ENJOY SAFER TECHNOLOGY™

CTB-Locker: Multilingual Malware Demands Ransom

Comme nous l'avons vu dans les articles publiés précédemment concernant les ransomware, comme TorrentLocker qui cible le Royaume-Uni avec phishing Roya Mail et le ransomware qui cible les pays aux alentours, ces types de menaces apparaissent de plus en plus fréquemment dans un grand nombre de pays dont la France.

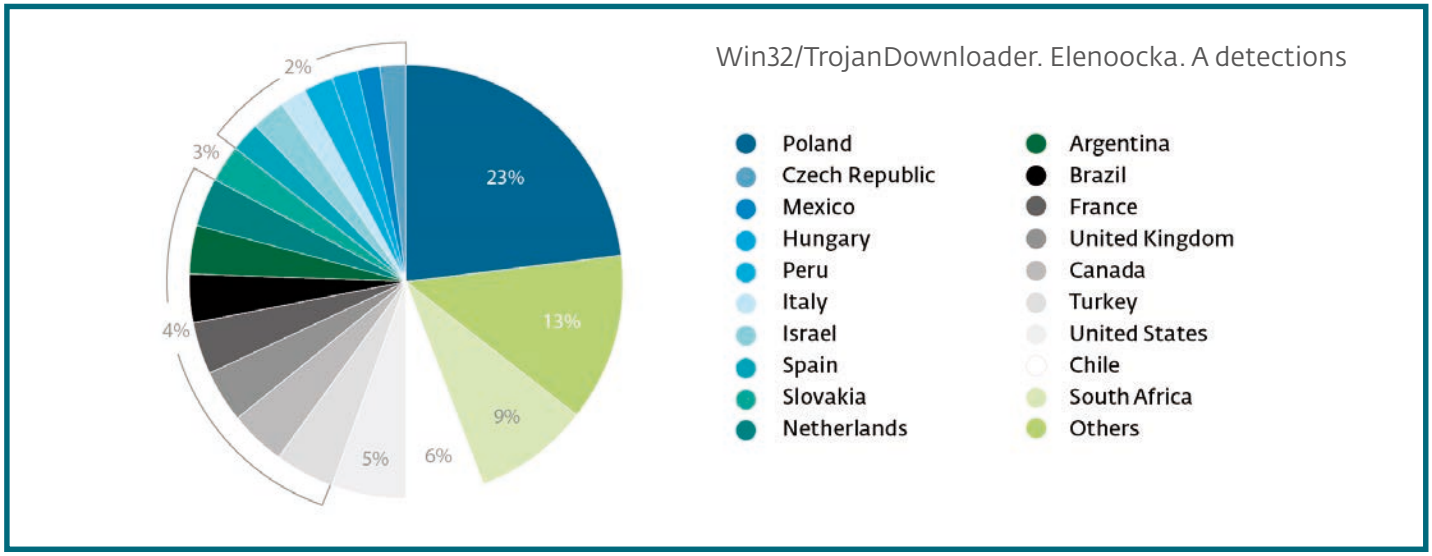
Il y a quelques jours, nous avons commencé à recevoir des rapports de plusieurs campagnes de phishing dans divers pays, principalement en Amérique latine et en Europe orientale. Cet email qui est censé contenir un fax n'est en fait rien de plus qu'une campagne visant à diffuser du code malveillant, dont le but ultime est de chiffrer les fichiers de leurs victimes, puis d'extorquer une rançon en bitcoins pour la récupération des informations chiffrées.

Subject: [Hobson Industries Ltd] 4 pages from +07786690048
From: [redacted]
Date: Mon, January 19, 2015 9:16 am
To: [redacted]
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file | Add to Address Book | View Message Details

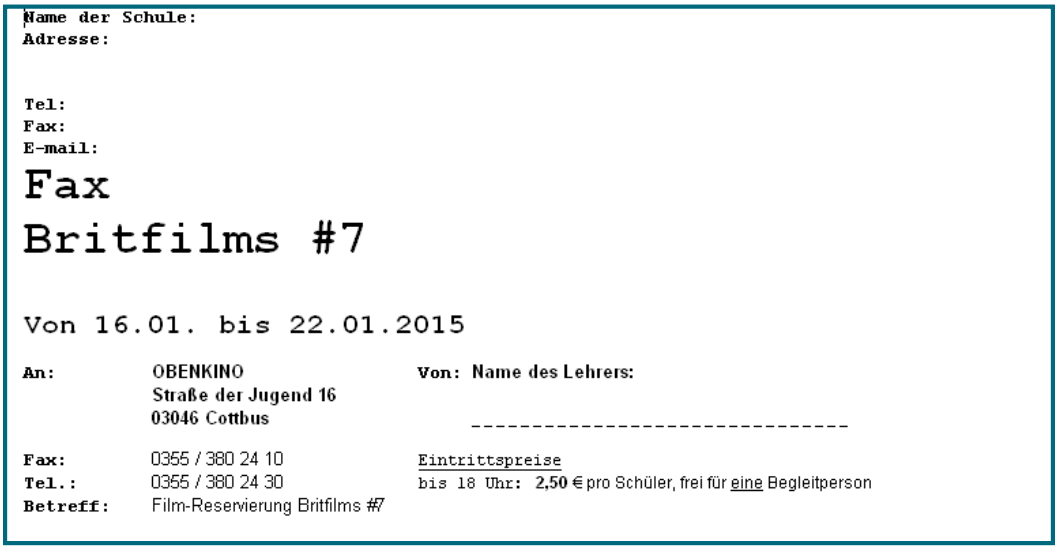
```
Number: +07786690048
Date: 2015/01/18 16:16:36 CST
Pages: 4
Reference number: AH-BF409986D-5742
Filename: mediatise.zip

--
Hobson Industries Ltd
Aida Stebbins
```

Dans cet article, nous allons voir comment ces campagnes propagent une nouvelle variante du Ransomware CTB-Locker, causant des maux de tête pour des milliers d'utilisateurs. La Pologne, la République tchèque et le Mexique font partie des pays les plus touchés, comme nous pouvons le voir dans les graphiques suivants comparant le pourcentage d'impact par pays:



Cette attaque commence par un courriel frauduleux arrivant dans la boîte de réception de l'utilisateur. Le sujet de l'email prétend que la pièce jointe est un fax; le fichier est détecté par ESET comme Win32 / TrojanDownloader. Elenoocka.A. Si vous ouvrez cette pièce jointe et que votre logiciel antivirus ne vous protège pas, une variante de Win32 / FileCoder.DA sera téléchargée sur votre système : tous vos fichiers seront chiffrés et vous les perdrez à jamais, sauf si vous payez une rançon en bitcoins pour récupérer vos informations.



Name der Schule:
Adresse:

Tel:
Fax:
E-mail:

Fax

Britfilms #7

Von 16.01. bis 22.01.2015

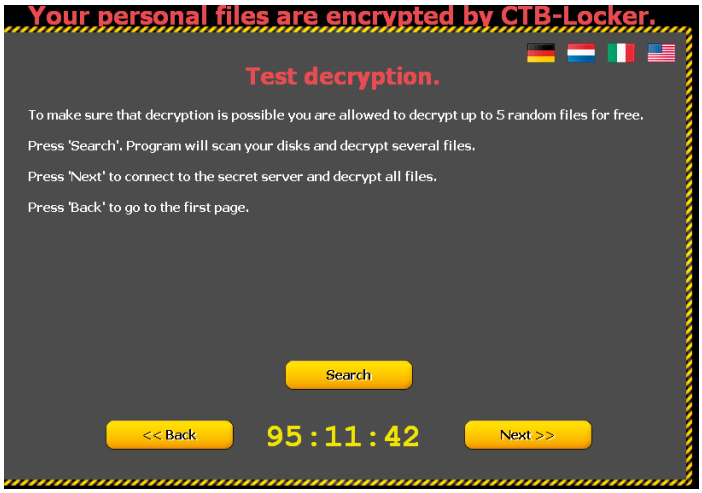
An:	OBENKINO Straße der Jugend 16 03046 Cottbus	Von: Name des Lehrers:
Fax:	0355 / 380 24 10	Eintrittspreise
Tel.:	0355 / 380 24 30	bis 18 Uhr: 2,50 € pro Schüler, frei für eine Begleitperson
Betreff:	Film-Reservierung Britfilms #7	

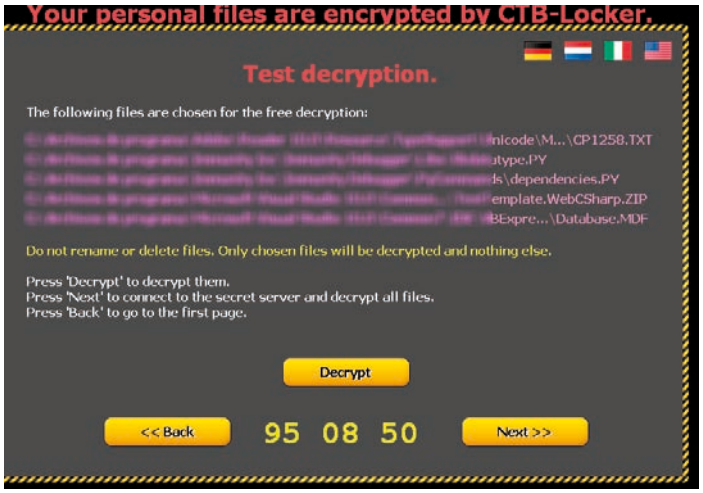
Certaines variantes de Win32 / TrojanDownloader.Elenoocka.A se connectent à une URL distante pour télécharger des logiciels malveillants qui sont détectés par ESET comme Win32 / FileCoder.DA et connu comme CTB-Locker. Cette famille de ransomware crypte tous les fichiers d'une manière similaire à CryptoLocker. La principale différence est que cette famille de malware utilise un autre algorithme de chiffrement, d'où son nom.

Le résultat est similaire à Cryptolocker ou TorrentLocker, en ce que les fichiers avec les extensions telles que .mp4, .pem, .jpg, .doc, .cer, .db etc. sont chiffrés par une clé, ce qui rend leur récupération impossible. Une fois le chiffrement des informations terminé, le logiciel malveillant affiche un avertissement et modifie également le fond d'écran avec un message similaire à celui observé dans l'image ci-dessous :

Le message sera affiché en français, en allemand, en néerlandais, en italien ou en anglais, pour s'adapter à de nombreux pays. Même si l'espagnol n'est pas l'une des langues utilisées pour afficher le message de la rançon, nous avons recensé de nombreuses infections dans les pays hispanophones.

Afin de rassurer les utilisateurs quant à la récupération de leurs fichiers une fois que le paiement est effectué, les cybercriminels offrent une démonstration sur son fonctionnement, comme vous pouvez le constater dans l'image ci-dessous :





Une fois que l'utilisateur a visualisé la démonstration, les cybercriminels montrent comment déchiffrer les fichiers et comment envoyer les bitcoins (BTC). Ils offrent même un moyen d'échanger des bitcoins au cas où l'utilisateur n'en possède pas:

Un autre détail particulier du CTB-Locker: non seulement le message est affiché à l'utilisateur dans plusieurs langues mais il affiche également la devise appropriée à cette langue. Si l'utilisateur choisit d'afficher le message en anglais, le prix est en dollars américains, sinon la valeur sera en Euros. La rançon est de 8 Bitcoins, ce qui représente aujourd'hui (20 Janvier 2015) une valeur d'environ 1680 dollars.

D'un point de vue technique, Win32 / TrojanDownloader.Elenoocka.A est une menace basique. Actuellement de nombreuses campagnes similaires à celles présentées ci-dessus se propagent. Certaines menaces contiennent des factures en pièce jointe. Nous en avons également repérée une autre qui avait une facture attachée en pièce jointe _% année_% mois_% jour-1% heure_% MIN.scr nommée par exemple. facture_2015_01_20-15_33.scr Nous avons vu que les échantillons récents utilisent de plus un mot aléatoire, par exemple : stride_invoice_2015_01_20-15_33.scr, tiger_invoice_2015_01_20-15_38.scr etc. Ensuite, il ouvre un document leurre au format RTF dans Word. Ce document se trouve dans un répertoire nommé «DATA» à l'intérieur d'une archive CAB.

Il est vrai que la technique de chiffrement utilisée par CTB-Locker rend impossible la récupération des fichiers par l'analyse des fichiers chiffrés. Voici quelques mesures de sécurité recommandées tant pour les particuliers que pour les professionnels :

- Si vous disposez une solution de sécurité pour les serveurs de messagerie, activez le filtrage par extension. Vous pourrez ainsi bloquer des fichiers malveillants avec des extensions telles que .scr, comme celle utilisée par Win32 / TrojanDownloader.Elenoocka.A.
- Évitez d'ouvrir les pièces jointes dans les courriels d'origine douteuse par exemple lorsque l'expéditeur n'est pas identifié.
- Supprimez les courriels ou marquez-les comme spam pour empêcher les autres utilisateurs et les employés de l'entreprise d'être touchés par ces menaces.
- Gardez vos solutions de sécurité à jour pour détecter les dernières menaces qui se répandent et vérifiez que la technologie ESET LiveGrid soit bien activée.
- Effectuez des sauvegardes fréquentes de vos données

Limiter ces attaques n'est pas une tâche simple, et vous devez adopter une attitude proactive par la sensibilisation et la formations aux technologies de sécurité. Suivre les conseils ci-dessus pourrait vous aider à éviter tous types de menaces similaires.