TRAPS

Vyspělá ochrana koncových bodů

Řešení Palo Alto Networks® Traps™ poskytuje vyspělou ochranu koncových bodů, která brání sofistikovaným útokům proti známým slabinám a blokuje neznámý malware. Dosahuje toho prostřednictvím vysoce škálovatelného a nenáročného agenta, který používá inovativní nové pojetí obrany před útoky bez jakýchkoli předchozích poznatků o konkrétních hrozbách. Traps tak organizacím poskytuje účinný nástroj na ochranu koncových bodů před prakticky každým cíleným útokem.

Vyspělá ochrana koncových bodů by měla:

- Bránit všem útokům včetně těch, které zneužívají dosud neznámé slabiny
- Bránit všem škodlivým spustitelným souborům bez nutnosti předchozí znalosti
- Detailně dokumentovat zastavené útoky
- Být vysoce škálovatelná, nenáročná a nijak nenarušovat normální provoz
- Úzce se integrovat se síťovým a cloudovým zabezpečením

Navzdory přemíře produktů pro zabezpečení koncových bodů na trhu stále dochází k alarmujícímu množství napadení koncových bodů. Tradiční metody ochrany koncových bodů jednoduše nedrží krok s rychlým vývojem hrozeb (viz Obrázek 1). Místo snahy identifikovat každý z miliónů jednotlivých útoků nebo rozpoznat nebezpečné chování, které může být nezjistitelné, se řešení Traps soustředí na stěžejní techniky, které musí při realizaci útoku každý útočník uplatnit. Takovým přístupem dokáže zmařit útoky ještě předtím, než se může nebezpečná aktivita naplno projevit.

Různé typy útoků, ucelená ochrana

Útoky mívají nejrůznější formy a pronikají do počítačů různými cestami včetně webu, e-mailu a externích úložišť. Většina tradičních bezpečnostních produktů chrání koncové body před škodlivými spustitelnými soubory, které však představují tu nejméně sofistikovanou podobu útoků. Vyspělejší a cílenější útoky se do počítačů dostávají v podobě zdánlivě neškodných datových souborů, které otevírají legitimní aplikace. Škodlivý kód se totiž dá skrýt například do dokumentu Microsoft® Word® nebo PDF. Řešení Traps chrání koncové body blokováním

Obrázek 1: Nedostatky tradičních pojetí zabezpečení

malwaru v podobě spustitelných souborů a útoků v podobě datových souborů nebo síťových průniků.

Nejvyspělejší hrozby v současné době zneužívají slabiny v aplikacích, které běžně používáme. Často se šíří v podobě běžně používaných datových souborů (pdf, rtf, doc, ppt, xls aj.) nebo bývají individuálně zacílené na proprietární software používaný v různých odvětvích.

Jakmile se takový soubor otevře, škodlivý kód zneužije slabinu v legitimní aplikaci, aktivuje se a převezme plnou kontrolu nad koncovým bodem.

Jak prevence útoků funguje

Při každém útoku bez ohledu na komplikovanost musí útočník vykonat určitou sérii útočných technik. Některé útoky mohou mít víc kroků, jiné méně, ale ve všech případech musí být provedeny alespoň dvě nebo tři techniky, aby bylo možné cílový koncový bod zneužít. Řešení Traps používá několik modulů prevence narušení, které umí blokovat různé techniky používané útočníky. Každý útok navíc musí použít několik těchto technik v sérii, aby byl úspěšný. Na počítači s řešením Traps jsou takové útočné techniky zcela neúčinné, takže aplikace už nejsou zranitelné.

Agent Traps se při spuštění vloží do každého procesu. Pokud se pak nějaký proces pokusí provést některou z klíčových útočných technik, pokus o útok narazí, protože se agent Traps postaral o imunitu procesu proti útočným technikám. Traps útočnou techniku okamžitě zablokuje, ukončí proces a uvědomí o zastavení útoku uživatele i administrátora. Zároveň všechny detaily nahlásí součásti Endpoint Security Manager (viz Obrázek 2). Vzhledem k řetězové povaze většiny útoků k zablokování celého útoku stačí zabránit jen jedné technice v řetězci.

Výchozí zásady Traps chrání víc než 100 procesů – každý z nich desítkami proprietárních modulů EPM (Exploit Prevention Module). Ovšem na rozdíl od jiných produktů není řešení Traps omezeno jen na ochranu těchto procesů či aplikací.

Protože se soustředí na útočné techniky a ne na samotné útoky, dokáže útokům bránit i bez předchozích poznatků o slabině, bez nainstalovaných oprav a bez signatur nebo aktualizací softwaru. Je důležité rovněž poznamenat, že Traps se nesnaží vyhledávat nebo monitorovat škodlivé aktivity, což má obrovskou výhodu vzhledem k minimálním nárokům na CPU a paměť.

Prevence škodlivých spustitelných souborů

Kromě prevence narušení používá Traps vícevrstvé pojetí prevence škodlivých spustitelných souborů. Pro zajištění ucelené ochrany se soustředí na tři klíčové oblasti (viz Obrázek 3). Kombinace těchto metod nabízí bezkonkurenční úroveň ochrany před malwarem:

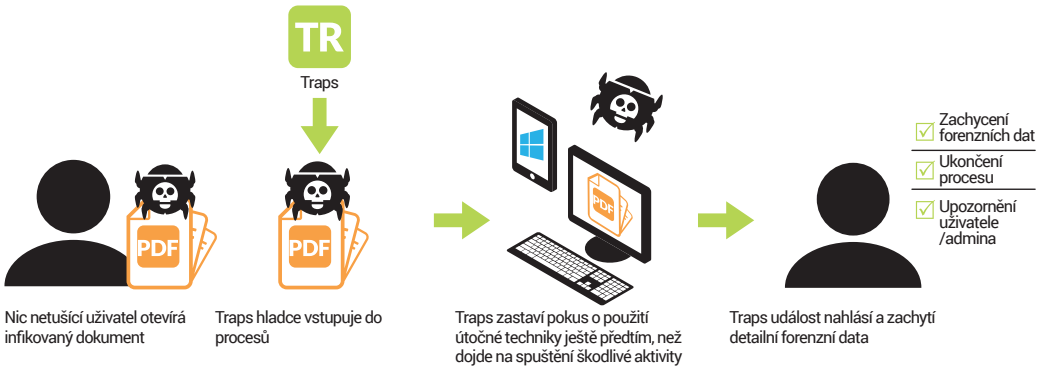
1. **Restrikce založené na zásadách:** Organizace mohou snadno nadefinovat zásady omezující konkrétní scénáře spouštění. Můžete například chtít zabránit spouštění souborů z adresáře .tmp Outlooku nebo zakázat spouštění určitého typu souborů přímo z USB jednotky.
2. **Vyspělá kontrola spouštění:** Agent Traps umožňuje granulární kontrolu nad vnořenými procesy, složkami, nepodepsanými spustitelnými soubory atd., nabízí také možnosti robustnějšího zabezpečení systému detailním ovládáním toho, jaké aplikace nebo hodnoty hash se mohou spustit
3. **Inspekce a analýza v prostředí WildFire™:** Agent Traps posílá v dotazech na cloudovou službu WildFire hodnoty hash a zároveň zasílá k rizikovému prověření všechny neznámé soubory .exe.
4. **Zmírňování technik malwaru:** Řešení Traps brání útokům blokováním používaných útočných technik, jako je například vkládání kódu.

Dokumentování útoků

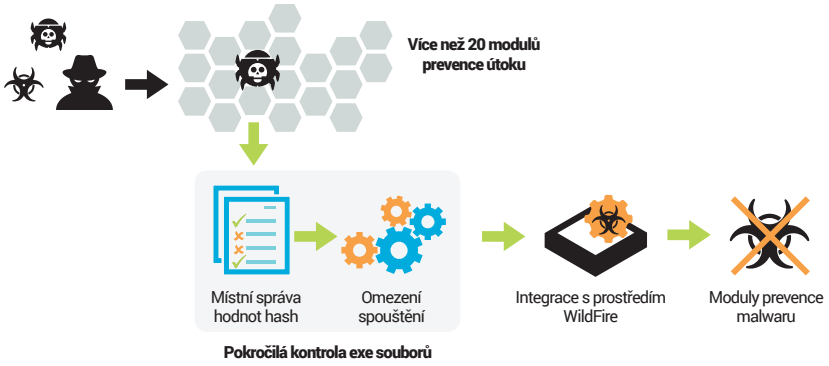
Forenzních informací zachycených o zastaveném útoku je nevyhnutelně méně než informací dostupných o útoku, který uspěl a napáchal škody. Navzdory tomu se i při odvrácení útoků dá získat spousta cenných poznatků. Na základě takových záznamů o pokusu o útok mohou organizace nasadit proaktivní obranné mechanismy i na jiné koncové body, které nemusí být chráněny.

Agent Traps zachycuje spoustu dat. Průběžně zaznamenává detaily o všech spuštěných procesech a předává zaznamenané informace součásti Endpoint Security Manager (ESM). Pokud zastaví nějaký útok, lze z koncového bodu stáhnout další detaily včetně úplného výpisu paměti a informací o aktivitách, o které se škodlivý kód pokoušel.

Traps umožňuje vyhledávat podle souborů, složek a registrů a umí na pomoc s probíhajícím vyšetřováním dotazovat všechny koncové body.



Obrázek 2: Prevence útoku – z pohledu uživatele



Obrázek 3: Správný způsob prevence škodlivých spustitelných souborů

Architektura nasazení Traps

Endpoint Security Manager – konzola

Infrastruktura Traps podporuje různé varianty architektury, takže je plně škálovatelná v rozsáhlých, distribuovaných prostředích. Při instalaci ESM se vytvoří databáze Microsoft SQL Server® a nainstaluje administrativní konzola v rámci IIS. Jsou podporovány verze Microsoft SQL 2008, 2012 a 2014 a SQL Server může být vyhrazený pro ESM anebo lze databázi vytvořit na existujícím SQL Serveru.

Endpoint Security Manager – servery

Servery ESM v zásadě fungují jako proxy mezi agenty Traps a databází ESM. Komunikace mezi agenty Traps a servery ESM probíhá přes HTTPS. Servery ESM neukládají žádná data, a tak se dají do síťového prostředí snadno přidat nebo z něj odebrat, aby bylo zajištěno dostatečné geografické pokrytí a redundance.

Agent Traps

Instalátor agenta Traps je balíček MSI o velikosti zhruba 10 MB, který se dá nasadit pomocí libovolného nástroje na distribuci softwaru. O následné aktualizace agenta se pak už může starat ESM.

Na disku agent zabírá necelých 25 MB a za chodu v paměti méně než 40 MB. Využití CPU se v praxi pohybuje pod úrovní 0,1 procenta. Na ochranu před manipulací používá agent různé metody, které zabraňují uživatelům a škodlivému kódu vypnout ochranu a zasáhnout do konfigurace agenta.

Nenáročná struktura umožňuje snadné horizontální škálování prostředí Traps pro rozsáhlé instalace až s 10 000 agentů na jeden ESM při zachování centralizované konfigurace a databáze zásad. Řešení Traps může koexistovat s většinou významných řešení na zabezpečení koncových bodů a jeho nároky na CPU a celkové vytížení systému jsou mimořádně nízké. Proto se optimálně hodí pro kritické infrastruktury, specializované systémy a prostředí VDI.

Externí protokolování

Kromě interního ukládání protokolů dokáže ESM zapisovat protokoly i na externí protokolovací platformu, například SIEM; podporuje formáty CEF, LEEF a syslog. Organizaci, která nasadí několik serverů ESM, umožňuje externí protokolovací platforma získat souhrnný přehled o všech databázích protokolů. Zaznamenané kritické události je navíc možné přesměrovat na e-mail.

Pokrytí a podporované platformy

Traps chrání systémy bez nainstalovaných oprav a je podporováno na jakékoli platformě s Microsoft Windows®: desktopech, serverech, průmyslových řídicích systémech, terminálech, VDI, virtuálních počítačích, integrovaných systémech atd. Řešení je navíc mimořádně nenáročné na systémové prostředky a dá se rozšířit pro ochranu procesů jakékoli aplikace. Proto se ideálně hodí na ochranu specializovaných systémů včetně bankomatů, pokladních systémů, systémů SCADA a mnoha dalších průmyslových aplikací, které potřebují neinvazivní ochranu proprietárních procesů.

Traps aktuálně podporuje následující:

Operační systém
Windows XP (32-bit, SP3 a novější)
Windows Vista (32-bit, 64-bit a SP2)
Windows 7 (32-bit, 64-bit, RTM a SP1; všechny edice kromě Home)
Windows 8 (32-bit, 64-bit)
Windows 8.1 (32-bit, 64-bit)
Windows 10 (32-bit, 64-bit)
Windows Server 2003 (32-bit, SP2 a novější)
Windows Server 2003 R2 (32-bit, SP2 a novější)
Windows Server 2008 (32-bit, 64-bit)
Windows Server 2012 (všechny edice)
Windows Server 2012 R2 (všechny edice)

Virtuální prostředí
Virtual Desktop Instance (VDI)
Virtual Machine (VM)
Citrix, VMware, VirtualBox a Parallels
Fyzické platformy
Desktopy, servery a tablety s Windows
Systémy průmyslového řízení (ICS) a SCADA
Bankomaty a pokladní systémy
Podporované prohlížeče
Internet Explorer 10 a novější
Chrome 27 a novější
Firefox 22 a novější
Opera 12 a novější

4401 Great America Parkway-
Santa Clara, CA 95054
Ústředna: +1.408.753.4000
Prodej: +1.866.320.4788
Podpora: +1.866.898.9087
www.paloaltonetworks.com

PAN_DS_TRAPS- AED-100115

NOTES