FLASH INFO **20 décembre 2013**

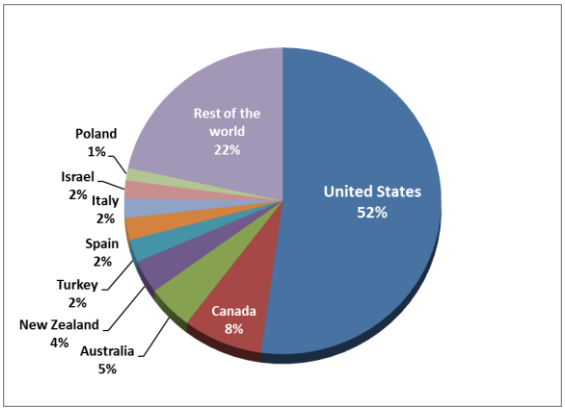
Cryptolocker 2.0 : Une nouvelle version de ransomware ?

Quelle est son origine ?

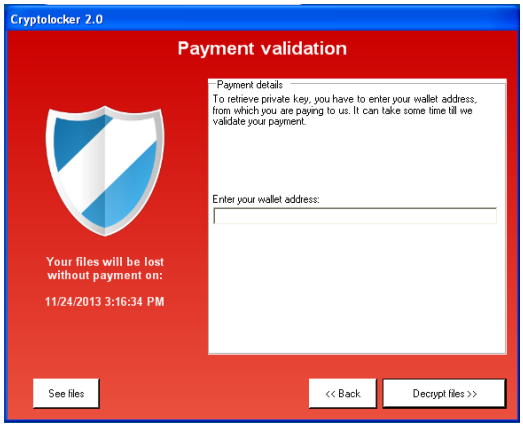
En 2013 un logiciel malveillant du type cheval de Troie est découvert : Cryptolocker. Il s'agit d'extorquer les gens en les manipulant par le chantage. Par le biais du chiffrement de données, le hacker réussit à prendre en otage les informations confidentielles de l'utilisateur et en informe ce dernier, puis il déclenche un compte à rebours pour le faire chanter. L'utilisateur doit alors payer afin de récupérer son bien.

Cryptolocker est détecté par ESET sous le nom Win32/Filecoder.BQ ou win32.Gpcode. Dans les analyses établies par les laboratoires du célèbre éditeur ESET, de juillet à septembre 2013, on remarque une forte augmentation de détections des types « ransomware » tels que le Cryptolocker, le Filecoders ou encore le Lockscreen. De nombreux pays sont touchés par ces demandes de rançons faites par les pirates sur internet, dont la France.

Les chiffres parlent d'eux-mêmes



Cryptolocker 2.0, une nouvelle escroquerie à distance



Comme nous pouvons le voir dans les captures d'écrans précédentes, le nouveau Cryptolocker ressemble de près à l'ancien. Il y a trois différences visibles entre les deux malwares. Cryptolocker utilise (comme mentionné dans le message de rançon) RSA-2048, tandis que Cryptolocker 2.0 affirme utiliser RSA-4096 (en réalité il utilise une version moindre : RSA-1024). Il affiche la date butoire avant suppression de la clé privée mais pas le compte à rebours comme c'était le cas dans le premier Cryptolocker. Enfin, il accepte comme moyens de paiement de la rançon uniquement le Bitcoins alors que les variantes des « cryptolockers » encaissaient MoneyPak, Ukash ou bons Cashu.

On peut ajouter un fait intéressant, c'est le changement de cible. Cryptolocker 2.0 est beaucoup plus tourné vers le grand public puisqu'il crypte d'autres types de fichiers, comme les images, la musique ou encore les vidéos (.mp3, .mp4, .png, .avi…). C'est-à-dire qu'il peut faire une demande de rançon contre des photographies souvenirs par exemple. Anciennement, les ransomwares visaient plutôt les entreprises.

Tableau comparatif Cryptlocker Vs Cryptlocker 2.0

	Cryptolocker	Cryptolocker 2.0
Nom de détection ESET	Win32/Filecoder.BQ	MSIL/Filecoder.D, MSIL/Filecoder.E
Langage	C++	C#
Méthode de paiement	Moneypak, Ukash, cashU, Bitcoin	Bitcoin
Algorithme de chiffrement des fichiers	AES	3DES
Algorithme de chiffrement de la clé	RSA-2048	RSA-1024
Emplacement de sauvegarde de la clé d'encryptage	Fin du fichier crypté	Fichier séparé: *%filename%.%fileext%.k*
Communication chiffrée C&C (Commande &Contrôle)	RSA	AES
Adresse C&C	Codée en dur, DGA	Codée en dur

En prenant en compte les différences entre les deux Cryptolocker, il est peu probable que le « Cryptolocker 2.0 » soit une nouvelle version du Cryptolocker et ne proviendrait pas non plus des mêmes auteurs. Il s'agit plus certainement d'une copie qu'un pirate a créé en s'inspirant du Cryptolocker à des fins illicites, c'est-à-dire gagner de l'argent en extorquant des internautes.

Pour plus d'informations : http://www.welivesecurity.com/

À propos d'ESET

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet depuis 26 ans, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 81ème récompense VB100 en août 2013, ESET NOD32 Antivirus détient le record mondial pour le nombre de récompenses Virus Bulletin (VB100), et n'a jamais manqué un seul ver ou virus « In-the-Wild » depuis le début des tests en 1998. ESET a été reconnue comme l'une des entreprises les plus innovantes en Europe pour 2011 au titre des HSBC European Business Awards et a été primée maintes fois par les laboratoires AV-Comparatives, AVTest et bien d'autres encore.
ESET NOD32, ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le monde.
ESET a son quartier général à Bratislava (Slovaquie), possède des filiales à San Diego (U.S.), Buenos Aires, et Singapour et des bureaux à Jena (Allemagne), Sao Paulo et Prague. Ses centres de recherche sont établis à Bratislava, San Diego, Buenos Aires, Singapour, Prague, Košice (Slovaquie), Cracovie (Pologne), Montréal et Moscou. ESET est également représenté dans plus de 180 pays à travers un réseau de partenaires.

À propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique.
À travers un vaste réseau de distribution, constitué de VAR, revendeurs locaux professionnels et des plus importantes enseignes spécialisées dans la distribution de logiciels, Athena Global Services propose des logiciels et équipements de sécurité novateurs destinés aux particuliers et aux entreprises, pour protéger et gérer leur environnement informatique : antivirus, pare-feu, chiffrement, politique de sécurité, authentification, sauvegarde, migration des données, et contrôle du trafic Internet.
En outre, ATHENA Global Services propose une gamme de logiciels utilitaires également dédiés à la protection et à l'optimisation des parcs informatiques. Grâce à son savoir-faire, ATHENA Global Services entretient des relations privilégiées avec les éditeurs mondiaux qui lui confient la localisation et la distribution de leurs logiciels.

Ses principaux partenaires éditeurs de solutions de sécurité :
DeviceLock – ESET Antivirus – StorageCraft – WebSure - SMSPasscode – 8Man - WhiteCanyon – EndSec Cloud Services – MDM

Ainsi que ses filiales Africa Global Services – Auxiliance – Marketing Land

Pour en savoir plus, veuillez visiter le site Internet : www.athena-gs.com

Contacts Presse
Marketing-Land – Marion Lecrique - marion.l@marketing-land.com - 01 55 89 09 60