OPSWAT®

# Metadefender – sokmotoros, multi-scan AV/AM eszköz

## A kártékony kódok felismerésének problémája

A hagyományos AV/AM eszközök kártékony kód felismerése időablakhoz kötött: csak azokat a kártékony kódokat ismerik fel, amelyek szignatúrája és lenyomata megtalálható az eszköz szignatúra-adatbázisában. Egy-egy újabb malware vagy malware variáns megjelenése után napoknak kell eltelnie ahhoz, hogy az új szignatúra bekerüljön az AV/AM eszközök adatbázisába.

A legtöbb üzemeltető és biztonsági szakember találkozott már azzal, hogy az adott kártékony kódot a vállalat AV/AM eszköze nem ismeri fel, viszont egy másik AV/AM eszköz képes ellene védelmet nyújtani. A jelenség oka abban keresendő, hogy a különböző gyártók különböző reagálási idő mellett frissítik szignatúra adatbázisaikat. Amíg a vállalat AV/AM eszköze nem képes az új variáns vagy új malware felismerésére, a hálózat és a munkaállomások védtelenek az új variánsú kártékony kódokkal szemben.

## Metadefender – multi-scan eszköz, akár 30+ AV/AM motor együttes vizsgálata

Az OPSWAT Metadefender egy teljesen egyedülálló, akár 30+ AV/AM motorral dolgozó multi-scan eszköz, amely kiküszöböli az egyes AV/AM gyártók felismerési időablakából eredő kockázatokat azáltal, hogy több, akár 30+ motorral vizsgálja át a fájlokat és adatforgalmakat.

Az integrált AV/AM motorok szinkronban működnek, azaz minden egyes objektumot egyszerre vizsgálnak át, ezzel csökkentve az átvizsgálási időt. A motorok rendszeresen frissíthetőek.

## A határvédelem megerősítése, webes forgalom vizsgálata

A Metadefender multi-scan engine képes a webes forgalom együttes, akár több motorral történő vizsgálatára. A sokmotoros vizsgálat biztosítja, hogy a felhasználók munkaállomását ne érhessék el a kártékony tartalmak.

A Metadefender szerver ICAP modulja számos vállalati proxyszerverrel integrálható, amely képes ICAP-en keresztül átadni a forgalmat a Metadefender szervernek. A Metadefender szerver az ICAP-en érkező forgalmat megvizsgálja, és ha bármely motor kártékony kódot talál a forgalomban, az oldal elérését blokkolja.

## A határvédelem megerősítése, email forgalom vizsgálata

A Metadefender képes az e-mail forgalmat megvizsgálni és védelmet nyújtani a levelezőrendszeren keresztül érkező kártékony kódok ellen. A fejlett, többvektorú malware támadások legtöbbje kártékony emaileket használ a támadás megkezdéséhez, így kiemelten fontos a levelező szolgáltatás védelme.

A Metadefender Mail Agentet használ a levelezés vizsgálatához. Az agenten keresztül a Metadefender minden fogadott vagy küldött levelet és csatolmányt képes átvizsgálni, beleértve a felhasználók egymás közötti levelezését is, amely az Exchange szerveren belül marad. A kártékony tartalmú leveleket a Metadefender képes karanténba helyezni, és a karantén állapotáról napi riportban értesíteni az üzemeltetőket.

## Intranet és portal rendszer integráció, API

A Metadefender megszólítható a leggyakoribb publikus API-kkal. Rendelkezésre áll az ICAP mellett CLI, COM, REST, JAVA interfész is, amelyekhez JAVA, C, Python, PHP, Ruby nyelveken lehet kiegészítőket és illesztéseket írni.

Az API rendszeren keresztül a Metadefender hozzáilleszthető bármely vállalati Intranet/Extranet szolgáltatáshoz. Lehetőség van intranetes vagy külső portalfelületekhez illeszteni, és olyan funkciókat megvalósítani, ahol például a portal rendszerbe történő fájl- és dokumentumfeltöltések vagy akár letöltések (pl. szerződések, nyomtatványok, stb.) csak akkor történhetnek meg, ha a Metadefender előbb átvizsgálta a feltöltött fájlokat és adatokat.

## Minősített és SCADA hálózatok védelme

Az OPSWAT multi-scan engine lehetőséget biztosít speciális funkciók megvalósítására. A Metadefender Security Suite Kiosk kiegészítőjével lehetőség van olyan adatbeléptető terminál létrehozására, amely a felhasználó hitelesítése után a csatlakoztatott USB adathordozót és az átemelendő állományokat akár 30+ AV/AM motorral vizsgálja át, majd a tiszta fájlokat és adatokat automatikusan átemeli a védett hálózatba.

Zárt hálózatok (pl. minősített hálózatok, szigorúan védett hálózatok, ipari, SCADA-jellegű hálózatok stb.) esetében is lehetséges a Metadefender offline manuális frissítése. Ebben az esetben egy külön, nem a védett hálózatba telepített alkalmazás gondoskodik arról, hogy a frissítések letöltődjenek, majd az Update Tool egyetlen fájlba szervezi a frissítéseket, így akár USB adathordozón vagy adatdiódán keresztül átemelhető a védett hálózatba.

## Helyi „VirusTotal"

Sok esetben az üzemeltetőkhöz érkeznek olyan dokumentumok, kódok vagy más fájlok, amelyeket azért küldenek, mert gyanúsak és át kell vizsgálni őket. A legegyszerűbb ilyenkor az adott fájl feltöltése a VirusTotal-ra, noha azt kevesen tudják, hogy a VirusTotal elmenti a feltöltött állományokat, így bizalmas tartalmú dokumentumok vizsgálatára nem javasolt.

A Metadefender webes felülete kiváltja a nyilvános VirusTotalt. Az üzemeltetők vagy akár maguk a felhasználók is feltölthetik a gyanús fájlokat a Metadefender webes felületén. Itt a rendelkezésre álló AV/AM motorok átvizsgálják, és megmutatják, hogy az adott állomány fertőzött-e vagy tiszta.

## Remediációs funkció, kliens oldali ellenőrzés

A Metadefender rendelkezik hordozható (portable) kliensoldali ellenőrzést lehetővé tevő modullal. A Metadefender Client egy alacsony erőforrás-felhasználású alkalmazás, amely a munkaállomásokon történő ellenőrzést teszi lehetővé. A kliens a memória tartalmát, a boot szektort, a gépen található fájlokat és mappákat képes átvizsgáltatni a Metadefender szerverrel. A vizsgálat nem terheli túl a munkaállomást, mivel a kliens az állományokat átadja a szervernek, tehát nem a helyi munkaállomáson történik a vizsgálat.

A Metadefender Client támogatja a Windows, Linux és Mac OS X munkaállomásokat, és tökéletesen alkalmas malware fertőzések utáni remediációra, olyan bizonyító vizsgálatokra, amikor az üzemeltető biztos akar lenni abban, hogy nem maradt fertőző kód vagy kártevő az érintett munkaállomásokon.

## Riporting, logging

A Metadefender szerver nem csak a webes felületen feltöltött vagy a Client által elvégzett vizsgálatok eredményét logolja, de tárolja a webes vagy email adatforgalom-vizsgálatokat, illetve azok eredményét is. A logolás a Metadefender helyi adatbázisában történik, de a logok továbbíthatóak a külső SIEM vagy syslog eszközök felé is.

## AV/AM motorok és csomagok

A Metadefender multi-scan rendszer előre definiált motorokkal, csomagban érkezik. A Metadefender 1, 2, 4, 8, 12, 16 vagy 20 AV/AM motorral vásárolható meg, és bővíthető további motorokkal is.

## Rendszerkövetelmények

*Operációs rendszer: Windows 7-10 v. Windows Server 2008 R2-2012 R2*
*Server 1 motorral: min 4GB RAM, min 16GB HDD*
*Server 4 motorral: min 8GB RAM, min 32GB HDD*
*Server 8 motorral: min 8GB RAM, min 32GB HDD*
*Server 12 motorral: min 16GB RAM, min 32GB HDD*
*Server 16 motorral: min 16GB RAM, min 32GB HDD*
*Server 20 motorral: min 16GB RAM, min 32GB HDD*
*Client: Windows 7, Windows 8, Windows 10, Mac OS X, Linux*
*Windows Installer 4.5 vagy magasabb,*
*.NET 4.0*

## Az Ön viszonteladó partnere: