Partnerství spamu a počítačových virů

Podle statistik je v současné době odesláno každý den kolem 68 miliard e-mailů. Z tohoto množství přes 52 procent představuje spam, tedy nevyžádanou poštu zpravidla komerčního charakteru. Jinými slovy: více než polovina veškeré celosvětové e-mailové komunikace je nevyžádaná/nežádoucí, více než polovina přenosové kapacity sítí je využívána zbytečně atd.

V poslední době se přitom v souvislosti s nevyžádanou elektronickou poštou objevil jeden zajímavý fenomén: spojení s pisateli počítačových virů a dalších škodlivých kódů. Proč k tomuto „manželství" dochází? Odpověď je zcela prostá: protože je to výhodné pro obě strany. Nešťastné je to pouze pro uživatele, tedy pro příjemce spamu. A virů.

Spam i viry mají několik společných znaků. Obtěžují uživatele, šíří se pomocí stejného kanálu (e-mail), nejsou legální apod. (Odmysleme si nyní fakt, že viry jsou ve své podstatě spamem: nevyžádanou poštou.) To ale nejsou hlavní důvody, proč se jejich tvůrci spojují. Navzájem si totiž mají co nabídnout: pisatelé virů mohou spamerům jako na zlatém podnose přinést obsáhlé databáze napadených počítačů, z nichž je možné právě spam rozesílat. Na tyto napadené počítače totiž viry umisťují speciální programy používané k rozesílání nevyžádané pošty. Spameři si tak nemusejí pořizovat vlastní komunikační prostředky (počítače, přenosové linky apod.), a navíc případné sankce nejsou směrovány proti nim, ale proti nic netušícím majitelům zneužitých počítačů.

A z druhé strany: spameři mohou poskytnout pisatelům virů rozsáhlé databáze e-mailových adres, na které je možné škodlivý kód rozeslat, a nástup epidemie tak výrazně urychlit. Je totiž prokázáno, že právě počátek epidemie je pro konečnou (ne)úspěšnost viru nesmírně důležitý. Pokud totiž škodlivý kód nedokáže získat před antivirovými firmami v prvních minutách a hodinách dostatečný náskok (rozuměj rozšíření), tyto rychle převezmou iniciativu a nekompromisně jej zbrzdí.

Škodlivé kódy přitom mají i další schopnosti, jak spamerům vypomáhat. Díky značnému rozšíření se totiž mohou věnovat (a nezřídkakdy věnují) DDoS útokům na vybrané antispamové servery. Tyto útoky probíhají tak, že se obrovské množství napadených uživatelských stanic pokouší ve vymezeném časovém okamžiku či úseku připojit k příslušným serverům, které nejsou schopné tento obrovský nápor požadavků zvládat a hroutí se. Ať jsme konkrétní: to je případ třeba e-mailového červa MiMail.L.

Dalším naprosto jasným důkazem pro spojení mezi pisateli škodlivých kódů a spamery je e-mailový červ Randex. Ten do počítačů instaloval backdoor (zadní dvířka), který byl ovladatelný přes IRC kanály a v konečném důsledku mohl instalovat proxy server využitelný právě pro rozesílání spamu. Pisatelé viru dokonce prodávali IP adresy takto napadených počítačů: k jejich smůle byl mezi kupci i nastrčený redaktor jednoho německého počítačového časopisu, který realizovanou transakci neprodleně předal orgánům činným v trestním řízení.

Také rodinka e-mailových červů Sobig z roku 2003 vešla svým spojením se spamery do historie. Většina verzí tohoto červa se šířila pouze do určitého data, aby dále zbytečně nezahlcovala provoz na komunikačních linkách (jen verze Sobig.F se celosvětově šířilo 300 až 500 mil. exemplářů). Mezitím ale jednotlivé verze Sobigu jednak „nastřádaly" velké množství použitelných e-mailových kontaktů a jednak do mnoha set tisíc počítačů na celém světě nainstalovaly spamovací programy.

Jak vidno, partnerství (z rozumu) pisatelů virů a spamerů je oboustranně prospěšné a velmi rozšířené. Bohužel, ke škodě drtivé většiny uživatelů elektronické pošty.

TOMÁŠ PŘIBYL, AEC
www.aec.cz