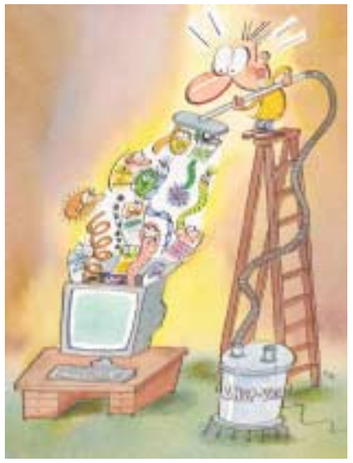
Co připomněl Blaster?

Virus-nevirus Blaster a jeho poselství, aneb bez personálního firewallu ani ránu

PATRIK MALINA

Vedrem vyprahlou a tradičně letně ospalou tuzemskou mediální scénu během srpna nevídaně oživila aférka s výskytem velmi zajímavého červu (nesprávně viru) s názvem Blaster.



Ačkoliv z pohledu zkušeného bojovníka na antivirové scéně se jednalo vlastně o poměrně nevinnou hříčku bez vážných následků, stal se tento programek dokonce středem pozornosti redaktorů veřejnoprávní televize(!), což se věru nestává každý den. Velmi příznačným na celé kauze je fakt, že Blaster se stal mediální hvězdou ze zcela jiného důvodu, než by bylo potřeba: jeho útok totiž poukázal na nesmírně závažné okolnosti, o nichž se ovšem v televizi nedozvíte a v novinách nedočtete. V tomto článku se nejen dozvíte, jak vlastně Blaster poukázal na to, že „císař je nahý“, ale především se pokusíme podpořit tvrzení, že personální (osobní) firewall není zbytečnost.

Cesta k Blasteru

Začněme letním příběhem, jenž představuje klíčové východisko pro další rady a návody v tomto článku. V průběhu první poloviny léta se výzkumné skupině LSD (The Last Stage of Delirium Research Group) podařil senzační objev v podobě odhalení velmi závažné bezpečnostní díry v útrobách operačních systémů Windows řady NT (tedy především 2000, XP, ale též zcela nových Windows 2003 Serverů). Protože to jsou chlapíci zodpovědní a uvědomili si, jakou potenciální rozbušku drží v rukou, rozhodli se neriskovat a vše neprodleně oznámili výrobci, tedy Microsoftu. V Redmondu jasně chápali, o co jde, a proto se vzápětí (cca po 2 dnech) na oficiálních stránkách *www.microsoft.com/security* objevilo vydání bezpečnostního bulletinu MS03-026 s potřebnou záplatou pro všechny postižené varianty Windows. To vše se stalo již 16. července 2003!

Protože skupina LSD byla hodně zodpovědná, neumístila na své stránky ani příliš podrobný popis svého objevu, aby jej někdo nemohl využít. Avšak i několik málo informací stačilo řadě zkušených programátorů k tomu, aby se vydali po dobré stopě a díru nalezli. S jistým odstupem se např. čínské skupině *www.xfocus.org* podařilo mezeru objevit a především vytvořit funkční zdrojový kód programu, jenž dokáže slabosti využít. Od této chvíle již začalo přituhovat, neboť pobodný kousek se podařil i jiným tvůrcům a vznikaly základy aplikací, jež spojovalo jediné: utajená cesta do útrob Windows vedla přes objevenou díru. Bohužel, následky se mohly velmi lišit.

V tuto chvíli již nic nestálo v cestě tvůrci Blasteru. Nemusel být extrémně dobrým programátorem, neboť podstatný kus cesty za něj urazili jiní. Stačilo vzít známé ingredience a lektvar dovařit. Zhruba měsíc po uvolnění bezpečnostní záplaty(!) se tedy objevuje Blaster, konkrétní vtělení objevené chyby a začíná kosit uživatele, kteří si mysleli, že se jich problém netýká.

Kudy chodí Blaster?

Co je tedy onou chybou, jež tak snadno propouští Blaster a umožňuje mnohem víc, jak si dále řekneme? Poněvadž je problém komplikovaný, nebudeme zabíhat do přílišných podrobností – opravdoví znalci nechť využijí webové odkazy pro detailní reference. Strašidelný potenciál díry spočívá v tom, že spojuje dvě velmi používané technologie ve Windows. Jednou je tzv. DCOM – zjednodušeně řečeno se jedná o architekturu programů a jejich komponent, jež dovoluje jejich rozprostření na více počítačů v síti a vzájemnou komunikaci. Druhou technologií je pak síťový protokol RPC, jenž právě dokáže na dálku ony komponenty zavolat a spustit podle potřeby.

Výzkumníci odhalili závažný fakt, že po zaslání specificky poškozených požadavků RPC dojde k tzv. chybě přetečení, jež prostě řečeno donutí DCOM dělat věci, které by neměl. Posléze již stačí zasílat další konkrétní požadavky na útokem obnažené rozhraní, a vzdálený systém je ve vašich rukou.

Aby následující scénář mohl být naplněn, musí cílový počítač, jenž má být obětí, splňovat ještě jednu podmínku. Tou je naslouchání na tzv. portu 135, k čemuž se ještě vrátíme – pro tuto chvíli stačí říci, že tato „dvířka“ bývají tradičně otevřená, neboť je systém hojně využívá pro běžnou službu sdílení souborů a tiskáren v lokálních sítích. A právě touto skulinou, pokud jste ji „vystavili“ navíc ještě do internetu, si k vám Blaster mohl najít cestu. Červ fungoval dosti jednoduše, neboť ze strojů obětí náhodně okukoval v okolních sítích další počítače a otevřené cesty, a tím si hledal nové cíle. Po průniku na další stroj využil protokol TFTP (trošku jednodušší FTP) a s jeho pomocí sám sebe přesunul na vyhlédnutou oběť a infikoval ji. Zde začínalo kolečko od začátku, hledáním nových potenciálních cílů.

Všimněte si jedné zásadní věci: netřeba použít e-mail, netřeba spouštět podezřelou přílohu v poště, netřeba navštívit podezřelou webovou stránku... Stačilo být připojen a nemít záplatu! A následky? Tvůrce byl nesmírně shovívavý, neboť vám „jen“ pravidelně nechal restartovat počítač. Jeho citlivost vyzdvihujeme proto, že díky oné chybě mohl naprosto cokoliv, jak uvidíte dále.

Port 135 a spol.

Jak jste jistě postřehli, klíčovým faktem je dostupnost portu 135 a jeho zneužití. O co vlastně jde a proč „to tam ve Windows máte“? Protože se jedná o mnohem obecnější problém a trvale velké nebezpečí, podíváme se na věc podrobněji.

Každý operační systém, jenž komunikuje po síti a využívá protokolovou sadu TCP/IP (stojí na ní celý internet a velká část lokálních sítí), pracuje s tzv. porty. Můžete si je představit jako přívodní roury do vašeho stroje – je jich 2 × 65 535 (polovina TCP, polovina UDP) a musí se do nich vejít veškerá komunikace, neboť každá roura buďto přijímá, odesílá nebo naslouchá. Mnoho síťových služeb používá určité očíslované porty (roury), jež jsou dobře známy, aby na nich přicházející klienti snadno nalezli, to co chtějí. Tak služba WWW typicky naslouchá na portu TCP 80, poštovní server na portech 25 TCP či 110 TCP a třeba překlad jmen DNS používají 53 TCP i UDP.

Nedílnou součástí operačních systémů Windows jsou také další služby, jež zajišťují často nezbytné operace. Jednou z nich je i ona zneužitá služba číhající na portu 135 TCP a UDP. Jednoduše řečeno slouží k tomu, aby si vzdálené počítače domluvily další porty, na nichž se budou bavit, právě když použijí třeba protokol vzdáleného spouštění aplikací RPC. Podstatné je, aby port 135 byl např. v lokální síti průběžně dostupný, neboť bez něj vám spousta věcí nebude fungovat, jak by měla. Na druhou stranu, z internetu k vám by měl být striktně nedostupný, neboť představuje nebezpečí a k ničemu kloudnému jej zde nepotřebujete.

Port 135 však není jediným potenciálním problémem. V jeho sousedství číhají další nástrahy v podobě portů 137, 138 a 139. Jsou totiž využívány protokolem NetBIOS, jenž například zajišťuje běžné sdílení souborů a tiskáren v sítích s Windows, což je služba, bez níž si tradiční uživatel nedokáže svou práci představit. Jenže, neopatrně vystavený port 139 do internetu opět představuje smrtící nebezpečí. Řeknete si, proč tolik řečí kolem portů? Protože představují při chybné konfiguraci stálé nebezpečí pro váš systém, a míra ohrožení je ve srovnání s mnoha viry a červy včetně Blasteru nesrovnatelně vyšší.

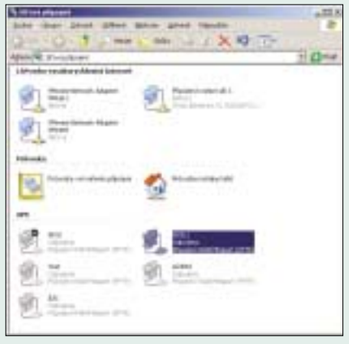
Proč antivir nestíhá?

Mnozí z vás se jistě pozastaví nad tím, proč zkoumat síťovou komunikaci, když mají antivir, jenž přeci vše řeší! Nemůže být ovšem většího omylu, jak vás nyní přesvědčíme. Antivirový software je jistě velmi důležitou pomůckou, ale proti útokům vůči konkrétním síťovým službám je bezmocný. Důvodem je samotná podstata jeho práce – antivir kontroluje podezřelá data, jež **dorazila** na váš počítač v jakékoliv podobě. Pokud

Jak nakonfigurovat osobní firewall

Na tomto místě naleznete podrobný návod pro konfiguraci osobního (personálního) firewallu. Pro ukázku jsme vybrali dvě běžně rozšířená řešení: jedním z nich je „Brána firewall pro připojení k internetu“, které je nedílnou součástí operačních systémů Windows XP a Windows Server 2003, druhým pak aplikace ZoneAlarm, jež patří mezi nejběžnější řešení, volně dostupná ke stažení z internetu. Předvedené postupy lze (obzvláště dle ZoneAlarmu) velmi podobným způsobem využít i u dalších produktů – poměrně podobně se chovají např. Kerio Personal Firewall či Sygate Personal Firewall.

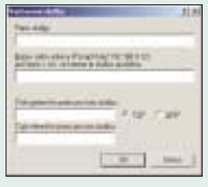
Brána firewall pro připojení k internetu



1) **Produkt není potřeba instalovat, neboť je součástí operačních systémů Windows XP/Server 2003. Úvodním krokem pro jeho využití je vstup do rozhraní Síťová připojení, kde zvolíme připojení, které budeme chránit. Typicky je to telefonické připojení sítě, jež používáme ke komunikaci k poskytovateli internetových služeb.**

2) **U vybraného připojení přejdeme pomocí pravého tlačítka myší na Vlastnosti a zobrazíme kartu Upřesnit. V horní části této karty zapneme osobní firewall zaškrtnutím příslušného pole. Tímto krokem jsme nastavili počítač tak, aby povolil odchozí komunikaci a zabránil jakémukoliv přístupu zvenčí. Chceme-li výslovně povolit vstup určitého typu komunikace směrem z internetu na náš počítač, stiskneme tlačítko Nastavení v dolní části.**

3) **Na této kartě Služby můžeme povolit základní komunikační protokoly, jež jsou potřebné pro elektronickou poštu, prohlížení webových stránek či využití služby Vzdálená plocha. Parametry na této kartě platí pro příchozí komunikaci a nijak neovlivňují vaši bezpečnost v opačném směru.**



4) **V tomto rozhraní lze přesně nadefinovat filtr pro konkrétní typ protokolu a číslo portu, na němž komunikace bude probíhat.**

5) **Na kartě Protokolování zabezpečení lze konfigurovat způsob pořizování záznamu o činnosti firewallu. Tato informace může být důležitá pro případné řešení následků některých útoků.**

6) **Karta ICMP je určena k detailnímu nastavení specifické komunikace podle stejnojmenného protokolu ICMP. Tato komunikace slouží k diagnostice, např. při použití příkazů Ping či Tracert. Pokud tyto možnosti neznáte nebo jim nerozumíte, pro jistotu služby nepovolujte a prostudujte si nápovědu.**

Personální firewall ZoneAlarm 4.0 Freeware

1) Práci s programem Zone Alarm zahájíte jeho instalací.

2) Ihned po prvním spuštění programu aplikace nabídne průvodce pro tvorbu základního nastavení. Máte možnost zkontrolovat výchozí vlastnosti a případně některé parametry upravit.

3) V dalším kroku uživatel definuje způsob, jakým bude ZoneAlarm informovat o své činnosti. Nechcete-li být obtěžováni, lze potlačit zobrazování varovných zpráv.

4) Následující obrazovka nabízí otevření internetové komunikace pro základní aplikace – v tomto případě především webový prohlížeč. Pokud se základním výběrem nejste spokojeni, můžete další aplikace přidávat pomocí pokročilého dialogu (Advanced).

5) Pro základní funkci programu jsou všechny podstatné informace zadány, a proto může následovat jeho spuštění.

6) Další možnosti konfigurace jsou dostupné ze základní obrazovky ZoneAlarmu. Na kartě Firewall naleznete základní úrovně zabezpečení ve formě posuvníků, pro dodatečnou konfiguraci zvolte tlačítko Advanced. Ve výchozím stavu je veškerá příchozí komunikace na internetovém rozhraní blokována.

7) Pokud se jakýkoliv neprověřený program pokusí navázat komunikaci, firewall zobrazí varování a dotáže se, zda chcete komunikaci přijmout či odmítnout, a to pouze v tomto případě, nebo ve všech podobných situacích.

s vámi někdo komunikuje na dálku a vede útok tímto způsobem, antivir nemá co kontrolovat, a proto nemůže nic odhalit. Ano, Blaster byl úspěšně odhalen antiviry, ale pozor: až ve chvíli, kdy už jste byli bezmocnou obětí! Podstatná část útoku proběhla **předtím**, než se u vás na počítači Blaster objevil a antivirus jej odhalil. Kdyby autor červu byl zlomyslnější, zlikvidoval by váš stroj dřív, než by antivirový software vůbec dostal šanci vstoupit do hry.

Přesvědčivým důkazem budiž navíc fakt, že ani soubor na vašem stroji nemusí být antivirem odhalen. Autor článku si na základě na internetu dostupných zdrojových kódů sestavil program, jenž dokáže vzdáleně připojit příkazovou řádku jakéhokoliv počítače, který naslouchá na portu 135. Ačkoliv jde jen o velmi mírnou modifikaci (ovšem poněkud drsnější) červu Blaster, zachytily jej jen některé antiviry. V den psaní článku (23. srpna), tedy více než 5 týdnů po objevení díry a 3 dny po poslední aktualizaci Live Update, je můj Norton AntiVirus (verze 9.05.15) naprosto v klidu, a ani na přímý dotaz na inkriminovaný soubor nenachází nic podezřelého. Co z toho plyne? Že třeba váš kolega v práci, jehož rovněž chrání tento či jiný antivir, může zneužitím stejného prográmku třeba zlikvidovat vzdáleně váš pevný disk.

Osobní firewall – nezbytnost

Z výše uvedených informací jasně vyplývá, že důsledná kontrola toho, co dorazí na váš stroj, nemusí před záškodníky stačit. V současné době se stává samozřejmostí provádění síťové kontroly, a to nejen ve firmách či rozsáhlých sítích, ale především na domácích počítačích připojených do internetu. Pochopitelně si to uvědomují i antivirové firmy, a proto nabízejí krom tradičních antivirů i tzv. osobní či personální firewally – najdete je v nabídce zmíněného Symantecu, ale i mnoha jiných výrobců (přehled najdete dále v tomto článku). Důležité je si uvědomit zásadní výhodu a potřebnost tohoto řešení: dnes již nemusí představovat největší nebezpečí soubor či program, který pronikl až na váš počítač, ale velmi zákeřná může být již samotná komunikace s vaším strojem po síti, aniž by byl přenesen jediný ucelený soubor na váš počítač. Kdykoliv stroj spustíte a připojíte k síti, měli byste ve výchozím stavu blokovat všechnu komunikaci s výjimkou té, která je pro vaši práci či zábavu nezbytná. Vámi otevřené kanály by měly být stále pod kontrolou.

Jak personální firewall pracuje?

Aplikace typu personální (osobní) firewall používá ke své práci několik principů, jež si zde popíšeme. Základem jeho činnosti je tzv. paketový filtr, jenž pracuje v podstatě v úloze důsledného vrátného. Jeho rukama na síťovém rozhraní projde každý balíček dat – paket – a je porovnán se sadou pravidel, načež následuje buďto propuštění, nebo zahození. Mezi tato pravidla patří především směr provozu (odesíláte vy nebo někdo posílá něco vám), dále číslo portu (tedy na jakou službu komunikace míří) a jedinečná identifikace odesílatele a příjemce pomocí tzv. IP (síťové) adresy. Je důležité si uvědomit, že číslo portu je vždy odchozí (tedy odkud jste komunikaci vypustili) a cílové (kam na protějším počítači míříte). Již kombinace těchto parametrů je použitelná pro velmi slušné zabezpečení.

Protože jsou však úskoky útočníků rafinované, umí toho firewally více. Další běžnější možností je kontrola aplikací na vašem počítači, jež chtějí síťové služby použít. Vše objasní příklad: po instalaci firewallu se pokusíte poprvé stáhnout poštu. Tato akce probudí firewall a ten se vás zeptá, zdali tomuto poštovnímu programu na vašem stroji povolíte odpovídající komunikaci. Po souhlasné odpovědi si firewall poštovní aplikaci označí a hlídá, aby se poštu nepokusil poslat jiný program. Navíc vás bude varovat, pokud by došlo ke změně původního poštovního programu (např. pomocí zákeřného červu) a tím vzniklo riziko neautorizované komunikace.

Mezi vlastnosti pokročilejších firewallů patří tzv. inspekce obsahu. Tento postup je používán k prověřování toho, co běžný paketový filtr nezvládne – kontroluje samotná data, tedy „náklad“, jenž od vás či k vám putuje. Existují totiž způsoby, jak např. pomocí předstírání webové či poštovní komunikace „protlačit“ otevřeným kanálem (na neblokovaném portu) něco nekalého. Inspektor obsahu se „koukne dovnitř“ a zběžně ověří, zda náklad není škodlivý, a poté vše opět buďto posvětí, nebo zlikviduje.

Osobní firewall v praxi

Pokud si pořídíte aplikaci tohoto jména, dokáže většinou spojit výše popsané funkce dohromady a vytvořit tak silnou bariéru mezi vaším počítačem a okolím. Následující odstavec formuluje obecné postupy při práci s typem programu, jenž se vyskytuje v mnoha podobách dle výrobce. Konkrétní typy najdete v tabulce.

Základním krokem je úspěšná instalace. Pokud nedopadne dobře, raději program odstraňte a zkuste nainstalovat znovu. V opačném případě riskujete, že nebude pracovat správně, takže buďto může „propouštět“, nebo naopak blokovat kdeco a shazovat počítač. Po prvním spuštění počítače s osobním firewallem bývá většinou definován výchozí konfigurační stav, který říká asi toto: dovnitř nepouštěj nic, ven pouze to, co uživatel osobně povolí. Pokud je základní ovládání prováděno pomocí „posuvníků“ či voleb s označení typu „nízká, střední, vysoká“ bezpečnost, nespoléhejte se na tuto informaci a vždy pátrejte, co se za výchozím nastavením skrývá.

Po prozkoumání programu se snažte docílit nastavení, jež jsme zmínili: cestu dovnitř uzavřete, a směrem ven povolte komunikaci např. webovému prohlížeči, poštovnímu programu, FTP klientu či antiviru (pro updatování). Pro další nastavení vřele doporučujeme seznámit se s postupem detailní konfigurace filtrů, jež osobní firewally obsahují. Než povolíte komunikaci dovnitř, měli byste si být jisti, že víte, co pouštíte, jinak vše zamítněte. Dále naleznete tabulku běžných typů služeb a naše doporučení, jak si osobní firewall nastavit. Konkrétní postup nastavení záleží na typu programu, jejž jste zvolili.

Při detailním sestavování vlastního filtru je potřeba si uvědomit některé okolnosti. U čísel portů je důležitý především cílový port, jenž směřuje na určitou službu – odchozí port bývá volen náhodně a za běžných okolností bývá vyšší než 10 000. Pokud tedy chcete pustit někoho na svůj počítač např. na program ICQ, jenž čeká na portu 1080, musíte povolit příchozí komunikaci na tomto portu a jako hodnotu pro odchozí port ze vzdáleného počítače ponechat „Any“ (cokoliv, nespecifikováno). Podobně od vás ven komunikuje např. webový prohlížeč tak, že odchozí port je náhodný a cílový port na vzdáleném počítači je tradičně 80. V naší tabulce doporučení najdete vždy **cílové** porty!

Zcela samostatnou kapitolou jsou protokoly pro komunikaci v sítích Microsoftu. Potřebné porty by měly být otevírány jen v lokálních sítích (tedy ne do veřejného internetu!), a navíc ještě pouze pro komunikaci s důvěryhodnými počítači. Protože potřebných portů je mnoho, nabízí většinou osobní firewall volbu typu „lokální sítě Microsoft“, kterou spouštějte opravdu jen pro nanejvýš důvěryhodné komunikační protějšky. Nezapomeňte, tudy útočil z internetu Blaster, a jistě jej budou mnohé červy následovat!

Verdikt

Netřeba dále zdůrazňovat, proč je osobní firewall nezbytnou součástí každého počítače, který je připojen do jakékoliv sítě. Na závěr si dovolíme ještě jedno doplnění: neméně důležitou péčí o váš počítač je pravidelné aplikování bezpečnostních záplat z dílny výrobce operačního systému. Pamatujete? Chyba MS03-026 byla opravena v půli července, a až za měsíc červ Blaster udeřil! Máte už potřebnou záplatu? 3 0525/FEL ❑

Zajímavé adresy

Chyba a záplata MS03-026
http://www.microsoft.com/security/security_bulletins/ms03-026.asp
Stránky skupiny LSD
http://lsd-pl.net/
Stránky čínské skupiny Xfocus
http://www.xfocus.org/
Zavedená čísla portů určitých služeb
ftp://ftp.iana.org/assignments/port-numbers
Stránka o personálních firewallech
http://www.free-firewall.org/

Přehled některých běžných řešení personálních firewallů

Jméno	Cena	Adresa
Kerio Personal Firewall	zdarma	*www.kerio.cz/kpf_home.html*
ZoneAlarm	zdarma	*www.zonelabs.com*
Sygate Personal Firewall	zdarma	*smb.sygate.com/products/spf/spf_ov.htm*
Outpost Personal Firewall	zdarma	*www.agnitum.com/products/outpost/*
Outpost Personal Firewall Pro	39,95 USD	*www.agnitum.com/products/outpost/*
Zone Alarm Pro	49,95 USD	*www.zonelabs.com*
Kerio Personal Firewall Full	1 420 Kč	*www.kerio.cz/kpf_home.html*
Sygate Personal Firewall Pro	39,95 USD	*smb.sygate.com/products/spf/spf_ov.htm*
McAfee Personal Firewall Plus	39,99 USD	*us.mcafee.com/default.asp*
Norton Personal Firewall	59,95 USD	*www.symantec.cz/region/cz/product/npf_index.html*
Kaspersky Anti-Hacker	1 390 Kč	*software.pcs.cz/pcssw.php?id=248*

Nejdůležitější služby pro internetovou a lokální komunikaci

Služba	Obvyklý port	Doporučené nastavení	
		Směrem ven	Směrem dovnitř
Internetové služby			
WWW (webové stránky)	TCP 80	propustit	blokovat
HTTPS (bezpečný web)	TCP 443	propustit	blokovat
SMTP (pošta)	TCP 25	propustit	blokovat
POP3 (pošta)	TCP 110	propustit	blokovat
IMAP4 (pošta)	TCP 143	propustit	blokovat
DNS (překlad jmen)	UDP/TCP 53	propustit	blokovat
FTP (přenos souborů)	TCP 20,21	propustit	blokovat
Lokální služby (sítě Microsoft)			
	UDP 67/68	propustit	propustit jen v důvěryhodné síti
	TCP/UDP 88	propustit	propustit jen v důvěryhodné síti
	TCP/UDP 135-139	propustit	propustit jen v důvěryhodné síti
	TCP 389	propustit	propustit jen v důvěryhodné síti
	TCP 445	propustit	propustit jen v důvěryhodné síti

Upozornění: tabulka obsahuje jen výběr důležitých služeb