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 18 juillet 2014
N° CERTFR-2014-ACT-029

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-029

1 - Liste noire de certificats SSL

Un code malveillant initie généralement des communications réseau pour :

- télécharger des outils supplémentaires ;
- réceptionner des commandes depuis un serveur CC ou depuis un autre poste compromis ;
- exfiltrer des données vers des serveurs complices.

Afin de camoufler ces opérations illégitimes auprès des différents équipements de sécurité réseau, une majorité de ces codes chiffrent leurs communications au moyen de protocoles standards comme le procotole HTTPS. En effet, ce dernier est souvent autorisé au niveau de différentes passerelles et routeurs.

C'est pourquoi une société de recherche en sécurité des systèmes d'information a établi une liste noire de certificats SSL associés à des programmes malveillants tels que *Zeus* ou *Shylock*. Pour l'instant, cette liste noire est succincte (elle comporte 125 empreintes SHA1 de certificats et 89 adresses IP de serveurs associés à de tels certificats) mais permet déjà d'identifier certaines menaces. Par ailleurs, pour en faciliter l'exploitation dans des systèmes de détection d'intrusion existants, ces listes sont également disponibles sous forme de règles *Suricata* pour les empreintes SSL, ainsi que de règles *Suricata* et *Snort* pour les adresses IP.

Le CERT-FR recommande, dans un premier temps, de chercher dans les journaux d'évènements (pare-feu, IDS, IPS, serveurs mandataires, etc.) si des connexions à ces adresses IP ont été observées, traduisant potentiellement la présence de machines compromises au sein du réseau.

Il peut également être pertinent de journaliser, voire de bloquer les connexions vers ces adresses IP ou d'intégrer ces listes noires à un IDS/IPS après en avoir mesurer les éventuels effets collatéraux (blocage de sites légitimes hébergés sur des infrastructures mutualisées, etc).

Documentation

- SSL Blacklist :
  https://www.abuse.ch/?p=8180

2 - Distribution de codes malveillants à l'aide de programmes d'installations piégés

La société F-Secure a publié récemment sur son blog un article [1] au sujet de la famille de codes malveillants nommée Havex. Ces codes ont été observés dans le cadre d'attaques ciblant plusieurs secteurs industriels et en particulier celui de l'énergie. Havex se présente sous la forme d'un code principal de type « Remote Access Tool » (RAT) capable ensuite de télécharger et d'exécuter des modules complémentaires.

Le groupe responsable du code Havex, nommé Energetic Bear par Crowdstrike [2] ou Dragonfly par Symantec [3], semble manifester un intérêt particulier pour les systèmes de contrôle industriels. En effet, un des modules

d'Havex permet d'identifier au niveau d'un réseau local la présence de systèmes répondant au protocole OPC (OLE For Process Control), typiquement utilisés dans le cadre d'une installation SCADA.

Le code Havex est distribué selon trois méthodes :

- à l'aide de courriels piégés ;
- à l'aide de sites légitimes compromis et redirigeant vers le kit d'exploits « Lightsout » ;
- enfin à l'aide de programmes d'installation piégés et mis à disposition sur des sites compromis d'éditeurs de logiciels à caractère industriel.

Un article sur le site digital bond [4] nomme trois sociétés concernées par cette dernière méthode de distribution. Il s'agit de MB Connect Line (société allemande spécialisée dans les routeurs industriels), eWON (société belge développant des solutions VPN pour accéder à des installations industrielles) et d'une troisième société Suisse dont le nom n'a pas été révélé.

La société eWON a publié sur son site un communiqué [5] détaillant le traitement de l'incident de sécurité dont elle a été victime. On peut y apprendre que le programme d'installation eCatcherSetup.exe en version 4.0 a été piégé et que la version 4.1 a été mise à disposition sur le site suite au traitement de l'attaque.

Le CERT-FR recommande donc aux utilisateurs des produits des sociétés MB Connect Line et eWON, et plus généralement de tout autre logiciel en lien avec les systèmes industriels, de suivre les mesures ci-dessous :

- vérifier les signatures des programmes d'installation téléchargés ou à défaut, de comparer une empreinte cryptographique du fichier téléchargé par rapport à une liste de confiance fournie par l'éditeur ;
- tester l'innocuité des programmes téléchargés à l'aide d'un anti-virus récemment mis à jour, la plupart des antivirus du marché étant aujourd'hui capables de détecter la présence du code Havex ;
- de qualifier l'installation de nouveaux programmes sur une instance de pré-production avant d'effectuer le déploiement sur les systèmes en production ;
- enfin, d'appliquer les recommandations disponibles dans le guide « Maîtriser la SSI pour les systèmes industriels » [6] publié par l'ANSSI.

Documentation

- 1 Blog F-Secure :
  http://www.f-secure.com/weblog/archives/00002718.html
- 2 Rapport CrowdStrike :
  http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf
- 3 Rapport Symantec :
  http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group
- 4 Rapport Digital Bond :
  http://www.digitalbond.com/blog/2014/07/02/havex-hype-unhelpful-mystery/
- 5 Communiqué eWON :
  http://www.ewon.biz/en/january-security-incident-follow-up-report.html?cmp_id=7news_id=4900
- 6 Guide Maîtriser la SSI pour les systèmes industriels :
  http://www.ssi.gouv.fr/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf

3 - Rappel des avis émis

Dans la période du 11 au 17 juillet 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-310 : Vulnérabilité dans Citrix XenDesktop
- CERTFR-2014-AVI-311 : Multiples vulnérabilités dans Citrix NetScaler Application Delivery Controller et NetScaler Gateway
- CERTFR-2014-AVI-312 : Multiples vulnérabilités dans Oracle Database
- CERTFR-2014-AVI-313 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTFR-2014-AVI-314 : Multiples vulnérabilités dans Oracle E-Business Suite
- CERTFR-2014-AVI-315 : Multiples vulnérabilités dans Oracle Supply Chain
- CERTFR-2014-AVI-316 : Multiples vulnérabilités dans Oracle PeopleSoft
- CERTFR-2014-AVI-317 : Multiples vulnérabilités dans Oracle Siebel
- CERTFR-2014-AVI-318 : Multiples vulnérabilités dans Oracle Communications Applications

- CERTFR-2014-AVI-319 : Multiples vulnérabilités dans Oracle Retail
- CERTFR-2014-AVI-320 : Multiples vulnérabilités dans Oracle Java SE
- CERTFR-2014-AVI-321 : Multiples vulnérabilités dans Oracle and Sun Systems Products Suite
- CERTFR-2014-AVI-322 : Multiples vulnérabilités dans Oracle Linux and Virtualization
- CERTFR-2014-AVI-323 : Multiples vulnérabilités dans Oracle MySQL Product Suite
- CERTFR-2014-AVI-324 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2014-AVI-325 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-326 : Multiples vulnérabilités dans Drupal
- CERTFR-2014-AVI-327 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-328 : Multiples vulnérabilités dans Cisco Wireless Residential Gateway

Gestion détaillée du document

18 juillet 2014 version initiale.