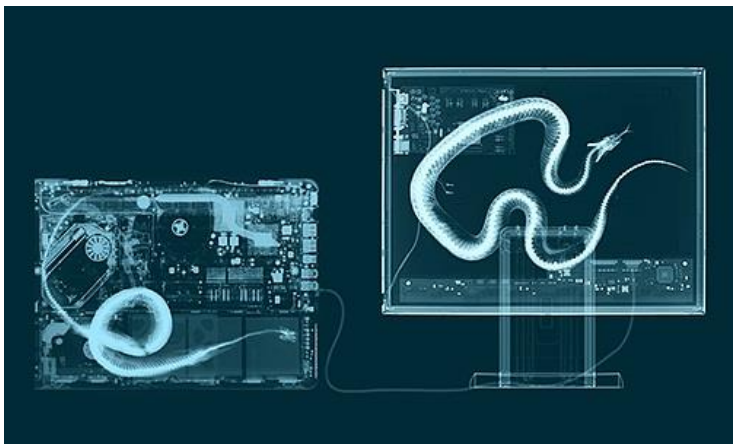
Epic Snake: la campagne de cyber-espionnage Turla se dévoile

L'opération « Epic » sert de phase de démarrage à la campagne d'infection Turla, qui comporte plusieurs étapes

Turla, également connue sous le nom de Snake ou Uroburos, est l'une des campagnes de cyber-espionnage en cours les plus sophistiquées. Lorsque la première recherche sur Turla / Snake / Uroburos a été publiée, elle ne répondait pas à une question majeure : comment les victimes ont-elles été infectées ?

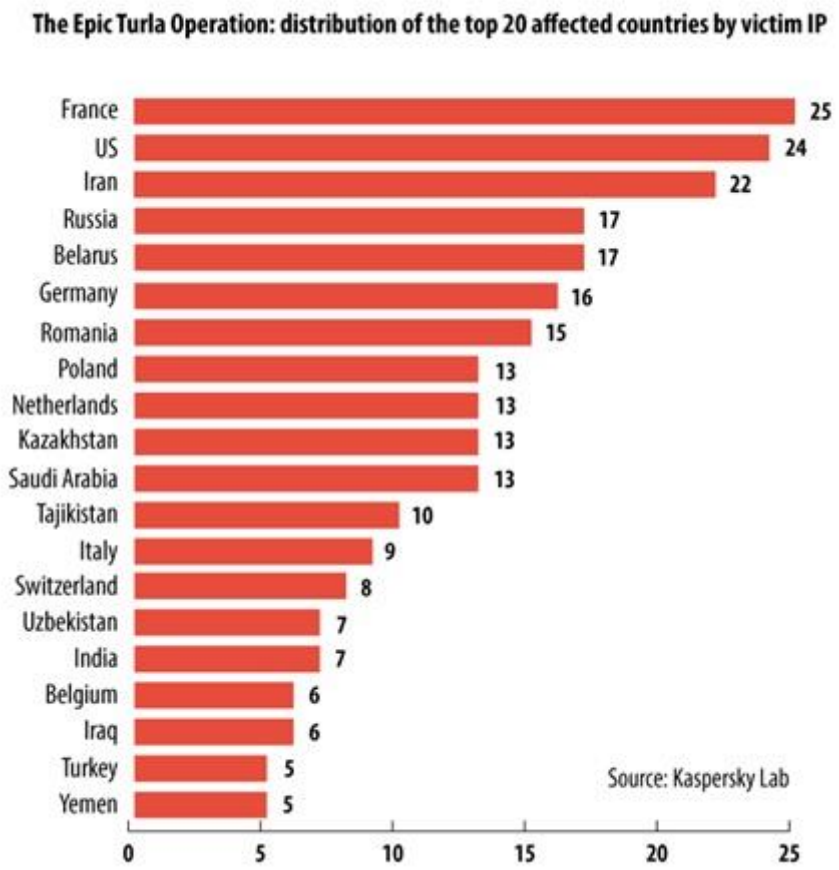


Les dernières recherches de Kaspersky Lab sur cette opération révèlent qu'Epic est l'étape initiale du mécanisme d'infection de Turla.
Pour lire le rapport complet, rendez-vous sur Securelist.com.

Turla en quelques points :

- Epic Turla / Tavdig : la phase initiale du mécanisme d'infection.
- Cobra Carbon system / Pfinet (+ autres) : mises à niveau intermédiaires et plugins de communication.
- Serpent / Uroburos : plate-forme de logiciels malveillants de haute qualité qui comprend un rootkit et des systèmes de fichiers virtuels.

Les victimes.



Le projet « Epic » est utilisé depuis au moins 2012. Il a enregistré un pic d'activité en Janvier-Février 2014. Récemment, Kaspersky Lab a détecté cette attaque contre l'un de ses utilisateurs, 05 aour 2014.

Les cibles d' « Epic » appartiennent aux catégories suivantes : entités gouvernementales (Ministères de l'Intérieur, Ministères du Commerce ou de l'industrie, Ministères des affaires étrangères / externes, les services de renseignement), les ambassades, les organisations militaires, les organisations de recherche et d'enseignement et les entreprises pharmaceutiques.

La plupart des victimes sont situées au Moyen-Orient et en Europe. Cependant, des victimes ont été identifiées dans d'autres régions, y compris les Etats-Unis. Au total, les experts de Kaspersky Lab ont dénombré plusieurs centaines d'adresses IP de victimes réparties dans plus de 45 pays, la France arrivant en tête de liste.

L'attaque.
Les chercheurs de Kaspersky Lab ont découvert que les attaquants derrière Epic Turla utilisent des exploits zero-day, de l'ingénierie sociale et des techniques de watering hole pour infecter les victimes.

Par le passé, ils ont utilisé au moins deux exploits zero-day : l'un pour l'Elévation des Privilèges (EoP) dans Windows XP et Windows Server 2003 (CVE-2013-5065), qui permet au backdoor Epic d'obtenir les droits administrateurs d'un système et de l'utiliser sans restriction ; et un exploit dans Adobe Reader (CVE-2013-3346) utilisé comme pièce jointe malicieuse.

Chaque fois qu'un utilisateur non averti ouvre un fichier PDF malveillant sur un système vulnérable, la machine sera automatiquement infectée, permettant à l'attaquant de prendre le contrôle immédiat et total du système ciblé.

Les hackers utilisent des e-mails de phishing ainsi que des attaques watering hole pour infecter leurs victimes. Les attaques détectées dans le cadre de cette opération sont différentes, en fonction du vecteur de l'infection initiale utilisé pour compromettre la victime :

- E-mails de spear-phishing avec des exploits Adobe PDF (CVE-2013-3346 + CVE-2013-5065)
- Ingénierie sociale pour tromper l'utilisateur et le forcer à lancer un programme d'installation de malware avec une extension ".SCR", parfois compressé en RAR
- Attaques watering hole utilisant des exploits Java (CVE-2012-1723), des exploits Adobe Flash (inconnu) ou des exploits Internet Explorer 6, 7, 8 (inconnu)
- Attaques watering hole reposant sur de l'ingénierie sociale pour forcer les utilisateurs à lancer des malwares de faux programmes d'installation « Flash Player »

Les attaques watering holes sont des sites Web fréquemment visités par les victimes potentielles. Ces sites sont compromis à l'avance par les hackers grâce à l'injection de codes malveillants. Selon l'adresse IP du visiteur (par exemple, les IP d'un organisme gouvernemental), les hackers utilisent des exploits Java ou des exploits de navigateurs, une fausse version signée du logiciel Adobe Flash Player ou une fausse version de Microsoft Security Essentials. Au total, nous avons observé plus de 100 sites injectés. Le choix des sites reflète l'intérêt spécifique des hackers. Par exemple, beaucoup de sites espagnols infectés appartiennent aux collectivités locales.

Une fois l'utilisateur infecté, Epic se connecte immédiatement au serveur de commande et de contrôle (C&C) pour envoyer un pack avec les informations du système de la victime. Epic est également connu sous les noms de « WorldCupSec », « TadjMakhal », « Wipbot » ou « Tadvig ».

Une fois qu'un système est compromis, les attaquants reçoivent de brèves informations sur la victime et peuvent ainsi implanter des fichiers pré-configurés contenant une série de commandes pour exécution. En plus de cela, les hackers téléchargent des outils personnalisés de « lateral movement ». Parmi eux, on trouve un keylogger spécifique, un archiveur RAR et des services standards comme un outil de requêtes DNS Microsoft.

Phase initiale de Turla :
Lors de l'analyse, les chercheurs de Kaspersky Lab ont noté que les hackers utilisant Epic déployaient un backdoor plus sophistiqué appelé « Cobra / Carbon system » ou « Pfinet » par certains produits anti-virus. Après un certain temps, les hackeurs sont allés plus loin et ont utilisé Epic afin de mettre à jour le fichier de configuration « Carbon » avec un ensemble différent de serveurs C & C. Le savoir-faire unique requis pour faire fonctionner ces deux backdoors met en évidence un lien clair et direct entre eux.

« *Les mises à jour de configuration pour le malware « Carbon system » sont intéressantes car c'est un autre projet de la campagne Turla. Cela indique que nous avons affaire à une infection en plusieurs étapes, qui commence par Epic Turla. Epic Turla est utilisé pour toucher les victimes dont le profil est critique. Si la victime est intéressante, il se met à niveau pour devenir le système* « Turla Carbon » », explique **Costin Raiu, directeur de l'équipe de recherche et de l'analyse globale de Kaspersky Lab**.

Langue & origine :
Les hackers derrière Turla ne sont clairement pas des anglais natifs. Ils orthographient souvent mal des mots ou des expressions, comme :

- *Password it´s wrong!*
- *File is not exists*
- *File is exists for edit*

D'autres indications peuvent aider à supposer l'origine des criminels. Par exemple, certaines des backdoors ont été compilées sur un système en langage russe. En outre, le nom interne de l'un des backdoors Epic est "Zagruzchik.dll», qui signifie « bootloader » ou « programme de charge » en russe.

Enfin, le panneau de commande du « vaisseau-mère » Epic définit la page de code en 1251, utilisé pour les caractères cyrilliques.

Liens avec d'autres menaces :

Fait intéressant, les connexions possibles avec différentes campagnes de cyber-espionnage ont été observées. En Février 2014, les experts de Kaspersky Lab ont constaté que les auteurs de menaces connues comme Miniduke utilisaient les mêmes web-shells pour gérer les serveurs Web infectés, ce qui est également le cas de l'équipe derrière Epic.

Pour en savoir plus, rendez-vous sur Securelist.com.

À propos de Kaspersky Lab

Kaspersky Lab est le plus grand fournisseur privé de solutions de sécurité informatique dans le monde. La société est classée parmi les 4 premiers fournisseurs de solutions de sécurité informatique pour les particuliers à l'échelle mondiale. Tout au long de ces 15 années d'existence, Kaspersky Lab n'a cessé d'innover et propose aujourd'hui des solutions de sécurité de pointe à destination des grands comptes, PME/TPE et des particuliers. Le groupe Kaspersky Lab est présent dans près de 200 pays et territoires, offrant une protection à plus de 300 millions d'utilisateurs à travers le monde. Site Web : http://www.kaspersky.com/fr/

** La société a été classée quatrième dans le classement IDC Worldwide Endpoint Security Revenue by Vendor, 2011. Ce classement a été publié dans le rapport d'IDC Worldwide IT Security Products 2012-2016 Forecast et parts de marché des fournisseurs 2011 (IDC #235930, Juillet 2012). Le rapport classe les éditeurs de logiciels selon les revenus des ventes de solutions de sécurité en 2011.*

Pour en savoir plus : www.kaspersky.com/fr/
Pour plus d'informations sur l'actualité virale : http://www.securelist.com
Salle de presse virtuelle Kaspersky Lab : http://newsroom.kaspersky.eu/fr/

Contacts presse

Hotwire pour Kaspersky Lab
Marion Delmas / Charlène Mougeot / Elodie Godart
01 43 12 55 62 / 64 / 68
kasperskyfrance@hotwirepr.com