BALASYS

ZORP MALWARE DETECTION

FORRADALMIAN ÚJ VÉDELEM A ROSSZINDULATÚ E-MAILEK ELLEN

„Az átlagos biztonsági eszközök a legtöbb esetben nem képesek az APT malware-ek észlelésére." – SANS Digital Forensics and Incident Response Blog

A hagyományos vírusvédelmi rendszerek tehetetlenek az APT-kkel szemben

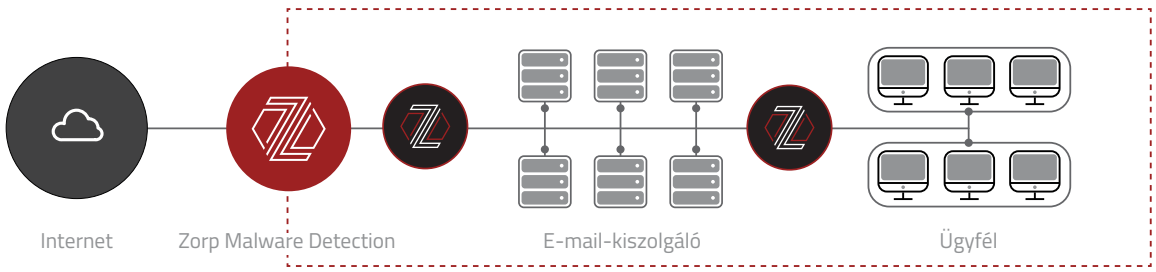
A hagyományos vírusvédelmi eszközök hatástalanok az APT (Advanced Persisten Threat) támadásokkal szemben. Az APT-k nem általános, hanem célzott támadások, amelyek egy kiszemelt célpontra, például egy speciális banki rendszerre vagy egy adott ország védelmi infrastruktúrájára irányulnak. Az APT-k célja egy konkrét feladat végrehajtása egy vagy több számítógépen kémkedés, üzemzavar vagy - legjellemzőbben - bizalmas üzleti adatok ellopása céljából.

Általában az APT malware-t alkalmazó támadók e-mail-csatolmányok segítségével törnek be a vállalati infrastruktúrába. A célba vett felhasználó által feltételezhetően használt szoftver (például az operációs rendszer, az MS Office, a PDF-olvasó vagy egy Java-verzió) „zero-day" sérülékenységeit igyekeznek kihasználni, mivel így a támadás sikere szinte garantálható. A hagyományos vírusok legtöbbjétől eltérően az APT-k nem idéznek elő olyan jelenségeket, amelyek alapján a számítógép fertőzöttségének gyanúja felmerül, így hónapokon vagy akár éveken keresztül is észrevétlenek maradhatnak...

Új megközelítés a valós idejű APT-védelem terén

A Zorp Malware Detection (ZMD) egy többrétegű malware elemző eszköz a rosszindulatú kódokkal fertőzött e-mailek és fájlok észlelésére. A hagyományos vírusok csatolmányokban történő felismerésén túl, a ZMD képes a célzott APT támadásokat is észlelni, mellyel komplex védelmet nyújt a potenciálisan káros e-mailek ellen. A többszintű észlelési rendszer lehetővé teszi több víruskereső motor integrálását az ismert rosszindulatú kódok kiszűrésére, valamint egy dinamikus, viselkedés-alapú elemzést az ismeretlen („zero-day") támadások azonosítására.

A ZMD nem egy univerzális vírusvédelmi megoldás. Sokkal inkább egy gondosan megtervezett támadási felület, amely hatékonyan alkalmazható az e-mail-forgalom védelmére. Olyan mélységű szűrési és észlelési képességet biztosít vállalata számára, amelyek a legtöbb vírusvédelmi eszközből hiányoznak. Emellett pedig a modern anti-sandbox technikák akadályozására is képes.



Zorp Malware Detection mintaarchitektúra

Komplex, többszintű e-mail-elemzés

Az e-mail csatolmányok több ellenőrzési fázison mennek keresztül, amelyek a fájlok tartalmát és viselkedését különböző szempontból elemzik. A statikus elemzés az első, amely több mint 20 külső vírusmotort és egyéb malware-adatbázist használ párhuzamosan, mely kiemelkedő találati arányt nyújt. Ha nem található fertőzés, a ZMD a fájlt dinamikus elemzésnek veti alá mélyebb ellenőrzés céljából. Ebben a fázisban a ZMD kontextuális elemzéseket végez több eszközzel, mely során a csatolmány digitális lábnyomait és annak a (szimulált) környezetre gyakorolt hatásait vizsgálja.

Megosztott-mappák elemzése

A Zorp Malware Detection (ZMD) folyamatosan felügyeli a megosztott Windows mappákat, észleli az új fájlokat, lefuttatja az elemzést rajtuk, és feltölti az ellenőrzött fájlokat egy külön mappába. A ZMD riportot is csatol az elemzés eredményéről. A fertőzött fájlokat karanténba helyezi.

APT támadások valós idejű megelőzése

A Zorp Malware Detection legerősebb fegyvere a támadókkal szemben egy virtuális sandbox technológia, amely futási környezetet szimulál az e-mail mellékletek viselkedésének vizsgálatához. Jelenleg ez a technológia biztosítja a legmagasabb szintű védelmet az olyan rosszindulatú programok ellen, amelyek az MS Office és az Adobe sebezhetőségeit használják ki.

Testre szabható sandboxing és ellenőrzés

Az igényei alapján segítünk Önnek egy virtuális vagy fizikai sandbox környezet felállításában. Az APT támadások gyakran egy adott felhasználót céloznak meg, így akár olyan egyedi elemző klienst is készíthetünk, amely tökéletes mása a felhasználó futási környezetének, beleértve az operációs rendszer, az MS Office, a szervizcsomagok, a PDF olvasó és a Java verziókat. Az elemzés eredménye alapján a ZMD adminisztrátor egyedi viselkedési mintákat definiálhat, új szintre emelve ezzel az email-ek feletti kontrollt.

Kiemelkedő teljesítmény

A Zorp Malware Detection napi mintegy 20 000 e-mail csatolmányt képes elemezni. A megoldás horizontálisan skálázható - vállalati környezetben tetszőleges számú ZMD node-ot állíthat fel, amelyeket egy külső terheléselosztó kezel. A dinamikus elemzés esetében az elemzés ideje csatolmányonként 2–9 perc.

ZORP
MALWARE DETECTION

A Zorp Malware Detection előnyei

- Forradalmi megközelítés a malware-észlelés terén
- Viselkedés-alapú védelem a célzott támadások ellen
- Nagy hatékonyságú, addicionális biztonsági réteg
- Rugalmas, tapasztalt bevezető csapat
- 7/24 órás támogatás (opcionális)
- Magyar fejlesztés – „Tiszta" kódbázis
- Kiemelkedő ár-érték arány

BŐVEBB INFORMÁCIÓK

A Zorp Malware Detection honlapja | Próbaverzió igénylése | Árajánlat kérése

BALASYS