McAfee Advanced Threat Defense (ATD) SANDBOX

Find, Freeze and Fix: Nová koncepce v boji proti „advanced malware"

McAfee ATD je sofistikované řešení kombinující několik přístupů k identifikaci ne/známého (zero-day) pokročilého škodlivého kódu (Advanced Malware). Integruje se nejen se stávající McAfee infrastrukturou, tzn. od perimetru až po koncová zařízení, ale ve větších organizacích maximalizuje schopnost detekovat jakýkoli malware i efektivně na nákazu reagovat v minimálním časovém rozpětí.

K čemu je McAfee ATD Sandbox?

Slouží jako místo pro simulaci reálných akcí, které by proběhly na koncovém stroji po „spouštění" analyzovaného kódu. McAfee ATD umožňuje simulovat až 60 virtuálních image **přesně dle prostředí zákazníka** (na rozdíl od poskytovatelů virtuálních sandboxů kde jsou systémy unifikované) a nabízí i **analýzy pro malware obcházející detekci** ve virtuální prostředí sandboxu. Po analýze poskytuje detailní popis toho, jak se malware chová na cílovém stroji a umožní adekvátní zásahy i na IPS, Email a web gateway či endpointech na úrovni informační i reaktivní.

Klíčové vlastnosti:

Efektivní a výkonná analýza malware

> Využívá sofistikované metody „rozbalení" kódu pro efektivní a kompletní analýzu
> Jedinečná kombinace dynamické a statické analýzy

Úzká integrace nejen s McAfee produkty

> Propojuje a urychluje všechny fáze ochrany před malware od detekce až po odstranění nákazy z celé sítě.

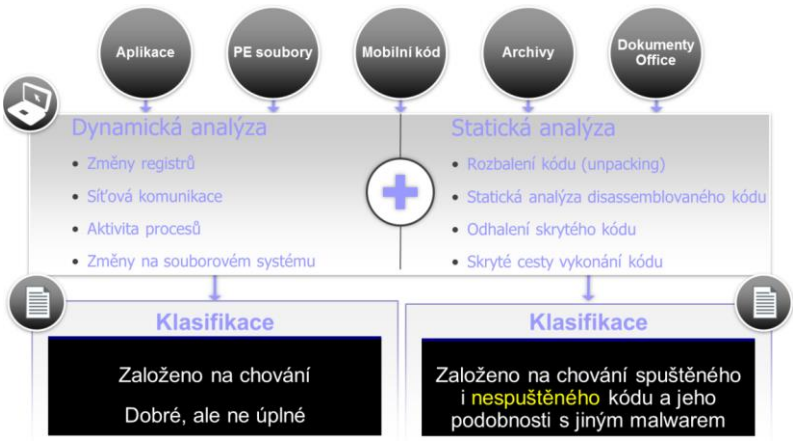
Centralizace analýz pokročilého malware

> Úspora nákladů díky sdílení informací mezi jednotlivými bezpečnostními prvky
> Snadné nasazení ve formě appliance

Find: Dynamická a statická analýza

Dynamická analýza je založena na **Sandboxingu** - otevírání příchozích dokumentů a aplikací ve vlastním obrazu virtuálního stroje, který přesně odpovídá typickému prostředí/stroji organizace, tzn. má stejnou konfiguraci i softwarové vybavení (např. gold image: Windows 7 Pro SP1, Mozilla Firefox 20, MS Office 2010, Adobe Reader X 10.1). Cílem je ověřit, jak se budou příslušné dokumenty a aplikace v prostředí organizace chovat. Některé druhy malware jsou schopny dynamickou analýzu obcházet, např. pozdržením spuštění škodlivého kódu, detekcí virtuálního prostředí a ukončení běhu, nebo čekáním na uživatelský vstup.

Odpovědí je statická analýza, která rozklíčuje veškeré „funkce" a chování škodlivého kódu bez ohledu na to, zda jsou v konkrétním prostředí uplatnitelné. Mapuje všechny možné alternativy běhu kódu. Tento způsob detekce je vysoce účinný proti snahám malware vyhnout se detekci či maskovat své aktivity. Samotná ochrana proti dynamické analýze je jeden z indikátorů toho, že se může jednat o malware.



Významným způsobem šetří zdroje díky několika vrstvám anti-malware kontroly. V prvních fázích se využívají „klasické" antivirové detekční metody, kterými jsou zejména:

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

- antivirové signatury McAfee poskytující rychlou detekci známého malware.
- McAfee Global Threat Intelligence (GTI) – globální reputační systém poskytující informace o výskytu malware na webových stránkách, škodlivých emailech, IP adresách a dalších entitách spolu s přiřazením reputačního skóre.
- Real-Time Emulation Engine simulující spuštění na koncovém zařízení a zaznamenávající následné chování kódu. Tento přístup je nazýván jako „jednoduchý" sandboxing, jelikož nevyužívá tolik zdrojů jako dynamická analýza.

Pokud tyto metody na stupnici od 1 do 5 bezpečně neidentifikují škodlivost kódu, spouští se dynamické a statické analýzy kódu v „reálném" prostředí, na které je malware zaměřen.

Freeze: Žádné další šíření škodlivého kódu – McAfee ATD buď přímo, nebo pomocí TIE úzce integruje s dalšími bezpečnostními řešeními od perimetru až po koncové body, kterým umožňuje okamžitě zakročit v okamžiku, kdy ATD detekuje malware.

McAfee Threat Intelligence Exchange (TIE) je platforma, která kombinuje sílu bezpečnostních McAfee produktů (i produktů třetích stran) a v reálném čase zajistí blokaci a šíření malware na další koncové stroje (či ven z korporátní sítě), případně nakažené stroje umístí do karantény, odřízne infikované stroje od Command & Control center a zastaví aktuálně běžící instance malware. Zajišťuje také komunikaci mezi VirusScan Enterprise na koncových strojích a McAfee ATD takovým způsobem, že antivirus na koncové stanici se může rozhodnout využít pokročilé skenovací metody ATD v případě podezřelých souborů. McAfee zároveň skrze TIE otevírá své produkty informacím třetích stran. Blacklisty IP adres, URL, hashů, odcizených certifikátů a dalších „Indicators of Compromise" mohou být skrze tuto komunikační vrstvu automaticky distribuovány mezi bezpečnostní řešení bez nutnosti dodatečného skriptování a údržby. Kromě automatizované distribuce informací pomáhá TIE i analytikům se sběrem informací z koncových strojů a jejich interpretací na úrovni ePolicy Orchestratoru. Analytik tak dostane k dispozici seznamy podezřelých souborů, jejich umístění, hashe, a další metadata. Zároveň může přímo z ePO ověřit, jaké informace o daných souborech poskytuje služba VirusTotal. Architektura TIE je cíleně postavena tak, aby integrace do stávající sítě proběhla jednoduše a během několika okamžiků.

McAfee Cloud Threat Detection – Jedná se velmi účinné a cenově dostupné řešení, které nabízí cloudově založenou statickou analýzu pro posouzení škodlivosti souboru. Využívá metodu „machine learning", která pracuje s poznatky získané z McAfee Labs. Cloud Threat Detection využívá kombinace cloudové analýzy a informací získaných z řad McAfee produktů (především z McAfee Web Gateway a Network Seucrity řešení). Nad těmito daty pak uplatňuje své analýzy za využití strojového učení a tzv. Big Dat (spolupráce s McAfee Labs). Díky tomu dokáže klasifikovat a detailně popsat známé i neznámé hrozby a poskytnout detailní data pro další analýzy (metadata, URL adresy, názvy souborů stanic a jejich lokaci). McAfee Cloud Threat Protection vyžaduje spolupráci buď s McAfee Web Gateway nebo Network Security IPS zařízeními.

Přímá integrace s McAfee produkty:

- **McAfee Web Gateway –** přeposílá podezřelé soubory na komplexní analýzu
- **McAfee Network Security Platform -** vytahuje soubory z protokolů SMTP, HTTP a HTTPS
- **McAfee Endpoint Threat Defense and Response –** využití dynamické analýzy na základě reputace, analýza chování a využití strojového učení
- **McAfee Enterprise Security Manager** – rychlá identifikace, vyšetřování a řešení bezpečnostních incidentů
- **McAfee Threat Inteligence Exchange (TIE) –** kombinuje data z více zdrojů.
- **REST API -** jakékoliv další řešení může poslat na McAfee ATD soubory na otestování skrze API.

Fix: napravit napáchané škody - V této fázi se jedná o odstranění dopadů malware na koncových strojích skrze McAfee ePolicy Orchestrator, jako jsou změny v registrech, soubory zapsané na disk, úpravy konfigurací, aj.

Modelová řada	ATD-3000		ATD-6000	
Velikost v racku	1U		2U	
Výkon (možnost vytvářet clustery)	Až 150.000 objektů denně		Až 250.000 objektů denně	
Počet virtuálních strojů*	30		60	
Maximální kapacita	600 GB		1200 GB	
Virtuální modelová řada	ATD-VM1008	ATD-VM1016	ATD-VM3032	ATD-VM6064
Počet instancí sandboxů	8	16	32	64
Podporované typy souborů	PE, Adobe, MS Office, archivy, obrázky, Java, Android Application Package, URL adresy			
Metody analýzy	McAfee Anti-Malware, GTI reputation: file/URL/IP, Gateway Anti-Malware (emulation and behavioral analysis), dynamic analysis (sandboxing), in-depth code analysis, custom YARA rule			

* ATD dokáže alokovat pro každou VM instanci pouze jedno jádro