Els 5 virus més perillosos de l'any 2012

Els virus més perillosos enganyen, roben, extorsionen i a vegades s'apropien de les dades que els usuaris tenen en el seu disc dur.

La elit del programari maliciós aprofita vulnerabilitats en les aplicacions més populars per introduir-se se dins de l'ordinador, escampar-se i executar operacions no volgudes ni desitjades per el usuari durant mesos o anys.

Aquí presentem una llista dels virus més perillosos i actius que han afectat a molts ordinadors aquest any 2012. Per a tots hi ha vacunes i solucions, en alguns casos dràstiques com formatar el disc dur, però la millor és sempre la prevenció, no obrir la porta a desconeguts (correus amb adjunts d'origen estrany, pàgines desconegudes, la instal·lació de programes baixats, etc …). I el més important, tenir un Antivirus actualitzat.

SIREFEF, EL "ROOTKIT" QUE DEIXA EL PC COM UN ZOMBI

També conegut com a "ZeroAccess" és un virus complex i que es sap amagar molt bé. El seu principal propòsit és convertir el PC infectat en un node d'una enorme xarxa d'ordinadors (botnet).

El propòsit de la xarxa infectada és guanyar diners fent "clicks" en anuncis publicitaris o instal·lar falsos Antivirus que demanen diners a canvi de unes neteges immediates i miraculoses.

L'usuari se'n dona compte però l'ús de la connexió a Internet és constant i pot arribat a 50Gb mensuals de més, depenent de la velocitat de la connexió ADSL. En el pitjor dels casos, el PC zombi pot participar en accions "cyberterroristes".

La millor cura pel Sirefef és una vacuna específica com per exemple:

* Elisiref – de SATINFO Barcelona.
* ESET Sirefef EV Cleaner
* Panda Sirefef / ZAccess Desinfection Tool.

En la majoria dels casos, les infeccions es van produir al executar arxius sospitosos, en la majoria dels casos es feien passar per utilitats, còdecs de so o imatge.

REVETON, EL VIRUS DE LA POLICIA (RANSOMWARE)

Una vulnerabilitat de JAVA ha permès que des de principis de 2012, milions d'ordinadors acabessin segrestats per un virus que es fa passar per la policia.

Al·legant diversos motius com per exemple descàrrega d'arxius il·legals o el contingut en l'ordinador de pornografia infantil, el virus demana entre 50€ i 100€ per via targeta Ukash o altres sistemes de pagament.

El virus en qüestió es coneix per varis noms, Reveton, FBI Moneypak, Ransom, Rannoh, etc… però en el nostre país es coneix com el virus de la policia o SGAE.

Els remeis més infalibles, executats en "mode a prova d'errors" , són:

* Kasperky windowsUnlocker
* Polifix
* Malwarebytes

Com a mesures preventives, es recomana tenir el JAVA actualitzat (Versió 7 a dia d'avui) i fer servir eines com "Winlockless" de HISPASEC que impedeix que les aplicacions es situïn en el inici de Windows.

W32/IFRAME, LA WEB QUE ROBA CONTRASENYES (PHISHING)

L'amplia familia de virus IFrame, és la prova fefaent que una pàgina WEB pot ser perillosa. Aquests virus aprofiten la etiqueta HTML <iframe> utilitzada per inserir pàgines dins de pàgines, per injectar codi maliciós en llocs que aparentment són inofensius.

Entre les accions que aquest tipus de programari maliciós hi ha el robatori d'informació personal (phishing), l'engany (compres fraudulentes), l'enviament de publicitat no sol·licitada o l'atac a altres llocs WEB mitjançant tècniques de DOS (Denegació de Servei).

L'eliminació d'aquests virus corre a càrrec dels propietaris de les pàgines WEB infectades, ja que si no netejen el codi de les seves pàgines i no actualitzen el programari del seu servidor, la infecció continuarà ubicada en el servidor. També és important que es defineixin contrasenyes segures en el cas que s'utilitzi un gestor de continguts com "Wordpress" o "Drupal".

Per l'usuari la millor defensa consisteix en utilitzar verificadors de reputació i navegadors segurs com el Chrome que obre cada pàgina en una cel·la de memòria aïllada o instal·lar la extensió WOT (Web of trust) en els navegadors Firefox i Explorer.

També es pot instal·lar el Browser defender en el Firefox que filtrarà els resultats de les pàgines obtingudes en una cerca a google.

DORKBOT, EL VIRUS DE SKYPE (CHAT)

El troià Dorkbot és un exemple de virus "sociable", es propaga per via SKYPE amb els missatges falsos i arxius ZIP que una vegada oberts, instal·len un segrestador similar al del virus Reveton.

El que defineix Dorkbot és que s'aprofita de la confiança dels usuaris (enginyeria social), un atac contra el que cap Antivirus ens pot defensar. Si la infecció és voluntària no s'hi pot actuar.

La desinfecció es pot fer amb un antivirus instal·lat en un LiveCD o treient el disc dur del PC i connectant-lo com a secundari en un altre ordinador que ja tindrà instal·lat un Antivirus actualitzat, ja que aquest virus no ens permet arribar al escriptori quan posem en funcionament el nostre PC.

Per prevenir la infecció s'aconsella configurar SKYPE per tal d'estalviar-nos sorpreses d'aquest tipus i per suposat utilitzar el Xat amb sentit comú.

DNSCHANGER, EL SABOTEJADOR DE CONNEXIONS (HIJACKER)

Ha sigut un dels virus més sonats de l'any 2012, i encara se'n segueix parlant. És el DNSChanger i derivats, uns virus que modifiquen la configuració del sistema per tal que tota la navegació sigui redirigida a pàgines amb publicitat.

Després de que els servidors DNS utilitzats per el virus s'apaguessin per les autoritats, desenes de milers d'usuaris es varen quedar sense connexió (realment si que tenien connexió però no tenien cap servidor de noms que resolgués el nom del domini a la IP correcte). Però això no ha acabat, amb el perill de les variants d'aquest sabotejador com "RSPlug", "Zlob" o "Puper" poden seguir donant molts problemes als navegants.

Per tal de poder restablir la configuració de DNS i eliminar els efectes dels virus canviadors de DNS, es recomanen les següents eines de seguretat:

*Avira DNS-Change-Tool
*Kaspersky TDSKiller
*McAfee AVERT Stinger

La infecció es pot prevenir seguint els criteris explicats anteriorment per navegar de forma segura i evitar infeccions accidentals.

El que ens pot servir per descobrir si estem patint una infecció és l'aparició de pàgines "estranyes" o inesperades alhora de navegar.

No cal ser desconfiat però si previngut.

Article publicat el 27 de desembre de 2012 en http://gbinfor.blog.cat/