Detekce kybernetických útoků pomocí IP Flow

Účel tohoto dokumentu

Množství kybernetických útoků stoupá neustále. Jsou sofistikovanější, přesněji cílené a dokážou překonat standardní postupy ochrany sítě na jejím perimetru. Pokud tyto útoky prolomí bezpečnostní mechanismy, mohou se snadno rozšířit v síti organizace a šance na obranu budou velmi limitované. Většinou se zaměřují na citlivá data, systémy, specifické uživatele a zcizují duševní vlastnicí, korporátní a státní tajné informace v úmyslu vydobýt si nekalou konkurenční výhodu v komerčních i státních sektorech.

Tento dokument popisuje:

- Největší výzvy v ochraně sítí proti pokročilým kybernetickým hrozbám
- Řešení pokročilých kybernetických útoků za pomoci IP Flow
- Jak využít své stávající podnikové infrastruktury, pro usnadnění nasazení a nižší náklady na řešení

Obrázek 1: Výčet výrobců zařízení, z nichž Flowmon umí exportovat provozní data[i]

Výzvy

Již známé kybernetické hrozby jsou efektivně detekovatelné a potlačené systémy firewall, antivirus, IDS/IPS, nebo dalšími nástroji. Avšak pokročilé hrozby jsou vyvíjeny tak, aby nebyly odhalitelné běžnými nástroji, a pokud proniknou chráněným perimetrem sítě, mohou se snadno a nekontrolovatelně šířit a chovat se tak, aby se zdály být legitimními. Díky jejich skryté aktivitě mohou získat přístup k citlivým informacím a systémům a to po dlouhou dobu bez odhalení. Naše výzva je umět tyto hrozby detekovat, ne pouze vyvíjet způsoby jak těmto situacím čelit ve chvíli, kdy se v ní ocitneme.

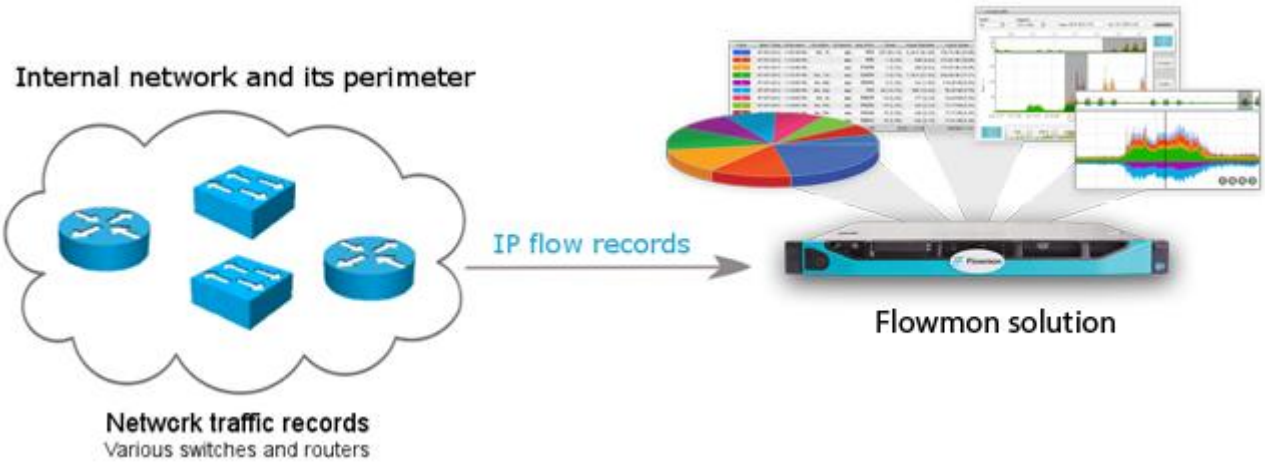
Jedním z příkladů je malware známý jako Flame, který operoval nedetekovaný po dobu pěti let, než byl nakonec pouhou náhodou odhalen. Flame pronikl do více než pěti tisíc sítí, kradl data a uděloval přístup na infikované stanice.

Analýza aktivit v datové síti je jediná metoda detekce takovýchto kybernetických útoků. I přesto, že se zdají být neviditelné v legitimním datovém provozu, mohou být odhalené za pomoci detailní analýzy síťového provozu a detekcí opravdových provozních anomálií. Takováto analýza a detekce byly plně zautomatizovány, protože dnešní velikosti provozů na sítích, jejich komplexitě a dynamičnosti byla tato činnost manuálně neproveditelná.

Řešení

Řešení pokročilých kybernetických hrozeb na datových sítích kombinuje níže uvedené elementy pro zajištění kompletního pohledu do sítě a automatickou detekci kybernetických hrozeb:

- Náhled do provozu sítě je zajištěn aktivními síťovými prvky (routery, switche), které jsou schopny generovat IP flow záznamy (NetFlow, JFlow, sFlow, IPFIX,…) o komunikaci v síti.
- Automatická analýza provozu sítě se provádí systémem FlowMon, který byl opakovaně zaznamenán analytickou společností Gartner v jejich reportu výrobců těchto technologií jako jeden z deseti nejlepších řešení pro monitoring provozu sítě a detekci pokročilých hrozeb na světě.



Obrázek 2: Komponenty řešení pro detekci kybernetických útoky na základě analýzy IP flow.

Odborníci na bezpečnost získají díky tomuto ucelenému řešení úplný přehled o problémech, anomáliích nebo výskytu specifických aktivit, které jsou běžně následovány úspěšnými útoky. Typické útoky zahrnují:

- Hledání slabých článků sítě – pokusy pro identifikaci možných cílů útoků, nebo šíření nebezpečného softwaru,
- Malware mitigation – útoky na stanice v rámci vnitřní sítě za účelem sběru dat, nebo vytvoření „zadních vrátek“ pro neautorizovaný přístup do síti,
- Botnety – probíhající komunikace mezi koncovými stanicemi a kontrolními systémy útočníků,
- Únik dat – únik citlivých informací z interní sítě za pomoci malwaru nebo vnitřních útočníků.

Přínosy

Řešení Flowmon se zaměřuje na detekci komplexních a nebezpečných hrozeb, které se nabourávají do interních sítí i přesto, že je chráněn perimetr a může nepozorovaně operovat po celé měsíce či roky. Hlavní přínosy zahrnují:

- Ochrana vnitřku sítě, která je nejvíce zranitelná pro pokročilé kybernetické hrozby,
- Detekce hrozeb blíže k původu a včas, čímž se minimalizuje škoda a snižuje se riziko dalšího šíření.
- Škálovatelný, neinvazivní a efektivní monitoring bezpečnosti celé sítě.
- Zjednodušení a automatizace cenově náročného manuálního procesu kontroly incidentů.
- Schopnost využít stávající síťové infrastruktury.

Komponenty řešení

Náhled na provoz v celé síti
Nová funkcionalita mnohých routerů a switchů poskytuje celistvý monitoring sítě – od uživatelských stanic, serverů, až po mobilní zařízení. Většina dnešních switchů a routek dodávají nativní IP flow data bez výkonnostního zatížení prvku. Díky těmto datům je možné detekovat hrozby, které proniknou perimetrem sítě a snaží se ukrýt v běžném provozu.

Agregace IP flow dat, ukládání a analýza pro detekci útoků a podezřelého chování
Flowmon přední řešení v oblasti Network Behavior Analysis (NBA), poskytuje automatickou detekci hrozeb, incidentů a anomálií. Flowmon zpracovává data v reálném čase a tím zajišťuje prostor pro okamžité řešení problémů. Flowmon také zajišťuje dlouhodobé ukládání provozních dat pro případnou forenzní analýzu a to až několik let zpětně. Hlavní komponenty Flowmon řešení jsou:

- Flowmon kolektor – pro agregaci a ukládání IP flow dat (NetFlow v5/v9, IPFIX, sFlow, JFlow, atd.) z neomezeného počtu zdrojů. Poskytuje pokročilé nástroje pro reporting a analýzu IP flow dat.
- Flowmon ADS (Anomaly Detection System) – systém pro zapracování IP flow dat a hrozeb za použití principů Network Behavior Analysis technology.

Volitelné součásti řešení Flowmon zahrnují:

- Flowmon sondy - specializovaná zařízení pro export NetFlow nebo IPFIX dat z prostředí, kde není možné generovat IP flow data za pomoci stávající síťové infrastruktury.

Jak chránit Vaši síť před pokročilými kybernetickými hrozbami?

Kombinace exportu IP flow dat z aktivních síťových prvků a řešení Flowmon pro automatickou detekci hrozeb poskytuje efektivní způsob, jak chránit Vaši organizaci před pokročilými kybernetickými hrozbami, kde běžně používané nástroje nestačí. S kompletní viditelností do vnitra sítě, řešení zjednodušuje její správu a snižuje náklady na provoz a vývoj.

Více informací

Pro více informací, prosím kontaktujte Flowmon Networks nebo Vašeho Flowmon Networks partnera.

[i] Použitá loga patří jejich příslušným vlastníkům