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 07 septembre 2015
N° CERTFR-2015-ACT-036

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-036

1 - Sécurité des Autocommutateurs

Dans leur grande majorité, les entreprises disposent d'un réseau téléphonique interne permettant à leurs employés de communiquer entre eux et vers l'extérieur. Plusieurs technologies existent pour ces réseaux : elles peuvent être analogiques ou numériques (généralement sur des réseaux IP). Les équipements gérant ces réseaux sont appelés autocommutateurs (PABX ou IPBX) et il convient de s'assurer qu'ils soient correctement sécurisés.

Risques

Un autocommutateur peut être détourné et configuré à des fins frauduleuses et déclencher des appels vers des numéros surtaxés, qui seront facturés à la victime. Le CERT-FR insiste sur le fait que ce type de fraude est couramment constaté et que les montants facturés peuvent être supérieurs à plusieurs dizaines de milliers d'euros.

Parmi les techniques fréquemment utilisées, on peut notamment citer le détournement des systèmes de messagerie vocale : certains de ces systèmes disposent en effet d'un mécanisme de notification vers l'extérieur lorsqu'un message vocal est déposé. Un attaquant peut configurer cette option pour envoyer le message de notification vers un numéro surtaxé.

Autre technique utilisée, la fonction *DISA* (Direct Inward System Access), qui permet à un utilisateur externe d'accéder aux fonctionnalités de l'autocommutateur normalement accessibles uniquement en interne. Si cette fonctionnalité est ouverte, ou si les utilisateurs y ayant accès n'ont pas choisi un mot de passe suffisamment robuste, un attaquant peut l'utiliser pour contacter des numéros surtaxés.

Il est à noter que des communications internes pouvant être confidentielles transitent à travers ces équipements, dont les défauts de configuration peuvent être exploités pour espionner les communications vocales de l'entreprise.

La fonction *d'Entrée en Tiers* permet de s'insérer dans une conversation sans invitation. L'insertion d'un tiers est généralement indiquée par un signal sonore, mais cette indication peut être désactivée. Un attaquant peut exploiter cette fonctionnalité à des fins d'espionnage des conversations téléphoniques dans l'entreprise.

La fonction *d'Interphonie* parfois appelée *Décroché Automatique*, autorise un utilisateur à appeler un autre téléphone et à le faire décrocher automatiquement sans action de l'appelé. Un attaquant peut exploiter cette fonctionnalité pour transformer un téléphone en mouchard et mettre la pièce sur écoute. Les téléphones de conférence ou pieuvres qui équipent souvent les salles de réunion sont des téléphones à part entière et peuvent donc aussi être détournés à des fins malveillantes.

Recommandations

Le CERTFR recommande de respecter au minimum les mesures suivantes :

- utiliser un réseau d'administration dédié déconnecté d'Internet pour administrer les équipements ;
- choisir des mots de passe robustes pour les comptes servant à l'administration et changer de manière systématique les mots de passe par défaut ;

– choisir des mots de passe robustes pour les comptes utilisateurs, en particulier ceux permettant d'accéder aux boîtes vocales depuis l'extérieur ;
– désactiver les fonctionnalités qui ne sont pas utilisées ;
– séparer les utilisateurs en groupes et activer seulement les fonctions dangereuses pour les groupes le nécessitant ;
– mettre en place un filtrage des numéros sortants vers des numéros surtaxés ou l'international ;
– configurer des restrictions en fonction des plages horaires ;
– maintenir les équipements à jour en appliquant dès que possible les correctifs fournis par le constructeur ;
– activer la journalisation et surveiller les journaux afin de détecter au plus tôt toute anomalie;
– sensibiliser les utilisateurs aux risques associés à l'utilisation de la téléphonie sur IP, notamment en matière de confidentialité.

2 - Présentation des RODC partie 3 - Recommandations et conclusion

Dans la deuxième partie de cette série consacrée aux RODC, les détails techniques ont été présentés. Ce dernier article liste les recommandations à suivre pour une mise en œuvre sécurisée des RODC.

Recommandations

Comme le montrent les éléments techniques détaillés dans la deuxième partie, les RODC diffèrent des RWDC, de par leurs attributs LDAP, les éléments qu'ils peuvent manipuler ou les opérations de réplication qu'ils effectuent.

Certaines recommandations propres aux RODC sont donc à appliquer :

– utiliser les RODC uniquement dans les cas d'usage définis en première partie, par exemple sur un site physique distant de sécurité moindre ;
– définir un groupe d'administration propre à chaque RODC, via l'attribut `Managed-By`, et y affecter ou retirer au besoin les administrateurs délégués ;
– ne pas retirer les entités privilégiées interdites par défaut des listes noires des RODC (du groupe global "Denied RODC Password Replication Group" ou des attributs `ms-DS-Never-Reveal-Group` de chaque RODC) ;
– interdire de manière globale à tous les RODC la mise en cache des entités non natives privilégiées du domaine (utilisateurs et machines), en les ajoutant au groupe d'interdiction "Denied RODC Password Replication Group" ;
– ne pas utiliser le groupe d'autorisation "Allowed RODC Password Replication Group". En effet, ce groupe du domaine est par défaut global à tous les RODC du domaine. Une population appartenant à ce groupe sera alors autorisée à être mise en cache sur tous les RODC. Or, lors de la mise en place d'un RODC, il convient de définir une population autorisée à être mise en cache, spécifique à celui-ci. La démarche consiste à laisser le groupe d'autorisation vide et à ajouter les populations ciblées dans l'attribut `ms-DS-Reveal-OnDemand-Group` des RODC concernés ;
– ne pas ajouter de groupes couvrant une large population aux listes blanches des RODC, tels que "Domain Users" ou "Domain Computers", qui remettraient en cause l'utilité de la liste blanche et pourraient mettre en danger le domaine ;
– définir une procédure de changement de la configuration du cache d'un RODC. En effet, il n'existe pas de moyens de purger le cache d'un RODC. Le seul moyen d'invalider les secrets d'une entité de sécurité (utilisateur ou machine) mis en cache sur un RODC, est de changer le mot de passe de cette entité sur un RWDC. Lors du changement des listes blanches ou noires de la PRP (*Password Replication Policy*) d'un RODC, il est donc nécessaire de procéder au changement de mot de passe des entités (utilisateurs et machines) nouvellement interdites ou anciennement autorisées figurant dans le cache du RODC ;
– vérifier/auditer régulièrement la liste de management (attribut `managed-By`), les listes blanche (attribut `ms-DS-Reveal-OnDemand-Group`) et noire (attribut `ms-DS-Never-Reveal-Group`), la liste des entités mises en cache sur les RODC (attribut `ms-DS-Revealed-Users`);
– ne pas modifier les attributs du schéma appartenant au `Filtered Attribute Set` (FAS), en particulier la propriété `fRODCFilteredAttribute`. En effet, cela aurait pour conséquence d'autoriser leur réplication sur des RODC. De même, il est nécessaire de vérifier que les nouveaux attributs pouvant contenir des informations sensibles, ajoutés lors d'extensions de schéma, sont bien définis comme appartenant au FAS.

Conclusion

Lorsqu'ils sont utilisés à bon escient, les RODC permettent de répondre à des problématiques de sécurité importantes, telles que le déploiement d'un contrôleur de domaine sur un site géographique où la sécurité physique n'est pas assurée, ou encore l'installation de plusieurs contrôleurs de domaine dont l'administration peut être déléguée sans augmenter le nombre d'administrateurs du domaine.

Cependant, la configuration des RODC peut s'avérer complexe, notamment dans le cas où plusieurs RODC sont utilisés au sein d'un seul et même domaine, puisque les groupes d'autorisation et d'interdiction de mise en cache des secrets d'utilisateurs sur un RODC sont des groupes globaux au domaine et sont donc communs à tous les RODC du domaine.

Une connaissance des attributs `ms-DS-Never-Reveal-Group`, `ms-DS-Reveal-OnDemand-Group` et `managed-By` des RODC est donc nécessaire afin d'arriver à une configuration plus pointue, permettant de remplir l'objectif annoncé des RODC : limiter la compromission d'un RODC à une seule population restreinte pouvant y être mise en cache, sans mettre en danger le reste du domaine.

Références

TECHNET Read-Only Domain Controller Planning and Deployment Guide - https://technet.microsoft.com/en-us/library/cc771744.aspx

MS-ADTS Active Directory Technical Specification - https://msdn.microsoft.com/en-us/library/cc223122.aspx

MS-DRSR Directory Replication Service (DRS) Remote Protocol - https://msdn.microsoft.com/en-us/library/cc228086.aspx

MS-ADOD Active Directory Protocols Overview - https://msdn.microsoft.com/en-us/library/hh871909.aspx

TECHNET Repadmin /rodcpwdrepl - https://technet.microsoft.com/en-us/library/cc742095.aspx

3 - KeyRaider

Seuls les ordiphones ayant été débridés sont en mesure d'installer des applications depuis des dépôts autres que l'`App Store`.

KeyRaider est le nom donné au dernier maliciel ciblant les ordiphones Apple ayant fait l'objet d'un débridage. Ce dernier aurait compromis 225 000 identifiants de comptes Apple. 92 échantillons appartenant à cette famille de maliciel ont été identifiés sur les dépôts tiers de distribution d'applications.

Distribution de KeyRaider

L'application en question est disponible sur le dépôt tiers Cydia, géré par la communauté chinoise Weiphone. Les utilisateurs de ces dépôts tiers peuvent librement partager leurs propres applications. L'application malveillante en question est embarquée au sein d'une application de "customisation" du système (`tweak app`), permettant d'ajouter ou modifier le comportement d'applications installées sur l'ordiphone.

Installation de KeyRaider

La charge utile se présente sous la forme d'une librairie `Mach-O`, utilisée comme greffon pour le cadriciel `MobileSubstrate`. `MobileSubstrate` est un jeu de librairies dynamiques (`dylib`) qui permet aux développeurs d'écrire des applications qui étendent ou modifient les fonctionnalités des applications déjà existantes.

A l'aide des librairies dynamiques chargées par `Mobilsubstrate`, KeyRaider est capable de modifier le comportement des fonctions système `SSLRead`, `SSLWrite` et `SecItemCopyMatching`.

Actions malveillantes

Les échantillons de cette famille de maliciels implémentent diverses fonctionnalités. La modification du comportement des fonctions sus-citées permet les actions malveillantes suivantes :

- vol des identifiants du compte Apple (identifiant, mot de passe et identifiant unique de l'ordiphone (`GUID`));
- utilisation d'identifiants subtilisés afin d'acheter des applications payantes sur l'`App Store` ;

– vol du certificat et de la clé privée associée du service de notification push d'Apple ;
– entrave au déverrouillage de l'ordiphone, via mot de passe ou via le service iCloud.

Recommandation

Le maliciel ne peut être installé qu'après débridage d'un ordiphone Apple. Les dépôts tiers n'imposent aucune réelle contrainte de sécurité et un utilisateur malveillant peut facilement mettre à disposition des applications malveillantes. Afin d'éviter la compromission de l'ordiphone, le CERT-FR recommande de ne pas le débrider et d'installer les mises à jour dès leur publication par l'éditeur.

Documentation

– Article d'analyse du maliciel KeyRaider
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/

4 - Rappel des avis émis

Dans la période du 31 août au 06 septembre 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-AVI-366 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2015-AVI-367 : Multiples vulnérabilités dans Drupal
– CERTFR-2015-AVI-368 : Multiples vulnérabilités dans Cisco Integrated Management Controller et UCS Director
– CERTFR-2015-AVI-369 : Multiples vulnérabilités dans le noyau Linux

Gestion détaillée du document

07 septembre 2015 version initiale.