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 04 janvier 2016
N° CERTFR-2016-ACT-001

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-001

1 - Exemple de typosquatting: signature de composants logiciels

Cet article fait suite à la publication du bulletin d'actualité CERTFR-2015-ACT-044, sur l'évaluation de la menace liée au typosquatting de nom de domaine. Il est question dans ce bulletin de typosquatting classique tirant parti de fautes de frappe de manière à ce que l'attaquant puisse répondre présent lorsqu'un utilisateur effectuera une erreur en tapant l'adresse d'un site Internet ou d'une adresse de courriel. Il est également question d'attaques par homoglyphes, pour lesquelles les domaines échangent par exemple la lettre i et l. Dans le cas présent, la variante utilisée est la répétition d'une lettre permettant aux attaquants la réservation d'un domaine dans le but d'obtenir un certificat numérique permettant de signer des composants logiciels en usurpant l'identité d'une société.

Durant la campagne de messages électroniques non sollicités de type Dridex du mois d'octobre 2015, décrite dans le bulletin d'alerte CERTFR-2015-ALE-012, il a été constaté que certains binaires Dridex étaient signés. Le certificat utilisé pour signer l'un de ces binaires est assigné à la société Russe Promtorg. Celle-ci possède le domaine `promtorg.ru` qui a été créé en 2004. Cependant, l'adresse de courriel renseignée au sein du certificat est l'adresse `support@prommtorg.ru`. On constate l'utilisation du domaine promtorg.ru avec une lettre m supplémentaire. Le domaine prommtorg.ru a lui été crée en 2015.

```
C:\Users\anssi>certutil crypted120med.cer
Certificat X509~:
Version~: 3
Numéro de série~: c8469b304eee2d03428875bc29134fb0
Algorithme de signature~:
ID d'objet Algorithme: 1.2.840.113549.1.1.11 sha256RSA
Paramètres de l'algorithme~:
05 00
Emetteur:
CN=COMODO RSA Code Signing CA
O=COMODO CA Limited
L=Salford
S=Greater Manchester
C=GB

 NotBefore~: 22/09/2015 01:00
 NotAfter~: 22/09/2016 00:59

Objet:
CN=Promtorg
O=Promtorg
STREET=Enginernaya 5/9
L=Novosibirsk
```

```
S=Novosibirsk
PostalCode=630090
C=RU
[...]
2.5.29.17~: indicateurs = 0, longueur = 18
Autre nom de l'objet
Nom RFC822=support@prommtorg.ru
[...]
```

La version de typosquatting présentée ici a permis à son auteur l'obtention d'un certificat valide permettant de signer des binaires au nom d'une société existante de manière à accroître la discrétion concernant la nature malveillante du code. Ainsi, malgré les avantages liés à l'utilisation de composants signés numériquement, cette technologie n'élimine pas tous les risques et cet exemple montre que le typosquatting peut être utilisé pour mener différents types d'attaques.

Documentation

- http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-044/
- http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-012/

2 - Nouvelle politique de support Internet Explorer

Contexte

En août 2014, Microsoft a annoncé une mise à jour de sa politique de support concernant le navigateur Internet Explorer. Cette nouvelle politique, applicable dès le 12 janvier 2016, précise que seule la toute dernière version d'Internet Explorer disponible pour un système d'exploitation pris en charge bénéficiera d'un support technique et de mises à jour de sécurité. En pratique, cela correspond aux combinaisons ci-dessous :

- Windows Vista SP2 : Internet Explorer 9
- Windows 7 SP1 : Internet Explorer 11
- Windows 8.1 : Internet Explorer 11
- Windows 10 : Internet Explorer 11
- Windows Server 2008 SP2 : Internet Explorer 9
- Windows Server 2008 R2 SP1 : Internet Explorer 11
- Windows Server 2012 : Internet Explorer 10
- Windows Server 2012 R2 : Internet Explorer 11

Dans tous les autres cas (par exemple Internet Explorer 8 sur Windows 7), Microsoft recommande d'envisager une migration vers l'une des combinaisons supportées. Les navigateurs Internet constituent toujours un vecteur privilégié par les attaquants pour compromettre des systèmes informatiques, c'est pourquoi le maintien en condition de sécurité de ces logiciels reste une action indispensable afin de limiter le risque d'attaques informatiques réussies.

Recommandations

Le CERT-FR recommande de n'utiliser que des navigateurs Internet supportés par leur éditeur respectif, afin de bénéficier des dernières innovations en matière de sécurité et des correctifs sur les vulnérabilités. S'il y a des adhérences logicielles entre une version antérieure du navigateur et une application interne de l'organisme, il est envisageable de dissocier les usages entre deux navigateurs. Dans ce cas, seul le navigateur maintenu à jour sera autorisé à accéder à Internet. Cette restriction peut être mise en place grâce à un relai HTTP.

Dans le cas d'Internet Explorer, Microsoft propose un guide pour faciliter la migration vers la version 11 du navigateur, tout en tenant compte des contraintes liées à un contexte d'entreprise.

Documentation

- Politique de support Microsoft concernant Internet Explorer :
  https://support.microsoft.com/fr-fr/lifecyclegp/Microsoft-Internet-Explorer
- Migration vers Internet Explorer 11 et compatibilité des applications d'entreprise :
  https://www.microsoft.com/fr-fr/download/details.aspx?id=49490

3 - Rappel des avis émis

Dans la période du 28 décembre 2015 au 03 janvier 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-564 : Vulnérabilité dans Cisco Jabber for Windows
- CERTFR-2015-AVI-565 : Vulnérabilité dans phpMyAdmin
- CERTFR-2015-AVI-566 : Multiples vulnérabilités dans Mediawiki
- CERTFR-2015-AVI-567 : Multiples vulnérabilités dans Adobe Flash
- CERTFR-2015-AVI-568 : Multiples vulnérabilités dans Wireshark

Gestion détaillée du document

04 janvier 2016 version initiale.