pour rechercher des fuites d'informations sensibles d'une entreprise cible.

Les escrocs pourront ainsi collecter un maximum de renseignements sur l'organigramme de l'entreprise, le nom des cadres financiers, les éventuels nominations et départs, des adresses de messagerie, des numéros de fax, et de téléphone, l'identité ainsi que les coordonnées des porteurs de parts et des dirigeants dont ils interceptent la signature au bas des documents officiels.

Ils s'imprègnent aussi des lettres de communication interne pour comprendre sa stratégie jusqu'à acquérir le langage, le vocabulaire propre à l'entreprise cible et connaître la `culture maison` afin de s'emparer des formules favorites des dirigeants dans leurs interventions, Ils peuvent aussi collecter des données de la vie privée des employés sur Facebook ou Twitter : prénom de leurs enfants, date d'anniversaire de la secrétaire de direction.

Dans certains pays, les moyens de paiement prépayés (en espèces) sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique. Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine permettant se faire croire à une correspondance légitime.

Toujours dans la phase de préparation, un complice pourra envoyer par courriel un `cheval de Troie` sous la forme d'un fichier joint apparemment banal : date de congés, organigramme, échange de mails, coordonnées d'un fournisseur ... afin de s'emparer des données sensibles d'un ordinateur cible.

Références

- Recommandations de la police nationale `http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/L-arnaque-au-president-ou-escroquerie-aux-faux-ordres-de-vir`
- Service Régional de Police Judiciaire de Clermont-Ferrand `http://www.haut-rhin.gouv.fr/content/download/9931/60796/file/Vade-mecum%20de%20l'entreprise%20.pdf`
- Recommandations de la Caisse d'Epargne `https://www.caisse-epargne.fr/cache/idf_fraudes_virements_internationaux_doc_20150520150345.pdf`
- Recommandations de la gendarmerie `http://www.cm-aveyron.fr/pdf_FOVI_N17.pdf`

- Recommandations de la gendarmerie http://www.rouen.cci.fr/Newsletter/19/FicheFOVI.pdf
- Recommandations de l'intelligence economique, l'action de l'Etat dans l'Eure http://www.eure.gouv.fr/content/download/10534/61225/file/IE_Mise_en_page%20N%C2%B0%205%20VER2.pdf
- Recommandations du Comité Economique de la région Rhone Alpes http://www.isere.gouv.fr/content/download/18670/119708/file/plaquette%20pr%C3%A9vention%20escroqueries%20aux%20virements.pdf
- Recommandations du crédit agricole http://www.credit-agricole.fr/entreprise/blog/finances/se-premunir-contre-la-fraude-aux-ordres-de-virements.html
- Recommandations du FBI IC3 http://www.ic3.gov/media/2015/150122.aspx
- Recommandations du FBI IC3 http://www.ic3.gov/media/2015/150827-1.aspx
- Glossaire SSI de l'ANSSI http://cert.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- L'enregistrement comme moyen de preuve au pénal http://www.avft.org/article.php?id_article=688
- SWIFT : (Society for Worlwide Interbank Financial Telecommunications) est un réseau crée par des banques afin de supporter les échanges interbancaires mondiaux.

2 - Porte dérobée sur FortiOS

FortiOS est le système d'exploitation utilisé sur les plateformes de sécurité réseau "FortiGate" du constructeur Fortinet.

Du code suspect a été identifié sur certaines versions du système, qui permettrait à un utilisateur malveillant de s'authentifier à distance via le protocole SSH avec les droits administrateur, à l'aide d'un compte non documenté.

Ce compte est activé sur les versions 4.3.0 jusqu'à la version 4.3.16 pour la branche 4.0 de FortiOS ainsi que sur les versions 5.0.0 jusqu'à la version 5.0.7.

D'après le bulletin de Fortinet, le code incriminé ne serait pas une porte dérobée, mais plutôt un compte générique utilisé pour communiquer avec les produits FortiManager.

Détails

Le noyau Linux de FortiOS lance le premier processus /sbin/init qui va être chargé de décompresser différentes archives contenant le système de fichiers puis d'exécuter le programme /bin/init. Ce binaire est le programme principal qui va, entre autres, gérer la communication entre un client et le serveur. C'est dans cet exécutable que se situe le code suspicieux.

Il est possible de s'authentifier avec le compte Fortimanager_Access en SSH via un paquet de type SSH_CMSG_AUTH_TIS, ce qui va déclencher une authentification de type challenge/response entre le client et le serveur.

Un challenge est envoyé à l'utilisateur, celui-ci est généré à l'aide du fichier spécial /dev/urandom qui sert d'interface au générateur de nombres pseudo-aléatoires du noyau.

Il existe trois méthodes d'authentification différentes (SHA1, SHA256 ou basée sur crypt()) et donc trois manières différentes de répondre à ce challenge. Une fois la réponse validée par le serveur, la connexion est acceptée et l'utilisateur peut profiter d'une console avec les droits administrateur.

Recommandations

Un code d'exploitation fonctionnel a été publié sur la liste de diffusion "Full Disclosure", il est donc recommandé de mettre à jour les équipements concernés avec les versions :

- à 4.3.17 ou supérieures pour la branche 4.3
- à 5.0.8 ou supérieures pour la branche 5.0
- à 5.2.0 ou supérieures pour la branche 5.2
- à 5.4.0 ou supérieures

Documentation

– Bulletin officiel de FortiGate

http://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability

3 - Rappel des avis émis

Dans la période du 18 au 24 janvier 2016, le CERT-FR a émis les publications suivantes :

– CERTFR-2016-AVI-023 : Multiples vulnérabilités dans PHP
– CERTFR-2016-AVI-024 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2016-AVI-025 : Multiples vulnérabilités dans Moodle
– CERTFR-2016-AVI-026 : Multiples vulnérabilités dans Oracle Database Server
– CERTFR-2016-AVI-027 : Multiples vulnérabilités dans Oracle Java SE
– CERTFR-2016-AVI-028 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
– CERTFR-2016-AVI-029 : Multiples vulnérabilités dans Oracle Linux and Virtualization
– CERTFR-2016-AVI-030 : Multiples vulnérabilités dans Oracle MySQL
– CERTFR-2016-AVI-031 : Multiples vulnérabilités dans les produits Apple
– CERTFR-2016-AVI-031 : Multiples vulnérabilités dans les produits Apple
– CERTFR-2016-AVI-032 : Vulnérabilité dans Cisco Modular Encoding Platform D9036
– CERTFR-2016-AVI-032 : Vulnérabilité dans Cisco Modular Encoding Platform D9036
– CERTFR-2016-AVI-033 : Vulnérabilité dans Cisco Unified Computing System Manager et Cisco Firepower 9000
– CERTFR-2016-AVI-034 : Vulnérabilité dans F5 BIG-IP

Gestion détaillée du document

25 janvier 2016 version initiale.