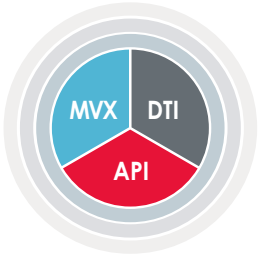
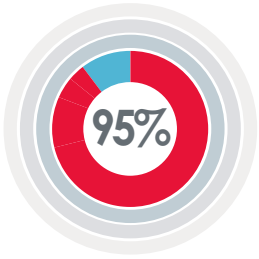
FireEye – valódi védelem a többcsatornás és újgenerációs támadások ellen



A FireEye újgenerációs támadások elleni védelmi rendszerének építőkövei

- **Multi-Vector Virtual Execution™ analízis**
- **Dynamic Threat Intelligence™ Cloud**
- **A meglévő biztonsági infrastruktúrával összekapcsoló API-k**



„A FireEye kipróbálása során a résztvevő cégek több mint 95%-a bukkant fertőzött kiszolgálóra az addig biztonságosnak hitt hálózataikon"
- a FireEye céges tesztelési eredményeiből.

Napjainkra a cybertámadások nagyon kifinomulttá váltak, és könnyedén áthatolnak az olyan hagyományos szignatúraalapú védelmeken, mint az újgenerációs tűzfalak, IPS rendszerek, vírusirtó programok és átjárók, megfertőzve a vállalati hálózatok túlnyomó többségét. A megszokott, szignatúraalapú védelmek kijátszása gyerekjáték lett, elegendő csak arra gondolni, hogy egy támadó kód szignatúráját milyen egyszerű a kódba beszúrt megjegyzésekkel eltorzítani és felismerhetetlenné tenni a szignatúra-felismerő motorok számára.

Az úgynevezett sandboxalapú, emulátorokat használó viselkedést vizsgáló felismerési eljárások sem garantálnak ma már megbízható védelmet, számtalan példa van arra, hogyan képes kijátszani egy támadó szándékú kód az emulált kliensközpontban történő vizsgálatokat.

A FireEye platform a megszokott védelmi rendszereket egészíti ki egy új típusú biztonsági megoldással, hogy védelmet nyújtson a modern, újgenerációs cybertámadások ellen. Az egyedülálló FireEye platform az egyetlen, amely olyan újgenerációs támadás elleni szerkezetet épít fel, amely valós időben, dinamikusan azonosítja és blokkolja a cybertámadásokat.

FireEye – újgenerációs védelem az újgenerációs támadások ellen

A FireEye platform lényegét egy szignatúramentes, teljesen virtualizált felismerő motor és egy támadási adatokat gyűjtő hálózat adja. A FireEye platformot több mint 40 országban, több mint 1000 ügyfél választotta, köztük a Fortune 100 listán szereplő vállalatok több mint egynegyede.

„A FireEye segítségével végre láthatóvá és megállíthatóvá váltak a hálózaton belüli és távmunkában dolgozó felhasználóinkat célzó támadások. Valódi előnye, hogy képesek lettünk pontosan meghatározni a tűzfalakon, URL gateway-eken, IPS rendszereken és vírusirtó programokon átjutó fenyegetéseket" - mondta a FireEye-ról a világ legtöbb profitot termelő vállalatait felsoroló Global 500 lista egyik pénzügyi szolgáltató cégének informatikai és adatbiztonsági igazgatója.

„A FireEye segítségével végre láthatóvá és megállíthatóvá váltak a hálózaton belüli és távmunkában dolgozó felhasználóinkat célzó támadások. Valódi előnye, hogy képesek lettünk pontosan meghatározni a tűzfalakon, URL gateway-eken, IPS rendszereken és vírusirtó programokon átjutó fenyegetéseket"

- mondta a FireEye-ról a világ legtöbb profitot termelő vállalatait felsoroló Global 500 lista egyik pénzügyi szolgáltató cégének informatikai és adatbiztonsági igazgatója.

FireEye – szignatúra- és sandboxmentes virtualizációs vizsgálatok

A virtualizáció a FireEye esetében nem sandboxot jelent. A FireEye eszköz egy saját virtualizációs architektúrában többféle felkészültségű (Windows XP SP1, SP2 stb.) kliens operációs rendszereket és rajta különböző alkalmazásokat (pl. JAVA, Flash player stb.) futtat. A gyanús kódok nem egy emulált sandbox környezetben, hanem virtualizált munkaállomásokon kerülnek lefuttatásra, ahol az elterjedt sandbox-megkerülési technológiák nem működnek. Mivel ténylegesen egy működő kliensen futnak le a kódok, a FireEye sokkal pontosabban ismeri fel a kódok tevékenységét, és olyan esetekben is felfedi a támadást, amelyekben a hagyományos vizsgálatok csődöt mondanak.

Védelem a polimorf és Zero-day fenyegetések ellen

A régi típusú, rosszindulatú programokat felváltó modern cybertámadások (polimorf kódok, 0-day támadások) célzott és folyamatos fenyegetést jelentenek. Az ilyen, többlépcsős támadások ártalmatlannak tűnnek minden olyan hagyományos és újgenerációs tűzfal, IPS rendszer, vírusirtó program és átjáró számára, amelyek szignatúrákra, gyanús viselkedések ismert mintáira és reputációanalízisre támaszkodnak.

A FireEye valódi virtualizációra alapuló vizsgálatai azonban nemcsak a már ismert támadási formákat ismerik fel sokkal pontosabban. Mivel a gyanús kódokat a FireEye eszköz a saját, virtualizált munkaállomásain futtatja le, a kódok tevékenységét és viselkedését a megfertőzött virtuális kliensen tudja megvizsgálni. Így olyan támadások és fertőzések is felismerhetők, amelyek dinamikusan módosítják kódjaikat és viselkedésüket, és természetesen azok a támadások is, amelyek ezeddig ismeretlenek voltak a hagyományos védelmi rendszerek számára.

Védelem napjaink újgenerációs cybertámadásai ellen

A FireEye platform kiegészíti a hagyományos és újgenerációs tűzfalak, IPS rendszerek, vírusirtó programok és átjárók által nyújtott védelmet, integrált, újgenerációs védelmet biztosít napjaink többvektorú webes, email-, fájl- és mobilalapú támadásai ellen.

A FireEye Multi-Vector Virtual Execution™ (MVX - többvektoros virtuális végrehajtás) alapja a saját, egyedi virtualizációs architektúra, amelyben több, eltérő felkészültségű kliens operációs rendszer fut. A gyanús kódokat a rendszer a valódi, de a FireEye platformban elszeparált klienseket futtatja le, megvizsgálja a kódok viselkedését és az esetleges fertőzések eredményeit (call back, állomány-módosulások stb.). Mivel a fertőzés valóban bekövetkezik a virtuális kliensen, a fertőzés után a FireEye sokkal pontosabban képes felismerni még a Zero-day eseményeket is.

A FireEye Dynamic Threat Intelligence™ (DTI - dinamikus támadási adatbázis) Cloud az MVX elemzéséből származó, anonim metaadatokat oszt meg a támadásokról, gyorsítva a támadások felismerését. A többvektoros támadásokról gyűjtött információk összehasonlításával a platform képes karanténba helyezni a zérónapi célzott adathalász emaileket, blokkolni az azokhoz kapcsolódó, az irányítás átvételére irányuló multi-protokoll kommunikációt.

Az **API architektúra** közös standardokra épülő malware metaadatoknak és FireEye API-knak köszönhetően integrációt és együttműködési lehetőséget biztosít más biztonsági megoldásokkal vagy a vállalat további védelmi rendszereivel.

Az Ön viszonteladó partnere:

FireEye™

biztributor
www.biztributor.com