

Virus: 25 anys de mutacions

SELENA SORO | Actualitzada el 13/07/2012 00:00

Avui fa 25 anys del famós virus Divendres 13, un *malware* que només actuava aquest dia i que als anys 80 va sorprendre milers d'usuaris desprotegits, en una època en què els virus només els curaven els metges i el Divendres 13 tan sols feia pensar en els mals auguris i en les pel·lícules de terror.

Aquest dimarts, l'FBI va alertar que un *malware* anomenat DNS Changer podria deixar sense connexió més de 250.000 internautes d'arreu del món. Finalment, però, el virus va tenir un impacte "mínim", segons les empreses subministradores d'internet. Dimarts a mitjanit només 47.000 ordinadors continuaven afectats.

Cinc lustres després del Divendres 13, els virus s'han fet més sofisticats, però també més inofensius per als usuaris corrents. Els antivirus són ara més efectius i poden preveure nous *malware* amb més facilitat, explica Vicente Díaz, analista sènior de Kaspersky Lab.

Els *hackers* es troben que ho tenen més complicat, i l'única esclatxa per atacar és l'imprevist. Per aquest motiu, afirma Díaz, el virus en l'àmbit domèstic es desplaçarà els pròxims temps cap als dispositius mòbils (*smartphones* i tauletes) i cap als ordinadors Macintosh. "Als Mac també hi poden entrar virus, però fins ara tenien menys usuaris i no sortia a compte; els Mac i els *smartphones* són camp fèrtil tenint en compte que la gent no s'ho espera", comenta.

Tot i això, cada cop són menys els *hackers* que es dediquen a esborrar discs durs, i més els que roben dades. Ahir mateix Yahoo! va confirmar la sostracció de 400.000 noms i contrasenyes. Un grup anònim de *hackers* va reivindicar l'atac com un avís per demostrar l'escassa seguretat de la plataforma.

Però fins i tot aquestes intrusions s'estan quedant enrere. Molts *hackers* rendibilitzen les seves capacitats treballant en espionatge industrial i entre països, i deixen de banda els sabotatges contra usuaris corrents.

Canvi de motivacions

"Avui el que més els mou són els diners", apunta Díaz. "Abans, en canvi, els ciberdelinqüents creaven virus per demostrar la seva habilitat tècnica i guanyar prestigi dins els seus cercles", afirma Díaz.

Josep Domingo-Ferrer, doctor expert en seguretat informàtica i professor a la URV, explica que molts dels virus que es creen els desenvolupen governs per atacar ordinadors d'altres països. "Algunes potències asiàtiques tenen unitats de l'exèrcit dedicades a ciberseguretat i també a ciberatacs", manifesta.



Aquest dimarts es van obrir diverses pàgines web perquè els usuaris poguessin comprovar que no estaven infectats pel virus DNS Changer. ARA



L'any 2011, el departament de defensa dels Estats Units va fer oficial la seva nova estratègia de defensa cibernètica: els atacs i els sabotatges contra el país a través d'internet s'elevaven a actes de guerra.

Amb aquesta etiqueta, si en un atac cibernètic es produïen danys generalitzats, es perdien vides humanes o hi havia algun perjudici econòmic significatiu, "el president consideraria respondre amb els mitjans al seu abast: econòmics, diplomàtics i, com a últim recurs, militars", segons va comunicar aleshores el subsecretari de defensa, William Lynn.

A l'estat espanyol hi ha diversos organismes que disposen de "capacitats de prevenció i resposta davant les ciberamenaces", segons recull l'Estratègia Espanyola de Seguretat, presentada a Madrid l'any passat. Aquests organismes estan distribuïts i inclosos en diverses entitats: el Centre Criptogràfic Nacional, el Centre de Protecció d'Infraestructures Crítiques i les forces armades.

MÉS CONTINGUTS MÈDIA

Tropicàlia

**Neox pren 'Padre de familia'
a La Sexta**

**Nous migdies a Catalunya
Ràdio: Un concurs i un
programa de servei**