

“La xarxa es convertirà en un escenari bèl·lic”



Eugene Kaspersky (Novorossisk, Rússia, 1965), fundador d'una empresa de seguretat informàtica, parla sobre els atacs pirata recents a multinacionals com Google i Sony i de la guerra virtual amb virus com l'Stuxnet.

Senyor Kaspersky, quan va ser l'última vegada que un especialista en antivirus com vós va ser víctima d'un atac virtual?

—Recentment, gairebé m'infecten l'ordinador dues vegades. En una conferència em van tornar la targeta de memòria amb un virus, però el nostre propi programa antivirus em va ajudar. En la segona ocasió, la pàgina web d'un hotel de Xipre estava infectada. Situacions semblants li passen a qualsevol, tant se val que hom siga molt prudent. Com qualsevol altra persona necessita protecció. Al cap i a la fi, un especialista en malalties de transmissió sexual també confia en els preservatius.

—De vegades els viròlegs s'entusiasmen per la perfecció mortífera dels seus objectes d'investigació. A vós també us pot entusiasmar la tècnica d'un virus informàtic?

—Com més enginyós resulta un virus, més fascinant és desxifrar-ne el codi. Si ho aconseguisc estic content. És cert que de vegades sent cert respecte professional, però no té res a veure amb entusiasme. Cada virus és un delictes. Els pirates informàtics són dolents. No en contractaria cap.

—Vós i la vostra empresa heu guanyat la guerra d'una nova era.

—No, perquè aquesta guerra no es pot guanyar. Només coneix delinqüents i víctimes. Allò que podem aconseguir solament és evitar que tot es descontrola. Només existirien dues solucions definitives, que no són convenients: prohibir els ordinadors... o les persones.

—La vostra empresa, Kaspersky Lab, té poc més de dos mil empleats. Això no obstant, és una empresa menuda si la comparem amb McAfee i Symantec. Les podreu abastar mai?

—En tot cas, és el que intentem. El nostre avantatge més important pel que fa a competència és Rússia. Moscou forma els millors programadors del món. Té una infinitat d'universitats tècniques eminentes. Certament els russos no saben construir automòbils com els alemanys, però escriuen programari de manera excel·lent.

—Fa temps us vau formar com expert en criptologia al KGB. Interfereix aquest fet en l'expansió cap a l'est?

—No, sinó més aviat el fet que si-
guem una empresa amb arrels russes.
Ocasionalment percebem desconfian-
ça. Malgrat tot, hem arribat a ser els
primers a Alemanya, creixem amb ra-
pidesa als EUA i fins i tot tenim clients
a la mateixa OTAN.

—**Qui?**

—Un ministre de Defensa. No reve-
laré de quin país.

—**De quins països provenen la
majoria de paràsits virtuals?**

—No es pot analitzar des d'aquesta
perspectiva, perquè els virus no porten
carnet d'identitat. Tanmateix la majo-
ria de les vegades podem identificar
l'idioma de l'autor, just en el moment
en què el creador es comunica amb el
virus i li dona una ordre.

—**Els programadors russos no es
dediquen només a fer el bé. Supo-
sem que també dominen el negoci
dels virus.**

—Segons els virus programats, som
al tercer lloc a escala mundial, per
darrere de la Xina i l'Amèrica Llatina.
Tanmateix els russos, lamentablement,
són els més refinats i capdavanters
en els negocis cibernètics criminals.
Avui dia creen virus i els cavalls de
Troia més complexos per encàrrec.
Blanquegen diners a través d'Internet.
Amb tot, la major part del programari
maliciós està escrita en xinès. Per tant,
pot provenir directament de la Repú-
blica Popular, però també de Singapur,
Malàisia, i fins i tot de Califòrnia, per-
què allí també hi ha pirates informàtics
que parlen mandarí.

—**Sorprenentment sembla que no-
més pocs virus provenen de l'Índia,
un país pròsper en tecnologies de la
informació i de la comunicació.**

—A l'Índia el nivell de criminalitat
és generalment baix. Aquesta és una
qüestió de mentalitat. L'Índia i la Xina
tenen aproximadament el mateix nom-
bre d'habitants, la mateixa densitat
d'ordinadors, un estàndard de vida i
unes arrels religioses semblants. Però
la Xina transmet virus sense parar.

—**Per què provenen de Rússia al-
gunes de les xarxes de pirates infor-
màtics més perilloses, però en canvi
té poques empreses de programari
de nivell internacional, com ara la
vostra?**

—N'hi ha algunes, però hi veig un
problema bàsic: el nivell d'ensenyam-

ment tècnic és tradicionalment elevat
i des de fa generacions es transmet de
professors a alumnes; això no obstant,
no hi ha professors que ensenyen com
crear una empresa a partir d'aquests
coneixements, perquè durant deu dè-
cades de comunisme no es podia par-
lar d'establir negocis. La majoria dels
dirigents de les empreses actuals van
nàixer als anys cinquanta, és a dir, a
l'època de la Unió Soviètica. Avui dia
encara tenen una mena de teló d'acer
mental. Els agrada viatjar a l'estranger
durant les vacances, però per als
negocis sovint es limiten als països
de l'antiga Unió Soviètica, perquè allí
hom parla la mateixa llengua, i tam-
bé entenen la cultura. Confie en una
generació nova, que ja no senta por
davant d'altres cultures, i que parle
anglès.

**“És probable que
l'Stuxnet sigui un
projecte d'Israel i
els EUA”**

—**Fa poc, el motor de cerca rus
Yandex va aconseguir 1.300 milions
de dòlars en la cotització en borsa
a Nova York, el millor resultat del
sector des de Google...**

—...cosa que representa un senyal
molt important per a tots els russos:
una empresa russa ha demostrat que
amb la força de la nostra intel·ligència,
i no amb matèries primeres, es pot te-
nir èxit. Hi ha un somni americà, i ara
també hi haurà un somni rus: guanyar
diners sense dedicar-se al petroli i al
gas.

—**Una vegada us vau descriure
com un gran paranoic. Quina seria
la pitjor catàstrofe que poden oca-
sionar els virus?**

—En els temps de la Unió Soviètica
fèiem broma sobre que un optimista
aprendria anglès perquè esperava que
el país s'obriera; un pessimista estudia-
ria xinès de valent perquè temeria que
els xinesos ens conqueriren; i, men-
trestant, el realista practicaria el co-
merç amb kalàixnikovs. Avui és així,
l'optimista aprèn xinès, el pessimista
aprèn àrab...

—...i el realista?

—Segueix comerciant amb kalàix-
nikovs. Actualment, fins i tot els nord-
americans afirmen obertament que
respondrien a un atac informàtic amb
un atac militar clàssic. Però, què faran
si el ciberatac contra els EUA es pro-
dueix des del seu propi país? Avui tot
depèn dels ordinadors, el subministra-
ment d'energia, els avions, els trens.
Tem que d'ací a poc temps la xarxa
es convertirà en un escenari bèl·lic, en
una plataforma per als atacs profes-
sionals a infraestructures vitals.

—**Quan ocorrerà?**

—Ahir. Ja hi ha hagut atacs d'aques-
ta mena.

—**Us referiu al supervirus Stux-
net? Es diu que va ser programat
per sabotejar plantes nuclears ira-
nianes.**

—Lamentablement, l'agència d'in-
tel·ligència israeliana no ens envia
informes. A Internet i als mitjans es va
parlar molt que Stuxnet era un projecte
comú d'Israel i els EUA. Considere
que és l'opció més probable. Per cert,
va ser un treball molt professional,
que realment m'imposa respecte, va
costar molts milions de dòlars i un
equip d'enginyers altament qualificats
se'n degué ocupar durant molts mesos.
No va ser fruit del treball d'amateurs,
sinó de persones completament pro-
fessionals i molt serioses, amb les
quals cal evitar enemistar-se. Són molt
susceptibles.

—**Quins danys pot causar un su-
pervirus com aquest?**

—Recordeu l'apagada general a
gran part dels EUA l'agost del 2003?
Avui estic bastant segur que aquesta
catàstrofe la va causar un virus. I d'ai-
xò ja fa vuit anys.

—**Ens voleu fer por com un bom-
ber que descriu els perills del foc
de manera especialment dramàtica
perquè, al cap i a la fi, guanya diners
amb la prevenció?**

—Si només m'interessaren els di-
ners, fa temps que la meua empresa
hauria entrat en borsa. Tant si em
creieu com si no, en primer lloc vull
netejar un poc el món. Els diners són
 importants, però vindran sols si faig bé
el meu treball.

—**De fa poc temps ençà, els pirates
informàtics tenen sempre en el punt
de mira empreses com ara Lockheed
Martin, Google o Sony...**

—...simplement perquè poden entrar en els seus sistemes de seguretat per accedir a informació confidencial. Això posa en perill les empreses, però també nacions senceres. Es tracta de la indústria de l'espionatge privat, en què també hi ha estats implicats.

—**Voleu dir que hi ha governs darrere de molts atacs?**

—No ho descarte.

—**Google va explicar que hi havia rastres de l'atac al seu servei de correu electrònic que conduïen fins a la Xina.**

—En aquest cas no tinc cap informació que la Xina en siga realment l'autora. Els professionals treballen amb servidors intermediaris, que poden estar a la Xina, però que es poden controlar des dels Estats Units. És possible que fóra la competència, mentre que ara tothom assenyala la Xina. En aquest negoci hi ha de tot.

—**L'any 2007, Estònia va provocar la ira dels russos, quan va retirar un monument a l'Exèrcit Roig. S'amagava el Kremlin darrere del posterior atac cibernètic a aquest país menut?**

—El govern, no, però sí els emissors de correu brossa indignats, que van dirigir equips de xarxes informàtiques especials, anomenats botnets, contra Estònia. Va ser el prototip d'un atac informàtic bèl·lic a un estat. Els atacants no només van paraitzar les pàgines governamentals, sinó que també van enviar tant de correu brossa que ràpidament va col·lapsar els servidors a Estònia. El país va quedar aïllat del món. Els sistemes bancaris, el comerç, el transport, tot va quedar paralitzat.

—**Els pirates informàtics russos també poden deixar Alemanya fora de combat?**

—(Riu) Això no ho fem. Aleshores qui ens compraria gas?

—**Què opineu del moviment Anonymous, en què s'agrupen molts fanàtics d'Internet i pirates informàtics en un grup poc tangible i realitzen accions de guerrilla?**

—Opine que fins ara Anonymous no ha causat danys importants, però tampoc defenc el moviment. Hi ha persones amb bones intencions que només volen indicar fallades en la seguretat, i n'hi ha d'altres amb males intencions. Imagineu-vos que deixeu



“Les xarxes socials faciliten el treball dels criminals”

les claus de casa al pany. Algunes persones us cridarien i us avisarien, mentre que d'altres difondrien per tota la ciutat que el vostre pis es troba obert ara mateix. Així és Anonymous. Imprevisible.

—**Terroristes com els d'al-Qaeda també podrien dirigir una guerra cibernètica en el futur.**

—Els terroristes utilitzen la xarxa per a la comunicació, la propaganda i el reclutament de membres nous i de fons de finançament. Fins ara, els cibercriminals altament qualificats són prou intel·ligents per no mesclar-se amb terroristes. Això no obstant, en el futur cal comptar amb ciberatacs a fàbriques, avions i centrals energètiques. Penseu en la quarta part de *Die Hard*...

—**...en què Bruce Willis s'ha d'imposar a un exèrcit de joves pirates informàtics.**

—La meitat del film és poesia a l'estil de Hollywood, l'altra meitat és absolutament realista. Això em preocupa.

—**No fa gaire van segrestar el vostre fill Ivan, de vint anys. Pocs dies després el van poder alliberar il·lès. Com és de perillós ser ric a Rússia?**

—Més perillós que a Munic, però menys que a Colòmbia, on, quan vaig anar-hi de vacances la major part del temps viatjava en un cotxe blindat. També segresten fills d'empresaris en altres països. Gràcies a Déu les autoritats russes i el meu servei de seguretat van poder alliberar Ivan. El meu fill va tenir part de culpa en el seu segrest, havia propagat als quatre vents la seua adreça al Facebook. En aquest aspecte, fa anys que li advertisc de no exposar cap informació personal a Internet. Les xarxes socials com ara Facebook o Twitter faciliten el treball dels criminals.

—**El vostre fill estudia matemàtiques i treballa com a programador. Es farà càrrec algun dia de l'empresa?**

—Si és bo, és possible.

—**A Silicon Valley pul·lulen els investigadors russos. Heu volgut anar mai als Estats Units?**

—Una vegada, l'any 1992. Acabava de tornar de Hannover a Moscou del meu primer viatge a Occident. Llavors, en pensar en el meu país, només podia moure el cap horroritzat. La diferència de nivell de prosperitat era immensa. Ara ha disminuït clarament i a través dels meus viatges m'he adonat que a tot arreu hi ha avantatges i desavantatges socials, econòmics i polítics.

**Matthias Schupp
Thomas Tuma**

Traducció de Blanca Juan