Den stora marknaden för IT-virus

Av Cecilia Gabizon, översättning E P S Agrell.

På Internet säljs allt: bankkortsnummer, verktygslåda för bedrägeri à 100 euros, spionprogramvara à 50 000 euros.

Redan under internets allra första tid föddes som en tvilling vårt första IT-virus, Creeper. Det firar nu sin fyrtioårsdag som en tandlös förfader, en hantverksprodukt; att jämföra med dagens industriprodukter. Vi har nu över 200 miljoner sådana. Varje vecka uppenbarar sig 10 000 nya malware/maliciels beredda att snatta, spionera, blockera och förstöra för miljardtals datorer. Marknaden för virus blomstrar inklusive designsida, grossistled, detaljister, verkställare och vanliga datoranvändare som ovetande medverkar.

Det finns virus för varje budget. För 100 euros kan man få den enklaste modellen. Vidare kan man hyra ett nät av infekterade datorer, botnets, för spridningen. Priserna sjunker och vi har sett specialerbjudanden för 8 euros i timmen. En sådan insats räcker för att infektera 15000 datorer, försäkrar de missdådare som säljer dessa tjänster. Endagshyran går annars på 100 euros alternativt 40 euros per gång enligt vad som fullt öppet skrivs på Internet. Denna stora torghandel sker praktiskt taget för öppen ridå. Det räcker att hitta till rätt sight. Där kan sedan envar bereda sin attack, sitt bedrägeri. Allt är till salu. För att eliminera en konkurrents webbsida räcker det att lansera en operation att stoppa all dess tjänsteutövning (DDoS) vilket inte behöver kosta mer än 500 à 1500 euros enligt vad F-Secure kunnat inhämta. Man kan köpa tio miljoner epostadresser för 140 euros och sedan organisera ett svep efter bankdata för 700 euros.

Merparten av köpare inriktar sina köp mot virus av mellankvalité, vars pris varierar mellan 200 och 2000 euros. Detta är modern malware för att ta kontroll över andras PC, inte alltför komplicerad men dock med förmåga att ändra utseende för att undvika säkerhetssystemens skydd. En lösnäsa, en blomma eller en mössa räcker ofta för att lura de första kontrollerna.

Nätverk av zombiedatorer

De flesta har fabricerats österut, förklarar Guillaume Lauvet, forskare i IT-säkerhet hos det internationella storföretaget Fortinet. *Ingenjörerna i de före-detta Sovjetrepublikerna är lika kompetenta som illa betalda. Alltså fabricerar de egna virus som ett andra arbete. I och med krisen har söndagsuppfinnare uppenbarat sig, som driver dessa affärer just under veckosluten*. Väl färdiga säljs sedan deras produkter via IRC (Internet Relay Chat)[1] f v b olika andra distributionsnät där de förses med passabla identiteter för att spridas till tusentals datorer. Näten kan så låta sig betjänas antingen av aningslösa personer när dessa använder sin dator eller av fjärrstyrda Zombie-datorer. Sex till sju miljoner av dessa robotiserade datorer arbetar dagligen med att fabricera floder av virus som sedan sprids med snabbaste teknik.

Malware som infiltrerat kan sedan söka och förmedla affärshemligheter eller information om t ex lösenord och kontonummer. Sådan information blir till handelsvara och köps av andra missdådare.

Marknaden är extremt segmenterad. Man kan t ex läsa följande på den välkända fildelningssighten *pastelbin.com*: *Jag är från Kina och intresserad av att köpa US Visakort… V v kontakta mig på*

[1] Vilken medger stärkt anonymitet jämfört med andra nätverk.

lioxiaodet2009@hotmail.com med angivande av pris. På likartade sidor säljs också hela listor med bankkortsnummer, oftast amerikanska. På Cvv2 är annonserna specificerade med angivna priser och på perfekt engelska. Kortnumren säljs för mellan 2 och 6 euros, beroende på den utgivande bankens nationalitet. Med lösenord kan priset gå upp till 50 euros. Ofta nog anges aktuell behållning på kontot. Det kan vara frestande belopp, men att verkligen komma åt dessa kräver arbete.

Brottslingen måste finna inhemska bulvaner som kan lyfta likvida medel utan att väcka uppmärksamhet och som sedan delar med sig till initiativtagaren. Alla parter i sammanhanget blir allt mer professionella och välorganiserade men verksamheten är riskfylld och priserna därför inte så höga. Laurent Hersault på Symantec rapporterar att han på en sight sett en annons *om ett konto med 180 000 dollar till salu för 300 dollar*.

Handeln med kort på detta sätt blomstrar och virushandeln expanderar in på nya arenor för att finna nya objekt att plundra: in på sociala media och in i våra mobiler. Intrång bara för ärans skull är ute. Virusen snickras till för att skörda pengar. T ex har masken Koobface infekterat tusentals facebookprofiler genom att missbruka den vänskapsrelation som upplevs. När en vän skickar ett meddelande, så är sannolikheten att detta öppnas enorm och fällan slår igen. Skurkarna surfar i alla diskussionsgrupper. I ett meddelande erbjuds ett foto av den skjutne Ben Laden men vad som levereras till de naivt nyfikna som öppnar, är istället den nämnda masken; allt enligt säkerhetskonsulten McAfee.

15 % av länkarna i Facebook är ilvilliga.[2]

Virusen görs numera förföriskt med effektiv marknadskänsla. *Förr i världen skickade man virus runt hela jorden. Nuförtiden har man en varierad fabrikation som förmår ge skräddarsydd fulkod till varje enskild dator,* preciserar Laurent Hersault, direktör för säkerhetsteknologi hos Symantec. *Man riktar in sig mot preciserade populationer med syfte att stjäla all information som kan ha ett kommerciellt* värde. På Facebook samlar skurkarna in data som sedan ger underlag för mer påtagliga attacker. När det blivit klart att målpersonen gillar golf och gärna far på semester till Saint Tropez så är det nog så lätt att skicka ett fixat meddelande om dessa intressen. *Men fortfarande bombarderar man massan av användare med länkar som lockar den aningslöse till infekterade sidor.* Av en miljon analyserade länkar i Facebook är 15 % illvilliga, försäkrar Symantec.

Virusens arkitekter fokuserar också våra mobiler. *Det är en kolossal marknad* understryker L. H. och det räcker att infektera en app för att ta kontroll över hela apparaten. Sedan transformeras viruset till kassako. Den ringer upp ett förprogrammerat betalnummer som sedan direkt debiterar telefonens ägare.

Allt eftersom de kluriga verktygslådorna sprids massivt på nätet, d v s sprids till småtjuvar, forskar ett antal genier fram ännu oupptäckta luckor i våra programvaror, nya ingångar. Dessa s k Zero Day innovationer finns det inledningsvis inget skydd emot eftersom de inte kan identifieras innan de börjat verka. Microsoft har således erbjudit en belöning på 250 000 dollar till den som finner den lucka som Sasser, ett särskilt kraftfullt virus, trängde sig in genom för att förlama Delta Airlines, ett antal sjukhus och en satellit, berättar Guillaume Lovet. Dessa radikalt nya typer av intrång är ändå relativt sällsynta. Man räknade till 14 förra året (2010), men vardera av dessa såldes för omkring några hundra miljoner euros på Nätet.

[2] Skriver Tidningen, men en så hög siffra måste nog inkludera både spam och virus.