Nycom
Informatique
Rue St-Jean 20 - 1260 Nyon
Tél. 022 / 362 59 54
Fax 022 / 362 60 45
www.nycom-informatique.ch

1991 25 2016

Logiciels de rançon : grave menace pour vos données

Depuis fin 2015, nous observons une montée en puissance d'un nouveau type de malwares. Dénommés "rançongiciel" ou "ransomware", il s'agit d'une menace extrêmement grave.

Concept

Après infection d'une machine, le malware chiffre les données (crypto-ransomware) sur tous les supports accessibles (connectés à l'ordinateur) : disques durs internes ou externes, clés USB, lecteurs réseau, stockage cloud, etc.

Le but du logiciel est de les rendre inaccessibles. Une rançon est ensuite exigée afin d'obtenir la clé et le logiciel permettant de déchiffrer les données. Le montant est variable, il se situe aux environs de 1'000.- francs et doit être payée en *BitCoin* via le réseau *Tor* : les auteurs sont ainsi très difficilement traçables. Payer revient à faire confiance à des cybercriminels et participe au financement de ce type de délit : vous n'avez aucune garantie qu'ils tiendront parole.

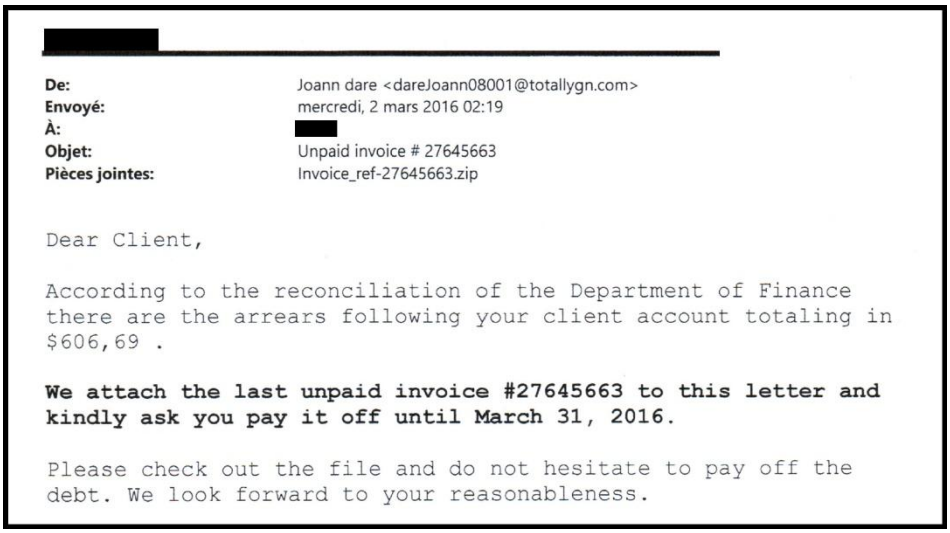
Origine

Le vecteur d'infection le plus communément observé jusqu'ici est l'email. Une version existe cependant pour les serveurs web.

Soyez donc d'une vigilance absolue dans les situations suivantes :

- Vous recevez un email (d'une adresse connue ou non).
- L'email en question contient un lien ou une pièce jointe (format zip, pdf ou doc par exemple).
- Le mot anglais "Invoice" figure dans l'email ou dans le nom de la pièce jointe.
- L'email peut aussi chercher à usurper l'identité visuelle d'une société connue.
- Une forme de pression est exercée : délai, menace de poursuite pour facture impayée, etc.

Ci-dessous, un exemple d'email infectant la machine en cas d'ouverture de la pièce jointe :



[redacted]

De: Joann dare <dareJoann08001@totallygn.com>
Envoyé: mercredi, 2 mars 2016 02:19
À: [redacted]
Objet: Unpaid invoice # 27645663
Pièces jointes: Invoice_ref-27645663.zip

Dear Client,

According to the reconciliation of the Department of Finance there are the arrears following your client account totaling in $606,69 .

We attach the last unpaid invoice #27645663 to this letter and kindly ask you pay it off until March 31, 2016.

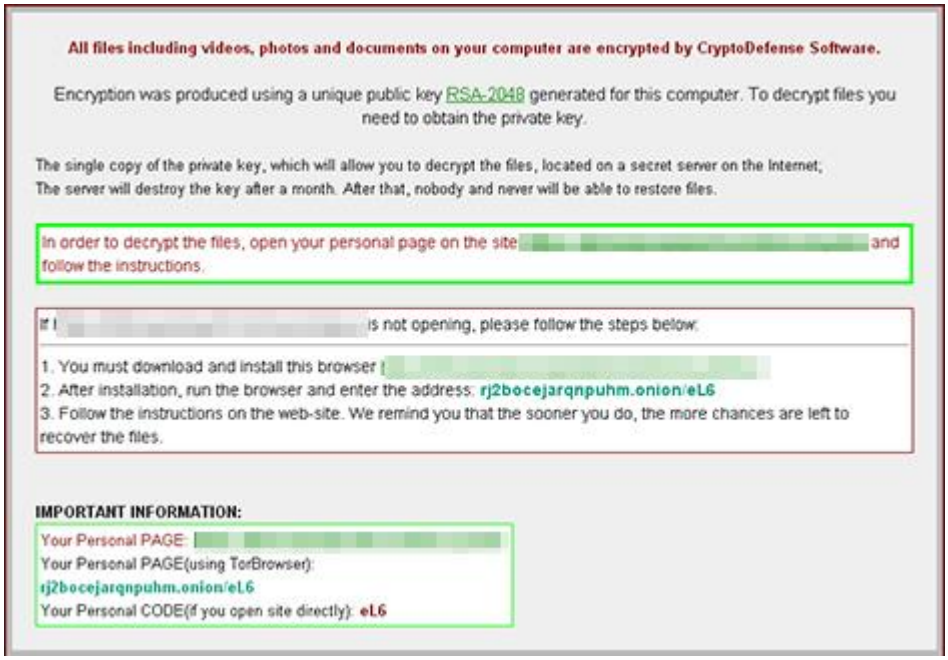
Please check out the file and do not hesitate to pay off the debt. We look forward to your reasonableness.

Symptômes

Vous remarquez que certaines de vos données sont devenues inaccessibles, de plus en plus le deviennent avec le temps. En outre, les noms des fichiers et/ou les extensions ne sont plus correctes (exemple : ma_lettre.docx devient ma_lettre.docx.vvv ou encore H4ERZ57CD.locky).

Des fichiers textes ou des fichiers images font leur apparition dans les dossiers contenant des données devenues inaccessibles (exemple : how_to_recover.txt ou what_happen_to_my_files.png).

Ci-dessous, un exemple de fichier faisant son apparition dans un dossier impacté par le chiffrement :



Solution

Les données cryptées sont irrécupérables. Si vous constatez les symptômes décrits précédemment, arrêtez immédiatement votre machine. Par précaution, éteignez également les autres ordinateurs/serveurs/NAS présents sur le réseau. Le malware ne pourra pas continuer son travail de chiffrement si les machines sont éteintes.

Le chiffrement peut parfois être long, ce qui laisse le temps de se rendre compte de la gravité de la situation avant que toutes les données personnelles ne soient chiffrées : soyez donc réactif.

Contactez-nous dans les plus brefs délais afin que nous identifiions le ou les postes touchés. Nous procéderons alors à la réinstallation complète du système et à la restauration de vos sauvegardes.

Plus que jamais, il est vital de sauvegarder régulièrement vos données sur un périphérique externe immédiatement débranché une fois la sauvegarde effectuée (principe de sauvegarde hors ligne). Redoublez de prudence, ayez du recul sur les événements et analysez la situation avant d'agir : l'ingéniosité des cybercriminels est sans limites.