Faux mail Chronopost et virus

Vu passer un mail malicieux Chronopost, qui est d'ailleurs de plus en plus utilisé comme source de SPAM malicieux ou non.
Du pur classique qui pointe vers un VPS Français.

Le mail :

avec un lien malicieux :

et qui sans surprise mène à un exécutable malicieux : http://bwc.dole.gov.ph/abx/Chronopost-Colis.exe

bwc.dole.gov.ph has address 112.199.100.77

inetnum: 112.199.0.0 - 112.199.127.255
netname: ETPI
descr: Eastern Telecom Philippines Inc.
country: PH
admin-c: RC536-AP

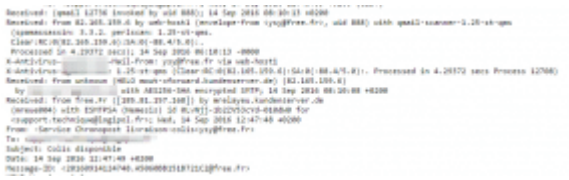
La détection VirusTotal de l'exécutable :

SHA256:	ea3049624ea76ac35126a973df1a941ce67f1262af775a161a8be2f67dc7f9a5
Nom du fichier :	Chronopost-Colis.exe
Ratio de détection :	7 / 57
Date d'analyse :	2016-09-14 12:36:37 UTC (il y a 1 minute)

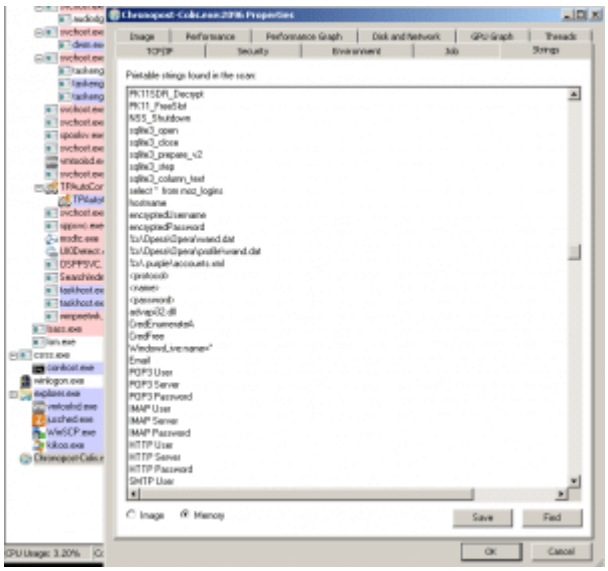
Antivirus	Résultat	Mise à jour
CrowdStrike Falcon (ML)	malicious_confidence_96% (D)	20160725

Antivirus	Résultat	Mise à jour
Invincea	virus.win32.sality.at	20160912
Kaspersky	HEUR:Packed.NSIS.MyxaH.gen	20160914
McAfee-GW-Edition	BehavesLike.Win32.Ransom.dc	20160914
Qihoo-360	HEUR/QVM42.0.0000.Malware.Gen	20160914
Rising	Malware.Heuristic!ET (rdm+)	20160914
SUPERAntiSpyware	Trojan.Agent/Gen-Kovter	20160914

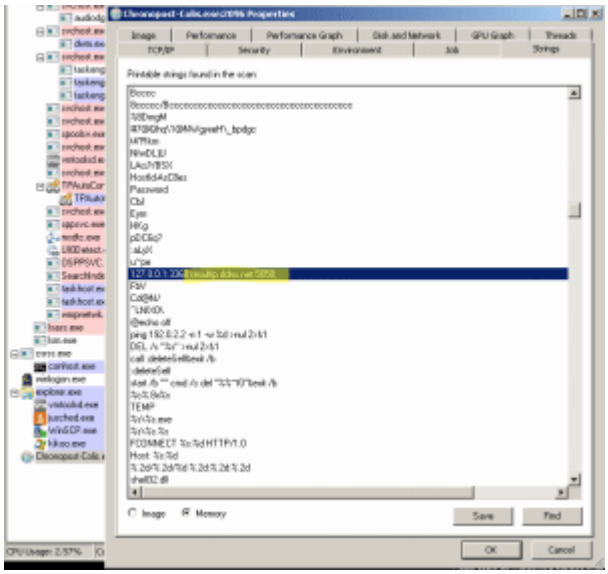
Le mail est envoyé depuis une adresse ysy@free.fr à partir d'une machine 185.81.157.168 (VPS – Inulogic Virtual Private Servers) :



Un malware qui va aller farfouiller dans les profils des navigateurs WEB pour voler des mots de passe WEB.



Le malware référence l'adresse resultip.ddns.net – encore un VPS chez Inulogic.



resultip.ddns.net has address 185.81.157.243

inetnum: 185.81.157.0 - 185.81.157.255
netname: INU-VPS01
descr: Inulogic Virtual Private Servers
country: FR
admin-c: GR8035-RIPE

Le serveur ne tournait pas au moment du test.

Il s'agit d'un RAT (Remote Tools Access) et plus précisément de Netwire RAT, un descriptif par Xylitol est disponible sur cette page : http://www.xylibox.com/2012/07/netwire-first-multi-platform-rat.html

EDIT – 23/11/2016

Toujours d'actualité, avec toujours un VPS Inulogic : 185.81.157.217
L'attaquant utilise toujours TeamViewer.