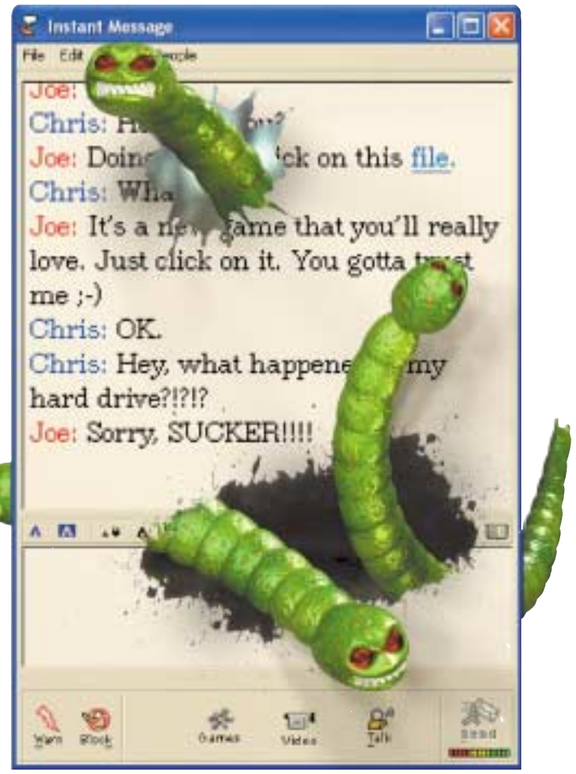
Automatičtí červi útočí

Poslechněte si rady zkušeného uživatele

VOJTĚCH BEDNÁŘ

Jedna ze základních pouček týkajících se bezpečnosti počítačů zní: nikdy neotevírej přílohu e-mailu, která vypadá jen trochu podezřele! Při jejím dodržení jsme si mohli být jisti bezpečím před červovou nákazou. Tedy alespoň donedávna.



Loňská invaze červa LoveSAN/Blaster a letošní Sassera ukázala, že v bezpečnosti operačních systémů na PC dochází k radikálnímu posunu. Červi byli až příliš dlouho úzce spojováni s e-mailem a dokonce s konkrétními klienty. Veškerá ochranná opatření jako antivirové systémy a firewally představovaly doplňující záchytnou síť. I v případě, že by touto sítí nově se objevivší škodlivý kód prostoupil, stále zde byla ještě jedna pojistka bránící jeho aktivaci – touto pojistkou byl poučený uživatel.

I přes velkou fantazii tvůrců červů a snahu udělat je „jako živé", tedy jako skutečné e-mailové zprávy, je možné poměrně snadno sestavit jakousi obecnou konstrukci toho, jak vypadá začervená zpráva. Na základě tohoto popisu ji je možné identifikovat vlastně nezávisle na rozhodnutí antivirového programu a podezřelý e-mail neotevírat a ihned zlikvidovat, čímž se aktivaci a rozšíření přiloženého červa zamezí. Kódy, které se díky vlastnostem, nebo spíše řečeno díky chybám konkrétních e-mailových klientů pokoušely aktivovat automaticky, nezávisle na vůli uživatele a jeho práci s přílohou, se příliš neujaly. Ukázalo se totiž, že nedostatky, které umožňují jejich existenci, je poměrně jednoduché záplatovat a že díky své vazbě na konkrétní aplikace a dokonce na jejich konkrétní verze nedoznávají přílišného rozšíření.

Jinými slovy, i přes značné množství různých červů mohl být elementárně chráněný a hlavně poučený uživatel relativně v klidu – červ se v jeho počítači bez jeho vědomí jen tak nespustil.

První změna

Červ Blaster, který během loňského léta zaútočil na obrovské množství počítačů s Windows 2000 a XP, nebyl úplně prvním automatickým škodlivým kódem na světě. Nicméně byl prvním, kterému se podařilo využít skutečně citlivé místo. Nešířil se e-mailem, ale pomocí známé a v době svého vzniku již nejen popsané, ale také záplatované bezpečnostní chyby v systému vzdáleného volání procedur RPC. Díky tomu byl vázán na operační systémy, které tento systém obsahují, avšak nikoliv na konkrétní aplikace nebo konkrétní uživatelem viděnou službu (e-mail). Jediný nakažený počítač dokázal sám autonomně vyhledávat a infikovat další oběti po celém internetu – uživatelská interakce nebyla vůbec zapotřebí. Kromě toho dokázal tento červ poměrně snadno projít i kontrolními a ochrannými aplikacemi – jeho chování totiž nemuselo být jednoznačně pochopeno jako škodlivé a mírněji nastavený firewall jej vcelku bez problémů propustil.

Reakce na příchod Blastera – prvního slavného a široce rozšířeného automatického červa – byla takřka okamžitá. Antivirové společnosti vydaly speciální jednoúčelové programy schopné ho najít a odstranit. Jejich kombinace s již zveřejněnou záplatou od Microsoftu pak Blastera i jeho další varianty nejen neutralizovala, ale také zajistila dotyčný operační systém před možností nové nákazy. Tím se dařilo výskyt viru postupně snižovat.

Problémem ale byla skutečnost, že Blaster obsahoval chybu. Tato chyba (nebo přesněji řečeno ne úplně ideální využití nedostatku RPC) způsobovala na některých systémech vypnutí této služby. Ve výchozím nastavení operačního systému (které je ale možné změnit) v takovém případě nastává restart počítače odložený o předdefinovanou dobu, kterou má uživatel na uložení své práce a ukončení všech programů. Tato doba je nastavena implicitně na jednu minutu a uživatel nemá viditelnou možnost restartování zastavit (taková možnost ovšem samozřejmě existuje). Vypínání služby a následné nekonečné restartování napadeného počítače při připojení k internetu pak nesmírně komplikovalo možnost jej záplatovat nebo alespoň vyčistit. Díky tomu se Blaster udržel na mnoha strojích po mnohem delší dobu, než by tomu bylo u konvenčního červa, který je po aktualizaci základních antivirových systémů v počítačích i na serverech obvykle z větší části během relativně krátké doby eliminován.

Druhá vlna

Červ Sasser, který letos zaútočil jako druhý masivně se šířící a zcela autonomní škodlivý kód, byl opět založen na nedostatku v operačních systémech typu Windows NT, tentokrát ve službě LSASS *(Local Security Authority Service)*. I v tomto případě se jednalo o zneužití známého bezpečnostního nedostatku, který byl již záplatován. Napadnutelné byly tedy jen ty operační systémy, které neobsahovaly patřičnou opravu, u nichž nebyly použity dodatečné bezpečnostní systémy nastavené na dostatečnou úroveň zajištění. Přesto se i Sasser masivně rozšířil. Jeho metoda napadání, přesněji řečeno vyhledávání obětí k napadání, byla poměrně zajímavá. Polovinu ze zkoumaných adres vybíral náhodně, zbytek podle stanovené masky. V důsledku se mezi nejvíce napadanými ocitly zejména systémy na univerzitách, v knihovnách

▲ **Stránky *www.virusbtn.com* cenného anglického časopisu o virech a antivirech.**

▲ **Encyklopedie virů *(www.symantec.com)*, popisy a postupy pro odstranění dotyčného viru.**

a podobně, což bylo přinejmenším zajímavé. V každém případě pokud byl Blaster prvním prototypem nového typu červa, Sasser se stal potvrzením tohoto nového rizika a také nepříjemné vyhlídky do budoucna.

Předpoklady pro existenci automatických červů

Aby mohli červi jako tyto dva zde popsané existovat, musí pro ně být připraveny základní předpoklady. Prvním a hlavním předpokladem je možnost dostat se do napadnutelného počítače. Komunikace, která začíná v nakaženém stroji a je směřována k potenciální oběti, musí vést k tomu, že tato oběť příjme a posléze také spustí stanovený programový nebo alespoň skriptový kód. Funkce, které to umožňují, jsou s tímto cílem buď přímo programovány, nebo jsou toho schopny v důsledku chyby, kterou obsahují. V prvním případě jsou ale vybaveny dostatečnými bezpečnostními mechanizmy, aby nemohlo dojít ke zneužití, zbývá tedy případ druhý.

Moderní operační systémy jsou vybaveny celou sadou protokolů a služeb, které pomáhají při provozu složitých síťových aplikací a prakticky umožňují jejich provoz. Obvykle jsou buď jednoúčelové a slouží jasně definovaným cílům, nebo jsou naopak konstruovány jako univerzální a umožňují ve svém rámci naprogramovat celou širokou škálu různých činností aplikací, s nimiž se setkáváme dnes a denně. I jednoúčelové služby však představují množství poměrně složitého kódu. Tento kód tvoří většinou celé týmy programátorů, tito programátoři na něm musí spolupracovat a mimo jiné právě proto existuje jen velmi málo lidí, kteří by se fyzicky vyznali v celých komponentách. To otevírá prostor pro bezpečnostní nedostatky.

Chybu, díky které se může do počítače dostat automatický červ, si nemůžeme představovat jako fyzický nedostatek programátora. Mnohem častěji se jedná spíše o schopnost použít nějakou věc, která za normálních okolností funguje bezproblémově, takovým způsobem, že toto její chování začne být nestandardní. Komponenta nebo služba se dostane do stavu, s nímž se při jejím programování nepočítalo, a proto je možné se do počítače dostat a spustit v něm kód červa nebo přinejmenším jeho zaváděcí část. Cenou za to je, že zneužitá služba nebo komponenta při této akci občas havaruje (to je příčinou onoho restartování v případě prozatím existujících automatických červů), ačkoliv ideálním stavem pochopitelně je dostat červa do počítače tak nepozorovaně, aby k žádnému restartování systému nebo omezování uživatele v době infekce a dalšího šíření červa nedocházelo.

Ne všechny služby jsou ve všech operačních systémech stejné a tedy neobsahují ani stejné bezpečnostní mezery. Ačkoliv automatického červa je možné vyvinout tak, aby využíval nedostatku konkrétní aplikace, jeho akční rádius by se tak omezil pouze na tuto konkrétní aplikaci nebo dokonce na její konkrétní verzi. Čím obecnější problém se tedy objeví, tím lépe pro takovéto červy. Desktopové počítače typu PC stále ovládají systémy společnosti Microsoft, přičemž neustále stoupá podíl systémů založených na technologii NT, tedy především Windows XP v různých verzích (Home, Professionall, ale také Tablet PC nebo Media Center). Společně s Windows 2000 mají tyto systémy velice podobné jádro a základní sadu služeb (v případě plné aktualizace jsou jejich základní součásti prakticky stejné). Vzhledem k tomu, že mnoho počítačů s těmito systémy je trvale připojeno k internetu, vzniká tak jedno veliké homogenní prostředí, velmi přátelské potenciálnímu výskytu automatických červů.

Mnoho počítačů je již vybaveno kvalitní externí ochranou. Jestliže samotné systémy NT příliš bezpečnosti z hlediska síťové komunikace nepřinášejí (a nezlepší se to pravděpodobně ani s očekávaným SP2 pro Windows XP), pak je nutné tyto systémy bezpečnostními prvky nějak dovybavit. Používají se různé typy antivirových systémů a firewallů, fungujících buď v rámci stejného systému, tedy přímo na počítači, který je potřeba chránit, nebo v rámci vyššího síťového prvku (proxyserveru, směrovače), přičemž není vzácností ani kombinace obou těchto způsobů s cílem dosáhnout vyšší úrovně celkového zabezpečení systémů.

Použití kvalitního a aktuálního antivirového programu a firewallu by teoreticky mělo zajistit bezpečné fungování počítače se všemi službami, které uživatel požaduje, zato však beze strachu z červů nebo dokonce z automatických červů. Existuje ovšem způsob, jak může škodlivý kód na několika úrovních obejít i velmi propracovaná bezpečnostní opatření. Toto kouzlo spočívá v tom, že stačí, aby se choval způsobem obvyklým pro běžně využívané aplikace.

V chování mnoha škodlivých kódů lze vystopovat základní patologické prvky, podle nichž je možné je eliminovat, v zásadě stačí zamezit několika věcem. Jedná se především o skenování portů, IP adres, nebo o monitorování toho, jak se chovají jiné instalované a spuštěné aplikace. Pokud ovšem autoři automatických červů přizpůsobí jejich metody síťové práce chování běžně využívaných aplikací, mají dobrou šanci, že se jim podaří svá pochybná dílka přes stávající ochranná opatření dostat, ledaže by tato opatření byla nastavena tak, že by jejich činnost začala výrazně vadit i samotným běžně používaným aplikacím.

Prostoru je víc než dost

I přes intenzivní vyhledávání a záplatování mezer si nemusíme dělat iluze o tom, že by se podařilo jednoho dne odstranit úplně všechny nedostatky. Je to proto, že jednak je velice obtížné určit, kolik jich vlastně jen v rámci systémů NT existuje, jednak není zcela stoprocentně možné vyloučit, zda záplatováním stávajících bezpečnostních mezer nevznikají náhodou mezery zcela nové, možná také ve zcela jiných částech systémů, než kde se nacházely ty, které se původně záplatovaly. V době, kdy se podařilo zažehnat nákazu červem Sasser, vyšlo najevo, že různé části NT systémů obsahují ještě skoro dvacet potenciálně nebezpečných míst, která mohou umožnit nákazu a redistribuci automatického červa. Lze se domnívat, že takových chyb nebo citlivých míst je v operačních systémech NT ještě mnohem, mnohem více.

▲ **FTP server našich sousedů *(www.sac.sk)*, na kterém najdete užitečné antivirové programy.**

▲ **Výborný přehled o problematice virů a červů získáte na Igiho stránce *www.viry.cz*.**

Druhým podstatným aspektem je pak skutečnost, že současní automatičtí červi ani zdaleka nevyužívali příležitostí, které jim jejich princip nabízí. Vedly k padání operačních systémů, měly tendenci vytvářet na napadených strojích servery, jichž si lze snadno všimnout, prováděly testování portů, spouštěly se způsobem, který lze poměrně snadno identifikovat. A především objevily se vždy až v okamžiku, kdy chyba, kterou využívaly, byla známá a existovala pro ni záplata. Z toho totiž vyplývá, že jejich autoři při tvorbě škodlivého kódu vycházeli právě z rozboru chování záplaty, jejího obsahu a činností, které provádí při své instalaci. Tak se jim vlastně podařilo dopracovat se k bezpečnostní mezeře, o které by jinak pravděpodobně neměli ani ponětí a kterou dávno před nimi objevil někdo úplně jiný.

Již z tohoto výčtu může být zřejmé, kde všude existuje prostor pro nové automatické červy. Podívejme se alespoň na základní body (týká se opět pouze NT systémů):

- Autor najde bezpečnostní mezeru dříve než Microsoft.
- Objeví způsob, jak činnost červa „přilepit" na běžnou komunikaci nějaké aplikace (Outlook, Internet Explorer) tak, že bude bez problémů procházet standardními antiviry a firewally.

Co je to automatický červ?

- Nevyužívá pro své šíření primárně elektronické pošty.
- Je založen na chybě nebo na vlastnosti standardní systémové komponenty.
- Umí infikovat počítač bez zásahu nebo svolení uživatele.
- Umí se maskovat a obcházet standardní bezpečnostní opatření.

Současné infekce automatickými červy

MSBlast/LoveSAN

- využíval chyby RPC ve Windows 2000/XP,
- sloužil jako agent k útoku na servery Microsoftu,
- způsoboval pády OS.

SASSER

- založen na nedostatku služby LSASS,
- šíří se podle sofistikovaného systému pravidel,
- také po něm padá operační systém, napadá W2K/XP,
- (jeho autor byl dopaden).

- Vymyslí nějakou formu koordinace činnosti mezi červy na různých nakažených strojích.

Kromě těchto základních rizik si nelze nevšimnout ještě jedné podstatné skutečnosti. „Škodlivý" efekt současných automatických červů vůči napadeným uživatelům se prakticky omezuje na vedlejší nedostatky, způsobené jejich nedobrým naprogramováním, špatným využitím bezpečnostních mezer, nebo je vyvolán omylem. Přitom by tito červi mohli skutečně škodit, mohli by mazat důležité soubory nebo nastavení, mohli by vykrádat data, mohli by působit chaos (takto jsou využívány spíše pro útok na někoho jiného). Ačkoliv zatím existující kódy vytvářejí v napadených počítačích „zadní vrátka", pravděpodobnost skutečného využití těchto zadních vrátek je pouze minimální. Především díky obrovskému počtu nakažených počítačů, jejich obtížné identifikaci, nepravidelné přístupnosti, nebo proto, že se nacházejí za firewallem, který sice propustí červa a jeho komunikaci, ale další eventuální kroky hackera využívajícího nákazy by již zaznamenal. Jinak řečeno, automatičtí červi se prozatím sice šíří, ale záměrně přímo neškodí. To by se ovšem v budoucnu mohlo změnit. Bohužel velmi zrůdným způsobem.

Proč přepadat planetu

Zeptejme se, proč vlastně červi a tedy i automatičtí červi vznikají? V některých případech se jedná jen o jakousi demonstraci možností nalezených bezpečnostních mezer. Jindy na sebe upozornují hlavně -náctiletí programátoři. Jen málo červů v současné době vzniká skutečně s cílem ubližovat uživatelům a tito červi se obvykle příliš nerozšíří z jiných důvodů (včasné zadržení antivirovými systémy, chyby v jejich programovém kódu, velice úzké cílení na jednu konkrétní část internetu nebo dokonce na jedinou subsíť a podobně). Autoři schopni naprogramovat kvalitního červa obvykle nemají za cíl zlikvidovat data napadených počítačů. Mohli by je ale vykrást a zneužít. Nebo by mohli využít velmi šikovně přímo napadených počítačů. Tedy například nechat na nich běžet náročné aplikace distribuovaného počítání, využít je jako oběti pro rozesílání nevyžádané pošty, pro provedení masivního útoku typu DDoS (jak se ostatně již velmi úspěšně stalo). Všechny tyto možnosti by v kombinaci se strategií automatických červů mohly přinést buď požitek svým autorům a těm, kteří je rozšířili, nebo pro změnu katastrofu jejich nepřátelům, jak se o tom již mohly přesvědčit například webové servery společnosti Microsoft. Pokud bereme současné nákazy pouze jako demonstraci technologie, pak nás ten pravý útok pravděpodobně teprve čeká. Je pouze otázkou, v jak vzdálené budoucnosti se jej dočkáme a jak tragické důsledky bude nakonec mít.

Automatičtí červi útočí

Představme si, že někdo napíše automatického červa, který bude ke svému šíření využívat doposud neznámou chybu v běžně se vyskytující službě, využívané prohlížečem Internet Explorer. Červ se začne šířit pod hlavičkou komunikace IE a tak si jej firewally nevšimnou. V cílových počítačích se nebude ukládat ve formě nových souborů, ale jako náhrada stávajících jednoduchých aplikací (třeba kalkulačky nebo poznámkového bloku). Není problém naprogramovat například kalkulačku (nehledě na to, že její zdrojový kód je běžně k dispozici), která bude kromě svého vlastního kódu obsahovat červa, jinak však bude funkčně i vizuálně shodná s původní. Spustitelný soubor je možné komprimovat a šifrovat, přičemž se dekóduje až v okamžiku své aktivace a tak komplikuje možnost svého odhalení, šifra se totiž může během distribučního cyklu červa měnit.

▲ **Seznam nejrozšířenějších virů na adrese *(www.wildlist.org)* vychází každý měsíc.**

▲ **Pravidelné srovnávací testy antivirových programů najdete na *www.av-test.org*.**

Červ se usadí v počítači a monitorováním komunikace jiných aplikací nebo dokonce činnosti lokálního firewallu zjistí, jak často a s kým se PC spojuje. Pak se pokusí napadnout okolní počítače v rámci místní či širší sítě, dříve než začne expandovat „ven". Červi v různých počítačích spolu budou komunikovat a utvoří jakousi vlastní „P2P" síť, v jejímž rámci se mohou vzájemně kontrolovat a poznají, pokud se někde začalo s čištěním a tedy hrozí prozrazení a likvidace jedné kopie, potažmo dalších. Přitom budou komunikovat v šifrované podobě způsobem, který bude zaměnitelný například s běžným prohlížením kódované webové stránky.

Jakmile si bude červ jistý svou pozicí v dané síti, začne pracovat. Vytvoří v počítači prostor pro spuštění libovolného kódu, rovněž šifrovaný a vymezený maximální zátěží tak, aby si uživatel nevšimnul případného zpomalení. V tomto stavu bude čekat na instrukce svého majitele.

Ten po nějakém čase své síti červů například poručí vykonat složitý výpočet. Zapůjčení superpočítače k jeho provedení by stálo mnoho peněz. A tak se výpočet rozdělí na množství malých úkolů a ty se rozešlou do sítě začervených počítačů. Červi se v nich nacházejí na různé úrovni řízení a sami tak celou síť ovládají bez nutnosti zásahu původního majitele. Část výpočtu, za který někdo dostane nemalé peníze, pak provede například právě ve vašem počítači program, který jinak považujete za kalkulačku a také jako kalkulačka běžně slouží.

Jinou možností je, že se na autora takovéto sítě červů přijde. Ten pak pošle nejbližšímu uzlu příkaz začít síť likvidovat. V lepším případě se červi rozpojí a z napadených strojů vymažou. V horším případě ještě předtím vezmou útokem například web místní vlády nebo policie. V nejhorším případě pak po vykonání takového útoku vymažou sebe i s kompletním obsahem všech napadených strojů – kalkulačka vám tak zničí vše, co máte na disku. To všechno s notnou dávkou štěstí, aniž byste si toho všimli vy sami, aniž by si něčeho všimly antivirové společnosti a aniž by bylo možné zjistit, kdo přesně je autorem a odkud se červ původně vzal a jak se vlastně do napadených strojů dostal. Vše klidně proběhne během několika dnů.

Bezpečnost (ne)pomůže

Používání aktuálního antivirového programu a dobře nastaveného firewallu zvýší úroveň bezpečnosti opravdu podstatným způsobem. Stejně tak důležité je i pravidelné aktualizování operačního systému, pokud možno aktualizování automatické. Přesto existuje možnost, že se vyskytnou nové hrozby. Noví červi které, jak jsme pospali výše, obejdou i ta nejlepší bezpečnostní opatření. Dvě zatím zaznamenané invazní vlny doprovázené vždy několika menšími „vlnkami" mohou být a s vysokou pravděpodobností v budoucnu budou následovány dalšími, mnohem nebezpečnějšími. Nebo je možné, že podvrženou kalkulačku již ve svém počítači většina z nás má. Že naše PC dělá kromě toho, co od něj očekáváme, také něco úplně jiného a až se to jeho majiteli znelíbí, prostě nám je na dálku zničí, aniž bychom s tím my sami nebo náš antivirus/firewall mohli cokoliv udělat, protože o hrozbě prostě nevíme, neznáme ji a neumíme ji identifikovat, natož pak odstranit. Tato představa není ani zdaleka utopická, dokonce přes všechny snahy o posílení bezpečnosti je velmi dobře možná. V posledních několika měsících byly navíc v rámci hledání problémů objeveny bezpečnostní mezery přímo v ochranném softwaru, v antivirových, testovacích a zajišťovacích aplikacích. To je skutečně alarmující skutečnost, která sice přímo vrata invazi automatických červů neotevírá, ale vydatně napomáhá k vytvoření takřka ideálního prostředí, v němž k ní může velice snadno v blízké budoucnosti dojít. Má se tedy smysl bát?

Bát se přímo asi nemusíme, ale mít se na pozoru rozhodně ano. Všechna opatření, která můžeme pro svou bezpečnost udělat, je třeba přijmout bez odkladu. Kromě toho bychom ale měli doufat v trochu štěstí a v profesionalitu společností, které se dnem i nocí starají o naši – uživatelskou – ochranu, tedy tvůrců antivirových aplikací, firewallů a operačních systémů.

Možné budoucí infekce

- Nová generace automatických červů může způsobit obrovské škody, zejména pokud jejich autoři objeví bezpečnostní chyby dříve než ti, kteří je lepí. V takovém případě se červ může dlouho a dobře maskovat, paradoxně pomocí primitivních a známých metod (vydávat se za kalkulačku).
- Červi budou napadat počítače prakticky bez šance uživatele s tím něco udělat, mohou umět obcházet antiviry a firewally, maskovat se, „přilepit" na standardní aplikace OS. Po infekci se mohou navzájem řídit a organizovat. Mohou sloužit svým pánům a mohou také škodit, a to zcela tiše a bez šance být odhaleni.
- Aktuální operační systém je základ, antivirový program nutnost a firewall nezbytnost. Vícestupňová ochrana je plusem, ale stoprocentní jistoty bezpečí nedosáhneme.

4 0350/FEL ❑