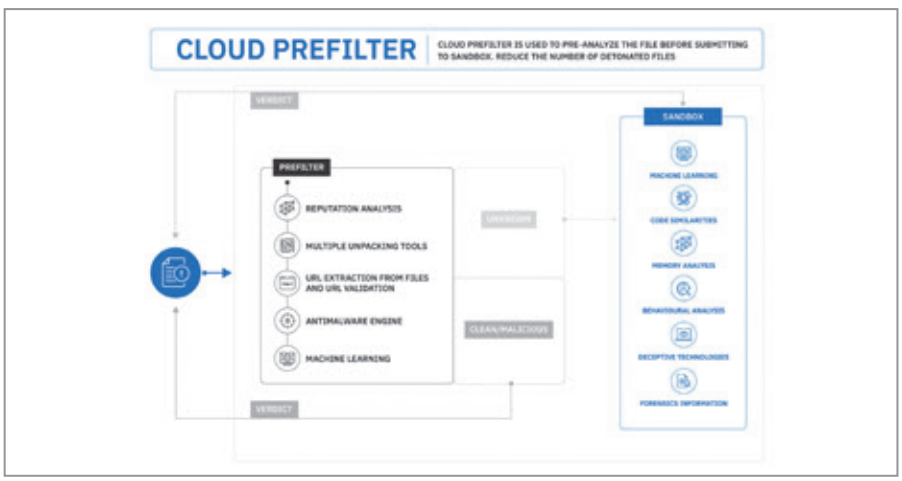
Dynamická analýza malwaru s Bitdefenderem

Všichni víme, že malware je trvalou hrozbou, kterou útočníci rádi zneužívají. Analýza malwaru je pak proces, jenž umožňuje týmům IT a bezpečnostním týmům pochopit účel a chování podezřelého souboru.



PAVEL ŠKORPIL

Z analýzy toho, jak malware vstupuje do systému a jak se v něm chová, získávají bezpečnostní týmy schopnost odhalovat a zmírňovat hrozby. Jen v loňském roce vzrostl počet kybernetických útoků v průměru o 50 %. A právě analýza malwaru to může pomoci změnit tím, že bude informovat bezpečnostní a IT specialisty o nových hrozbách, které se objevují na této scéně.

Existují tři základní způsoby analýzy malwaru: statická, dynamická a hybridní.

- Statická analýza malwaru zkoumá soubory bez spouštění kódu, takže se snadno používá a může pomoci identifikovat oblasti k prozkoumání. Navíc je použití této analýzy velmi rychlé.
- Oproti tomu dynamická analýza malwaru emuluje podezřelý kód a analyzuje pochybné akce. Toto je užitečné zejména při odhalování sofistikovaných útoků.
- A konečně je zde hybridní analýza malwaru, která spojuje výhody obou předchozích způsobů a identifikuje rizika kombinací statické i dynamické analýzy. Touto cestou se vydal i Bitdefender.

Dynamická analýza malwaru

Zatímco statická analýza závisí na zkoumání obsahu konkrétních souborů a programů z hlediska potenciálně škodlivého obsahu, dynamická analýza malwaru zahrnuje spuštění potenciálně škodlivého kódu a sledování jeho chování. Dynamická analýza malwaru je zvláště užitečná při odhalování hrozeb, které nebyly dříve zdokumentovány, jako jsou například hrozby nultého dne. Tyto hrozby obvykle nelze odhalit pomocí statické analýzy, a proto je dynamická analýza tak důležitá pro zajištění bezpečnosti organizací.

Sandboxing a detonace

Mezi technologie dynamické analýzy patří u Bitdefenderu „sandboxing“, což je technologie analýzy malwaru, která analyzuje soubory a adresy URL v zabezpečeném virtuálním prostředí. Kód se spouští v prostředí tzv. sandboxu, aby bezpečnostní analytici mohli zkoumat potenciální hrozby, aniž by vystavili provozní systém riziku nákazy.

Nejprve je ale Bitdefenderem provedena statická analýza obsahu, než je soubor vyfiltrován jako podezřelý. Následně je potenciálně nebezpečná část tohoto souboru (tedy ne celý soubor) přesunuta do cloudového sandboxu a tento podezřelý kód je spuštěn – neboli tzv. detonován. No a jelikož je dynamická analýza malwaru založena na chování detonovaného kódu, zaznamenává Bitdefender veškeré akce, které kód provádí, a to jak v prostředí sandboxu, tak mimo něj.

Kontext, záměr a chování jsou vlastnosti jedinečné pro různé typy malwaru. Ale vidět program, jak vykonává své funkce v reálném čase, to právě pomáhá bezpečnostním týmům pochopit, proti jakým hrozbám stojí a jak mohou své systémy před podobnými útoky chránit.

Výhody dynamické analýzy

Statická analýza je dobrá pro odhalení známých injektáží kódu, ale nedokáže poskytnout vhled do sofistikovanějších hrozeb malwaru. Dynamická analýza malwaru proto nabízí uživatelům Bitdefenderu hlubší přehled o potenciálních hrozbách malwaru než samotná statická analýza. Dynamická analýza také pomáhá týmům odhalit skutečnou povahu hrozeb a lze ji u Bitdefenderu s výhodou automatizovat pro rychlé odhalení nebezpečí. Ve chvíli, kdy se uvádí, že 62 % organizací má nedostatečný počet zaměstnanců v týmech kybernetické bezpečnosti, Bitdefender výrazně snižuje nároky na bezpečnostní tymy.

Výzvy a omezení

Přestože je dynamická analýza malwaru velmi užitečným nástrojem nejen pro analytiky SOC, pro lovce hrozeb a bezpečnostní týmy, je třeba si uvědomit, že útočníci jsou ale také obvykle velmi technicky zdatní. Vědí, co je to sandbox, a snaží se v cílovém systému sandbox detekovat. Vyzbrojeni těmito znalostmi mohou protivníci pracovat na oklamání technologie sandboxu například tím, že do malwaru umístí kód, který zůstane neaktivní, dokud nejsou splněny určité podmínky.

Závěr

Jak je vidět, sandboxing není jediným řešením malwarových hrozeb. Dynamická analýza malwaru za pomoci sandboxu je stále doporučována oproti samotné statické analýze, protože vede k vyšší míře detekce sofistikovaných malwarových hrozeb. Je však důležité, aby bezpečnostní týmy vzaly v úvahu, že se útočníci snaží o překonání této dynamické analýzy.

Nezapomeňte proto věnovat pozornost dalším vrstvám ochrany, jako je u Bitdefenderu například ochrana před bezsouborovými útoky, pokročilá ochrana před exploitacemi, technologie Bitdefender EDR a XDR nebo například velmi důležitý patch management.

Autor je Security Specialist