SDK pro pokročilou kontrolu hrozeb (ATC)

Potřeba vícevrstvého zabezpečení

Vzhledem k neustálému nárůstu nových kybernetických hrozeb jsou tradiční bezpečnostní mechanismy nedostatečné a nespolehlivé pro zajištění odpovídající obrany. Každý měsíc se objeví více než 12 milionů nových a variantních kmenů malwaru, takže sledování a potlačování jednotlivých hrozeb je nesmírně náročné. Problém ještě zhoršuje skutečnost, že malware i mechanismy používané k jeho šíření jsou stále sofistikovanější. Velké obavy vzbuzuje zejména ransomware.

Četnost útoků ransomwaru se ztrojnásobila a ukázalo se, že způsobují rozsáhlé škody, včetně ztráty citlivých dat, výpadků provozu, ztráty produktivity a poškození dobrého jména. Mnoho nových variant ransomwaru je úspěšných, protože využívají různé vektory útoku, soubory a zranitelnosti, a jsou často polymorfní už svým designem. Díky tomu útoky unikají mnoha antimalwarovým řešením, která se při detekci většinou spoléhají na signatury známých rodin ransomwaru. Vzhledem k tomu, že hrozby jsou stále častější a sofistikovanější, firmy vyžadují vícevrstvá řešení ochrany, která jdou nad rámec tradičních technologií detekce signatur, a dokonce i standardního heuristického skenování.

SDK pro pokročilou kontrolu hrozeb

Sada Bitdefender Advanced Threat Control (ATC) SDK využívá proaktivní dynamickou technologii, založenou na pokročilých heuristických metodách k detekci hrozeb typu zero-day v reálném čase. SDK, vrstva ochrany při spuštění rozšiřuje komplexní technologie detekce Bitdefender před spuštěním, a umožňuje organizacím přidat další vrstvu ochrany, která výrazně snižuje riziko napadení systému novým nebo vyhýbavým malwarem.

Sada ATC SDK, která funguje na základě předpokladu nulové důvěryhodnosti, trvale monitoruje aktivní aplikace a procesy, aby zjistila, zda jakékoli známky nebezpečného chování. Spoléhá se na skutečné charakteristiky chování namísto signatur nebo binárních či kódových otisků, což umožňuje sadě SDK důsledně odhalovat nové varianty ransomwaru, další hrozby zero-day a útoky bez souborů.

Jak SDK funguje

Sada ATC SDK nepřetržitě monitoruje procesy běžící v operačním systému pomocí filtrů v uživatelském režimu a modelu jádra, a vyhledává jakékoli podezřelé příznaky nebo abnormální chování. Na rozdíl od jiných heuristických skenerů monitoruje SDK procesy po celou dobu, kdy jsou aktivní, takže jej nelze porazit zdržovací taktikou některých pokročilých malwarů. Toto neustálé monitorování v reálném čase také brání malwaru ve zneužití nebo ovládnutí již důvěryhodných aplikací.
Procesy jsou monitorovány, zda neprovádějí akce podobné malwaru, jako je kopírování nebo přesouvání souborů v systémových složkách nebo složkách systému Windows, nebo v diskových umístěních s omezeným přístupem; spouštění nebo vkládání kódu do prostoru jiného procesu, aby se spustil s vyššími právy; samoreplikace; vytváření položky automatického spouštění v registru, přístup k místům registru vyžadujícím zvýšená práva nebo provádění nezákonných operací v nich; vysazování a registrace ovladačů nebo akce specifické pro ransomware, jako je odstraňování záložních souborů / stínových kopií nebo generování šifrovacích klíčů a další.
Vzhledem k tomu, že legitimní aplikace někdy provádějí jednu nebo více z těchto akcí, SDK neurčuje proces jako škodlivý na základě jediné akce. Hledá chování specifické pro malware a každému procesu přiřazuje skóre na základě jeho akce a kontextu. To je důležité, protože proces nemusí při individuální analýze naznačovat škodlivý záměr, ale kolektivní analýza poskytne poznatky potřebné k jeho posouzení. Pokud celkové skóre procesu dosáhne určité prahové hodnoty, je proces nahlášen jako škodlivý a poté je ukončen.

Zero trust,
Always monitor running processes

Maintain process ledger
based on process behavior

Process is terminated when
given threshold is reached

Využití signatur a heuristiky s kolektivní inteligencí a strojovým učením

- SDK využívá cloud Bitdefenderu - **Bitdefender Global Protective Network (GPN)** - k získávání informací o nově objevených hrozbách. Centrální Cloud pro zpravodajství o hrozbách, který je vždy aktuální a k němuž má přístup jakýkoli systém, také výrazně snižuje potřebu lokálních databází signatur, které zpomalují počítače.
- Bitdefender Global Protective Network (GPN) provádí **11 miliard dotazů denně** a využívá reflexní modely a pokročilé algoritmy strojového učení k extrakci vzorů malwaru, čímž zajišťuje ochranu v reálném čase proti jakékoli hrozbě.

Hlavní vlastnosti a výhody

Proaktivní, dynamická technologie ochrany založená na nepřetržitém sledování chování procesů:

- Vysoká účinnost proti ransomwaru, zero-day exploitům a pokročilým trvalým hrozbám (APT)
- Včasné odhalení pokročilých útoků a prevence průniku, což snižuje náklady na reakci na incidenty
- Oceněná technologie - Bitdefender dosáhl v testech Real-World Protection 2019 společnosti AV-Comparatives průměrné míry detekce 99,9 %, a získal ocenění "Produkt roku" poté, co ve všech 7 testech, provedených v roce 2019, získal hodnocení "Advanced+"
- Inteligentní optimalizace výkonu pro monitorování aplikací a procesů zajišťuje nízký dopad na výkon systému;
- Určeno k usnadnění nápravy / vyčištění zjištěného malwaru;
- Funguje jako další nebo poslední vrstva obrany proti známým i neznámým hrozbám, a doplňuje řadu antimalwarových technologií Bitdefender.

Specifikace

Bezproblémový proces integrace pomocí vazeb na rozhraní C; umožňuje integraci prostřednictvím dynamicky propojené knihovny; - Podporuje systémy/koncové body běžící v systému Windows 7 a vyšším (x86/x64).

Vyhodnocení ZDARMA

Testování Bitdefender Advanced Threat Control SDK je bezplatné a zahrnuje technickou podporu.

Kontaktujte nás

Další informace o řešeních Bitdefender získáte na adrese www.bitdefender.cz/firemni-reseni

O licencování technologií společnosti Bitdefender.

Společnost Bitdefender poskytuje komplexní řešení kybernetické bezpečnosti a pokročilou ochranu před hrozbami více než 500 milionům uživatelů ve více než 150 zemích. Od roku 2001 společnost Bitdefender trvale vytváří oceňované bezpečnostní technologie pro podniky a spotřebitele, a stala se poskytovatelem, kterého si vybrali přední nezávislí dodavatelé softwaru (ISV), dodavatelé hardwaru, poskytovatelé služeb a podnikové organizace, které chtějí integrovat bezpečnostní technologie do svých produktů a služeb. V současné době má společnost Bitdefender více než 150 technologických partnerů po celém světě. Další informace jsou k dispozici na adrese www.bitdefender.cz/firemni-reseni

Bitdefender®

Založeno 2001, Romania
Počet zaměstnanců 1800+

Sídlo
Enterprise HQ – Santa Clara, CA, United States Technology HQ – Bucharest, Romania

COUNTRY PARTNER pro Českou republiku a Slovensko
IS4 security s.r.o., Praha, Česká republika

Bitdefender-OEM-ATC-Datasheet-crea4396-210x297-cs_PL
14/04/2015 5 April 2020 9:12 AM15/04/20