

# Krizové nasazení IPS sondy při šíření malwaru v síti

**Někteří pokročilí domácí uživatelé občas namítnou, že antivirus nepotřebují a stačí používat zdravý selský rozum, aby se člověk problémům s malwarem vyhnul. Na úrovni firemní sítě se ale na selský rozum rozhodně nedá spoléhat.**

ROBERT ŠEFR

Antivirus je pro základní ochranu absolutní nutností, ovšem často bohužel i vrcholem bezpečnostních opatření uvnitř sítě. Roky mediální masáže týkající se aktualizací a způsobu využívání antivirů daly útočnickům dostatek času se na doporučená prostředí připravit.

Jeden z případů, kdy aktualizace selhávají, jsou takzvané 0-day exploity (zranitelnosti nulového dne). Výborný příklad takového exploitu se objevil poměrně nedávno – zranitelnost ve zpracování zástupců zneužitelná od Windows XP po Windows 2008 R2 (CVE-2010-2568).

Byla hojně zneužívána velkým množstvím malwaru prakticky ihned po uveřejnění. Stačilo podvrženého zástupce zobrazit v průzkumníkovi a malware byl automaticky spuštěn, aniž uživatel musel provádět další akce. Detailně popsany exploit a přímočarost jeho zneužití měly za následek renesanci starších kódů, konkrétně sofistikovaného viru Sality, kterému tvůrci tímto exploitem opět vlili krev do žil.

## Praktický příklad

Sality patří do skupiny polymorfních virů. Ty mění dynamicky svůj kód, tak aby unikly detekci antiviru, a infikují další spustitelné soubory. Sality navíc zvládá vyřadit z provozu několik desítek antivirových softwarů, takže po úspěšné infekci systému se stává téměř neomezeným vládcem a dále se pomocí zmíněného exploitu šíří po sdílených složkách.

V konkrétním případě, se kterým jsme se setkali, bylo napadeno virem Sality několik stovek počítačů. Antivirus neměl ve chvíli napadení k dispozici signatury proti této mutaci, takže virus se po síti šířil velmi jednoduše. Důležité bylo získat rychle kontrolu nad sítí.

Výrobce antiviru od nás dostal podklady pro tvorbu signatury (nakažené soubory).

Nakažené stroje bylo zatím možné čistit nástrojem McAfee Stinger (je zcela zdarma) určeným pro odstraňování perzistentního malwaru a rootkitů. V rozlehle síti ale nebylo jednoduché určit, které stroje jsou nakažené, případně které jsou hlavním zdrojem infekce (resp. komunikace s outsourcovanými správci firewallů byla natolik zdlouhavá, že jsme ji vzdali a hledali jiné řešení).

Vzhledem k tomu, že Sality funguje zároveň jako downloader (stahuje na infikované stroje další malware), bylo jisté, že infikované stroje se budou na síti chovat velmi agresivně. Rozhodli jsme se proto použít síťovou IPS sondu (McAfee Network Security Sensor), jejíž nasazení bylo otázkou necelých dvou hodin.

Nijak jsme nezasáhli do chodu sítě, sondu jsme nasadili pouze v detekčním módu na monitorovacím portu switchu. Z provozu bylo během několika minut zřejmé, které stroje bude nutné odpojit a vyčistit.

Infikované stroje zkoušely v síti velké množství útoků – od průzkumných, jako je skenování portů, po pokusy o exploitaci a přetečení zásobníku ve službách MS Windows nebo hádání hesel.

Během dalšího dne byla k dispozici aktualizace signatur pro antivirus, a tato konkrétní infekce byla zažehnána. Podobné situace se však mohou, a v rozsáhlé síti pravděpodobně budou, opakovat.

Antivirus je příliš lokální a těžkopádné řešení, které si samostatně s většími problémy nemůže poradit.

## Použijte pokročilé nástroje

McAfee Network Security Sensor poskytl při tomto jednorázovém zásahu dostatečné informace, ale pro dlouhodobé sledování a korelaci síťového provozu je vhodnější použít specializovaný nástroj, například McAfee Network Threat Behavior Analysis, který zpracovává netflow data ze switchů nebo IPS sond a dává administrátorům globální pohled na dění na síti.

Security Sensor odvede mnohem více práce při nasazení v in-line módu, ve kterém může útoky přímo zadržovat, než při monitorovacím IDS nasazení, které bylo zvoleno v uvedeném příkladě. V IPS módu sonda zabráni prvotní infekci, pokud je útok veden zvenku (např. stažený soubor), případně zabráni propagaci do dalších segmentů sítě, pokud je útok veden zevnitř (třeba nakažený flashdisk).

Pro útočníky ale není IPS žádnou neznámou ochranou a snaží se útoky maskovat. Typicky to provádějí změnou pořadí paketů, úpravou kódování nebo porušováním standardu použitého protokolu (souhrnně jsou tyto metody nazývány evasion techniques).

Sebelepší signatury mohou být nepoužitelné, pokud je útočník takto dokáže schovat před logikou IPS zařízení. Jeden z parametrů, který nás nadále utvrzuje ve vhodnosti volby řešení McAfee, jsou výsledky testů NSS Labs.

Kromě velmi vysoké propustnosti a kvalitních signatur (detekce přes 90 % oproti průměru konkurence, který je přibližně 50 %) zvládla sonda McAfee detekovat 100 % zmíněných „evasion techniques“.

Vyhrazená McAfee IPS sonda (nefunguje na klasické x86 architektuře, ale jde o dedikované čipy pro filtraci síťového provozu) umožňuje vytvářet virtuální síťová rozhraní podle VLAN nebo síťových rozsahů. Provoz celé interní sítě může být kontrolován na jediném zařízení, na kterém je pro každý segment definována odlišná politika.

Všechny tyto funkce mají dohromady jediný cíl: znepřístupnit život útočnickům, kteří si již navykli na antiviry a aktualizované operační systémy, ale s minimální prací pro administrátora a bez dopadu na infrastrukturu.

*Autor pracuje jako IT security consultant ve společnosti Comguard.*