Alerte vigilance Simplocker – L’ère des malwares 2.0 sur les mobiles a sonné : Simplocker un cryptolocker sur Android

	**Alerte vigilance Simplocker – L’ère des malwares 2.0 sur les mobiles a sonné : Simplocker un cryptolocker sur Android** Découverte intéressante d’un cheval de Troie sur mobile – Les ingénieurs de détection ESET ont repéré le week-end dernier un rançonlogiciel capable de chiffrer les fichiers sur Androïd.

Alerte vigilance Simplocker – L’ère des malwares 2.0 sur les mobiles a sonné : Simplocker un cryptolocker sur Android

Les experts savaient depuis un moment que les cybercriminels tenteraient de s’attaquer à la flotte mobile, une cible très en vogue dans un monde où le nombre d’utilisateurs frôle les 7 milliards en 2014 (Source : Union internationale des télécommunications). Tout le monde ou presque est donc susceptible d’être victime des attaques cybercriminelles en ce sens.

Découverte intéressante d’un cheval de Troie sur mobile – Les

ingénieurs de détection ESET ont repéré le week-end dernier un rançonlogiciel capable de chiffrer les fichiers sur Androïd.

Par le passé, d'autres types de malwares avaient été détectés – Un hybride comprenant les caractéristiques d'un faux antivirus (Rogue/FakeAV), combinées aux traits typiques d'un ransomware Lockscreen (sans chiffrement de fichiers) a été découvert il y a presqu'un an : ESET le nomme : Android/ FakeAV. Le mois dernier une polémique sur un ransomware de type « police/ gendarmerie » appelé Android/ Koler, n'était finalement pas « Cryptolocker » et ne chiffrait pas non plus les fichiers sur l'appareil infecté.

La situation a toutefois changé, avec cette récente découverte la semaine dernière, d'un cheval de Troie Android, détecté par ESET comme Android / Simplocker. Le malware scanne la carte SD du terminal mobile à la recherche de certains types de fichiers tels que les images, les documents, les vidéos sous les formats suivants : jpeg, png, bmp, jpg, gif, doc, docx, pdf, txt, avi, mkv, 3gp et mp4. Il les chiffre ensuite en utilisant l'algorithme AES-256 et exige une rançon afin de déchiffrer les fichiers.

Cette nouvelle menace a actuellement été repérée en Russie, un pays proche de la France, pouvant se propager à une vitesse ahurissante. Le message de la rançon est écrit en russe et le paiement exigé en hryvnias ukrainiens (monnaie Ukrainienne). Il est juste de supposer que la menace est dirigée contre cette région. Cela n'est pas surprenant, les premiers chevaux de Troie SMS pour Android (y compris Android / Fakeplayer) de 2010 provenaient également de la Russie et de l'Ukraine.

Le message du pirate :

AVERTISSEMENT votre téléphone est verrouillé!
L'appareil est verrouillé suite à la visualisation et la distribution de pornographie juvénile, zoophilie et autres

perversions.
Pour le déverrouiller, vous devez payer 260 UAH (équivalent à 16€).
1. Localisez la borne de paiement la plus proche.
2. Sélectionnez MoneXy
3. Entrez {instructions supprimées}.
4. Faites un dépôt de 260 hryvnia, puis validez.
N'oubliez pas de prendre vôtre reçu!
Après paiement, votre appareil sera débloqué dans les 24 heures.
En cas de non-paiement, vous perdrez toutes les données présentes sur votre appareil! »
Il impose à la victime de payer via le service MoneXy qui n'est pas aussi facilement traçable que l'utilisation d'une carte de crédit ordinaire.

Le cybercriminel héberge le C&C (Centre de commandes et de contrôles) du malware Android/ Simplocker sur un domaine du réseau TOR dit « oignon »,lui permettant de rester anonyme pour commander son malware à distance en toute tranquillité.

Tout comme Cryptolocker 2.0 sous le nom de Win32/Filecoder.BQ, le malware Android Simplocker livre la clé servant à décrypter les fichiers uniquement si la victime paye les 16€ qui lui sont demandés.

Important- Les recommandations d'ESET pour s'en prémunir :
Il est fortement conseillé de ne pas payer le cybercriminel. D'une part, cela encouragerait d'autres pirates du web à créer de nouvelles menaces. Et d'autre part, rien ne garantit que l'escroc remplisse sa part du marché une fois les 16€ encaissés. Il se peut en effet que l'accord ne soit pas respecté et qu'il ne déchiffre pas les fichiers.

Il est important de protéger son téléphone mobile afin de lutter contre les menaces et utiliser des mesures de prévention et de défense. Par exemple une application de sécurité pour mobile telle qu'ESET Mobile Security pour

Android permet de garder les logiciels malveillants hors de portée de votre téléphone.

Adhérer aux meilleures pratiques de sécurité, comme éviter de télécharger des applications non fiables en vérifiant les sources avant de cliquer sur des liens suspects comme par exemple : « Perdez 15 kg en 2 heures, en savoir plus. »

Sauvegarder ses fichiers, images, vidéos de tous ses appareils, que ce soit sur Android, Windows, ou tout autre système d’exploitation et le ransomware ne sera rien de plus qu’une nuisance.

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)

Références :

http://www.