TrickBot

Synthèse

Trickbot est un Trojan bancaire, il s'agit d'une variante de **Dyre** qui est apparue en octobre 2016. Le logiciel malveillant infecte l'ordinateur de la victime et lui dérobe ses identifiants et mots de passes bancaires, comptes PayPal et plus récemment les comptes Coinbase.

Fonctionnement

Infection

Le principal vecteur d'infection est un pourriel issu d'une campagne de spam, faisant croire au destinataire à un email officiel d'une banque. L'objet de l'email est une facture ou un devis. En pièce-jointe du courrier électronique, un fichier .Word activant une macro permettant la connexion à un serveur afin de télécharger les modules complémentaires (share32Dll) du logiciel malveillant.

Le module "share32Dll" permet aux utilisateurs de Trickbot de se propager sur les réseaux associés au poste infecté et d'établir une persistance via l'enregistrement de services faisant appel aux API Windows classiques. Ce module est apparemment conçu pour être utilisé de pair avec le module "worm32Dll" pour propager Trickbot au sein des réseaux partagés et réseau local via la faille "EnternalBlue SMB" (utilisé par Wannacry et NotPetya) et le protocole LDAP.

IOC

VERSION 1000053
TrickBot :
MD5 : 1938a6103f59ab7d3d0cda69beef2a64

PAYLOAD (share32Dll):
MD5 : 116cec037647d634f86cdce4df5d0247

PAYLOAD DECODED (share32Dll)
MD5: 35d19d0910e0989287b90b0e8ff34089

USED API CALLS
WinHttpOpen
WinHttpConnect
WinHttpOpenRequest
WinHttpSendRequest

WinHttpQueryDataAvailable
WinHttpReadData
WinHttpReceiveResponse
WinHttpCloseHandle

Share32Dll delivery domains (20/09/2017):
hxxp://duhasti8.beget.tech/toler[.]png

Worm32Dll delivery domains (20/09/2017)
hxxp://duhasti8.beget.tech/worming[.]png

188.137.122.105:449;Command&Control;
188.137.122.5:449;Command&Control;
187.248.44.85:449;Command&Control;
187.248.44.84:449;Command&Control;
194.87.99.117:443;Command&Control;
195.133.145.222:443;Command&Control;
185.99.2.78:443;Command&Control;
88.150.197.173:443;Command&Control;
195.133.144.27:443;Command&Control;
194.87.99.225:443;Command&Control;
185.99.2.79:443;Command&Control;
62.141.34.242:443;Command&Control;
194.87.93.97:443;Command&Control;
5.133.179.236:443;Command&Control;
185.212.128.91:443;Command&Control;
91.211.246.131:443;Command&Control;
185.99.2.100:443;Command&Control;
95.46.45.164:443;Command&Control;
185.212.128.90:443;Command&Control;
107.167.24.135:443;Command&Control;
194.87.92.223:443;Command&Control;
194.87.238.225:443;Command&Control;
178.156.202.74:443;Command&Control;
178.156.202.117:443;Command&Control;
93.171.216.33:443;Command&Control;
93.171.217.7:443;Command&Control;

https://www.vkremez.com/2017/09/lets-learn-reversing-trickbot-banking.html