Případová studie

COMGUARD
communication security

lastline

Efektivní ochrana proti pokročilému malwaru pro významnou bankovní instituci v ČR (NextGenerationSandbox)

Již několikrát jsme se prostřednictvím médií mohli dozvědět, že na finanční sektor bývají nejčastěji cíleny útoky hackerů. Těmito útoky mohou hackeři způsobit nemalé škody, jak těmto finančním institucím, tak i klientům využívajících jejich služby, v případě nedostatečného zabezpečení jejich IT infrastruktury. Většina bankovních institucí pracuje s citlivými daty svých klientů, a proto musí klást maximální důraz na jejich zabezpečení a zabránit jejich úniku skrze možné vektory.

Pro zajištění ochrany musí preventivně předcházet možným bezpečnostním rizikům a pro dosažení maximální míry zabezpečení jsou mimo klasické bezpečnostní IT technologie nezbytnou součástí i pokročilejší technologie, jako je sandbox, který dokáže odhalit i pokročilý malware, využívající různých maskovacích technik, kdy takovýto malware může být pro klasické IT security technologie prakticky neviditelný.

Výchozí situace

V rámci elektronické komunikace je tato bankovní instituce (dále jen společnost) vázána řadou interních směrnic a také značným počtem partnerských smluv, což samozřejmě vede ke kladení maximálního důrazu na aplikovaná bezpečnostní opatření. Společnost je vzhledem ke smluvním podmínkám také vázána přijímat v rámci elektronické komunikace určité typy souborů.

Z důvodů uvedených výše a povinnosti tyto soubory přijímat, vzniká zde značné riziko a možný vektor průniku škodlivého kódu do IT infrastruktury skrze emailovou komunikaci. Prostřednictvím infikovaného souboru by potenciální útočník mohl infikovat celou IT infrastrukturu zákazníka, čímž by mohl získat cenná data nebo narušit běžný chod společnosti.

Společnost hledala vhodné řešení, které dokáže testovat a kontrolovat soubory ve virtuálním prostředí, které bude nejvíce podobné jejich reálnému prostředí (image typického PC v infrastruktuře) a zároveň zde bude eliminováno riziko ohrožení vlastní interní sítě.

Tyto požadavky splňovaly pouze sandboxingové technologie, které v rámci virtuálního prostředí dokáží testovat různé soubory, aplikace apod. Sandbox dokáže vysledovat jejich chování po spuštění a zaznamenat jiné nekalé aktivity, maskovací techniky a další, které bývají používány pokročilým malwarem.

Společnost v minulosti testovala několik sandboxů od jiných výrobců, ale vždy tyto řešení neměly danou efektivitu při detekci a nesplnily tedy očekávání zákazníka.

Next Generation Sandbox od Lastline byl schopný tyto požadavky naplnit, a proto je také hodnocený, jako nejlepší na trhu, díky 100% detekci malwaru.

Případová studie

COMGUARD
communication security

Proof of Concept

Po testování konkurenčních zařízení společnost rozhodla, že upustí od záměru koupě. Nebyla spokojena s výsledky sandboxu, jelikož většina řešení využívá pro virtuální prostředí GOLD image, jenž dokáže pokročilý malware obejít. Dalším faktorem byla také licenční a cenová politika ostatních výrobců.

Po nepřesvědčivých výsledcích konkurenčních technologií společnost projevila zájem o řešení společnosti Lastline, kdy v sídle společnosti COMGUARD a.s. proběhla názorná prezentace technologie od tohoto výrobce a v rámci prezentace byly představeny unikátní funkcionality — Full System Emulation (FUSE), která nabízí kompletní simulaci prostředí počítače a umožňuje analyzování i nejpokročilejšího malwaru, ale také další přínosy Lastline.

Implementace a aktuální stav

Pro zákazníka byl použit Lastline Enterprise a PIN box appliance (all-in-one solution) běžící na vlastním hardware, jímž je server. V rámci testování technologie Lastline prováděla pouze monitoring emailové komunikace, aby prokázala, že v rámci ní se objevují infikované soubory. Následná identifikace potenciálně škodlivých souborů v emailové komunikaci, byl pro zákazníka jeden ze stěžejních faktorů, který jej motivoval k pořízení technologie, kdy v prvním týdnu monitoringu řešení zachytilo 3 škodlivé soubory, které nezachytily standardní bezpečnostní technologie nasazené v infrastruktuře zákazníka. Tyto soubory mohly ohrozit IT infrastrukturu zákazníka. Momentálně řešení funguje v módu in-line, což znamená, že je schopné přímo kontrolovat a blokovat infikované emaily nebo jejich přílohy.

V současnosti je Lastline integrován i s webovým provozem, kdy pomocí ICAP posílá stávající webová proxy stahované soubory, které přes ni projdou, k analýze do Lastline Enteprise. Zde probíhá kontrola a detekce souborů s integrovanými externími URL, obsahující skripty, spustitelné soubory, archivy atd. Na základě analýzy souborů v emailové a webové komunikace sandbox vyhodnocuje rizikové soubory a přiřazuje jim tzv. skóre dle jejich závažnosti.

Za dobu nasazení Lastlline, bylo z komunikace vybráno několik stovek podezřelých souborů. Sandbox vyhodnotil z uvedených podezřelých a potencionálně nebezpečných souborů téměř dvě desítky, jež vykazovaly známky nejvyššího skóre (95 ze 100) dle hodnotících kritérií Lastline. Tento výsledek potvrzuje, že i přes nasazené bezpečnostní technologie, které mají chránit IT infrastrukturu společnosti, prošly tyto vzorky, aniž by jimi byly zaznamenány.

Až díky Lastline Enterprise, který je nasazený za standardní emailovou ochranou a slouží, jako poslední linie ochrany a analýzy předtím, než je emailová komunikace doručena na emailový server, byly tyto nebezpečné soubory identifikovány.

Plány do budoucna

Tato bankovní instituce je spokojena s technologií Lastline, díky její efektivitě, jednoduchosti, variabilitě nasazení a do budoucna plánuje rozšíření jednotlivých Lastline funkcionalit o síťovou sondu Lastline Network Protection. Tato síťová sonda by pak měla v budoucnu za úkol analyzovat veškerý provoz v síti zákazníka, obdobným způsobem jako klasické technologie Intrusion Prevention System (IPS).

Klíčové vlastnosti Lastline Enterprise:

lastline

- **Vysoká účinnost detekce**
  (Nejlépe hodnocená detekční technologie dle NSS LABS)
- **Velmi malé procento False positives / False negatives incidentů**
- **Možnost napojení globální reputační databáze, která se proaktivně zdokonaluje a využívá machine learning techniky**
- **Korelace hrozeb dle závažnosti pro vaši síť**
- **Detailní náhled do průběhu útoku na vaši síť**
- **Otevřená API integrace s obsáhlou dokumentací**
- **Jednoduchá integrace s dalšími technologickými vendory**