TRUST IN GERMAN SICHERHEIT

G DATA BEAST

A hagyományos vírusvédelem korlátainak átlépése

G DATA CyberDefense AG | V-Detect Antivírus Kft. - https://virusirto.hu

Az interneten terjedő, úgynevezett vadon élő kártevők egyre kifinomultabbak, így a felismerésük egyre nehezebb feladat, ha csupán a hagyományos, szignatúraalapú felismerési technológiákra hagyatkozunk.

Az első korlát: utólagos felismerés

A szignatúraalapú észlelés definíció szerint reaktív módszer. Ennek a hagyományos módszernek a lényege, hogy a vírusirtókat gyártó cégek mintát szereznek az új kártevőkből, majd a minták elemzése után elkészítik azok ellenszerét, azaz megtanítják az általuk gyártott vírusirtót a felismerésükre. Ez azt jelenti, hogy csak azután készíthető szignatúra egy kártevőhöz vagy annak családjához, ha már a laboratórium azt rosszindulatúnak minősítette.

Mára a kiberbűnözők megtörték ezt a módszert azzal, hogy az általuk készített kártevőkből rendkívül gyorsan adnak ki új változatokat, úgynevezett mutációkat.

A második korlát: a kártevők egyedisége

A kiberbűnözés milliárd dolláros iparággá vált. A hagyományos vállalkozásokhoz hasonlóan a kiberbűnözők is automatizálási eszközök használatával növelik hatékonyságukat. Egyes kártevőkészítők például automatizált szolgáltatásokat használnak annak ellenőrzésére, hogy a különböző vírusvédelmek észlelik-e a kártevőket. Az észlelés regisztrálása után azonnal eltávolítják az azonosított mintát, vagy automatikusan módosítják programjaikat az észlelés elkerülése érdekében.

Emellett erős titkosítást és úgynevezett csomagolókat alkalmaznak a mintáikhoz, hogy elfedjék a rosszindulatú központi komponenseket. Egyes rosszindulatú programok szerzői akár néhány percenként tesznek közzé új kártevőmintákat, mások pedig minden egyes megtámadott célponthoz teljesen egyedi mintát generálnak (szerveroldali polimorfia).

Nyilvánvaló, hogy amikor a rosszindulatú fájlok ennyire egyediek, akkor nehéz olyan rosszindulatú mintákat találni, amelyek segítségével hagyományos aláírást lehet generálni, amely képes azonosítani a kártevők egész családját. Még ha vannak is olyan minták, amelyekkel aláírást lehet létrehozni, ez az erőfeszítés a gyakorlatban értéktelen lehet.

A harmadik korlát: a backend-elemzés elkerülése

A következő probléma, hogy a rosszindulatú fájlok azonosítása gyakran a biztonsági gyártók elemzési hátterére támaszkodik. Minden potenciálisan rosszindulatú mintát, amely a védelmi megoldásokat gyártók kezeibe kerül, alaposan kielemeznek, például sandbox- (homokozó-) rendszerekben, amelyek végrehajtják a mintákat, és megpróbálják azonosítani a rosszindulatú műveleteket. Sajnos a rosszindulatú programok gyakran úgy vannak kialakítva, hogy tisztában legyenek a környezetükkel, és észleljék, ha elemzés alatt állnak. Lehet, hogy úgy leleplezik valódi céljukat, hogy egy bizonyos időpontban, egy bizonyos helyen, egy bizonyos ideig tartó futás után mutatnak rosszindulatú viselkedést, vagy akár olyan felhasználói interakció felismerése után, amely általában nincs jelen egy homokozórendszerben.

Ezen problémák miatt a hagyományos felderítési módszerek mellett arra is szükség van, hogy a rosszindulatú viselkedést ott is észleljük, ahol az valóban megtörténik: az érintett rendszeren.

A korábbi megoldás: magatartásalapú védelem

A biztonsági gyártók ezért olyan észlelési technológiákat vezettek be, amelyek elemzik a folyamatok viselkedését a rendszeren annak megállapítására, hogy az rosszindulatú vagy jóindulatú-e. A hardver erőforrásainak kímélése érdekében az ilyen elemzés általában a különösen gyanús rendszerrészekre összpontosít, mint például a fájlrendszer, a rendszerleíró adatbázis vagy az automatikus indítási mappa. Ez lehetővé teszi a biztonsági szállítók számára, hogy felismerjék a még teljesen ismeretlen kártevőket.

A legtöbb ilyen védelmi megoldás megpróbálja a fenyegető magatartást értékekké alakítani, hogy meghatározza a „rosszaság” fokát. Matematikailag azonban nem lehet elkerülni a pontosság elvesztését, ha ezen értékek közül sokat összesítenek egy összpontszámba. Még a gépi tanulás esetén is előfordul, hogy ez a módszer bizonyos mértékű bizonytalansághoz, majd bizonyos szintű téves megítéléshez vezet.

A legtöbb otthoni felhasználót ez nem érinti hátrányosan. A vállalkozások azonban gyakran speciális szoftverekkel dolgoznak, és ezeket sokszor ártalmatlan, de másokhoz képest szokatlan

módon használják. Ha egy viselkedéselemző eszköz küszöbértéke túl magasra van állítva, az blokkolni fogja ezeket a folyamatokat, ha pedig túl alacsonyra, előfordulhat, hogy nem észleli a kártevőt.

A való világban a biztonsági megoldások gyártói sok esetben szeretnék úgy elkerülni az észlelési hibákat, hogy megkérik a felhasználókat, engedélyezzék (vagy tiltsák) a folyamatok végrehajtását. Ha ez a figyelmeztetés túl sűrűn fordul elő, a felhasználók vagy kikapcsolják a technológiát, vagy figyelmen kívül hagyják a figyelmeztetéseket. Akárhogy is, a fertőzések kockázata nő.

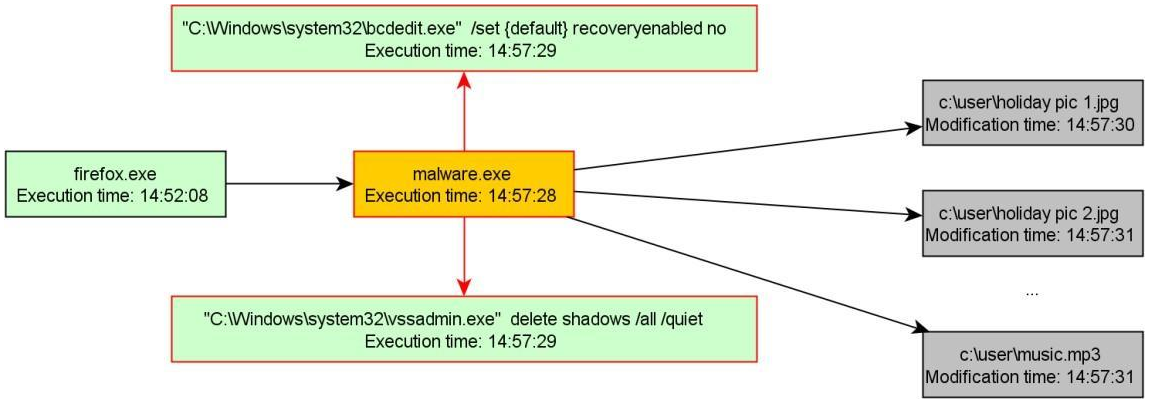
Az igazi megoldás: G DATA BEAST

A BEAST a G DATA által kifejlesztett viselkedésalapú észlelési technológia, amely figyeli a viselkedést, és minden megfigyelt műveletet eltárol egy helyi, könnyű gráfadatbázisban. A BEAST nem magának a rosszindulatú programnak az azonosítására támaszkodik, hanem az általános rosszindulatú viselkedés megfigyelésére. Ez különösen hasznos a ritka rosszindulatú programok és a sok mutációt tartalmazó kártevőcsaládok ellen.

Hogyan működik a BEAST: gráfalapú szabályfigyelés

Egy védett rendszeren a BEAST figyeli a viselkedést, és eltárol minden műveletet. A műveletek közé tartozik a fájlrendszerhez, a rendszerleíró adatbázishoz, a hálózati kapcsolatokhoz és a folyamatok közötti kommunikációhoz való hozzáférés. Amikor valamit hozzáadunk a gráfadatbázishoz, a gráf rosszindulatú viselkedési mintákat keres.

A következő grafikon használható az ilyen szabályalapú egyeztetés szemléltetésére:



Ebben a példában a felhasználót becsapta egy webhely, hogy letöltse és végrehajtsa a rosszindulatú „malware.exe” fájlt az internetről a Firefox böngészőben. Valójában ebben az esetben zsarolóvírus-fertőzésről van szó. A zsarolóvírus titkosítja a felhasználó fájljait, majd megkéri a felhasználót, hogy fizessen bizonyos összeget a fájlok visszafejtéséért.

A rosszindulatú folyamat itt azonnal elindítja a BCDEdit segédprogramot, hogy letiltsa a Windows indítási javítási funkcióját. Ezt követően elindítja a VSSADMIN rendszereszköz egy példányát az úgynevezett árnyékmásolatok törlésére, amelyek segítségével vissza lehetne állítani a véletlenül felülírt fájlokat. Ezután elkezdi több fájl titkosítását a C:\„user” könyvtárban.

Mivel a két fent említett rendszereszköz elindítása a zsarolóprogramok tipikus előkészítése a fájlok titkosítása előtt, azért, hogy megakadályozzák a felhasználót a rendszer helyreállításában, a (pirossal kiemelt) viselkedés egyértelműen rosszindulatúnak tekinthető. Ezért a „malware.exe” folyamat leállításra kerül, és a bináris fájlt karanténba rakjuk. Mivel a „vssadmin.exe” és a „bcdedit.exe” állományok jóindulatú rendszereszközök, amelyekkel a zsarolóvírus csak visszaél, ezek a rendszeren maradnak.

Új lehetőség: visszamenőleges eltávolítás

A G DATA automatizált háttérrendszerekkel és manuális elemzési folyamatokkal mindennap számos kompromisszummutatót (Indicator of Compromise, IOC) azonosít. Az IOC lehet egy Command&Control-Server (C&C), amelyet egy botnet működtetésére használnak, vagy egy bizonyos fájl, amelyet rosszindulatúként azonosítottak.

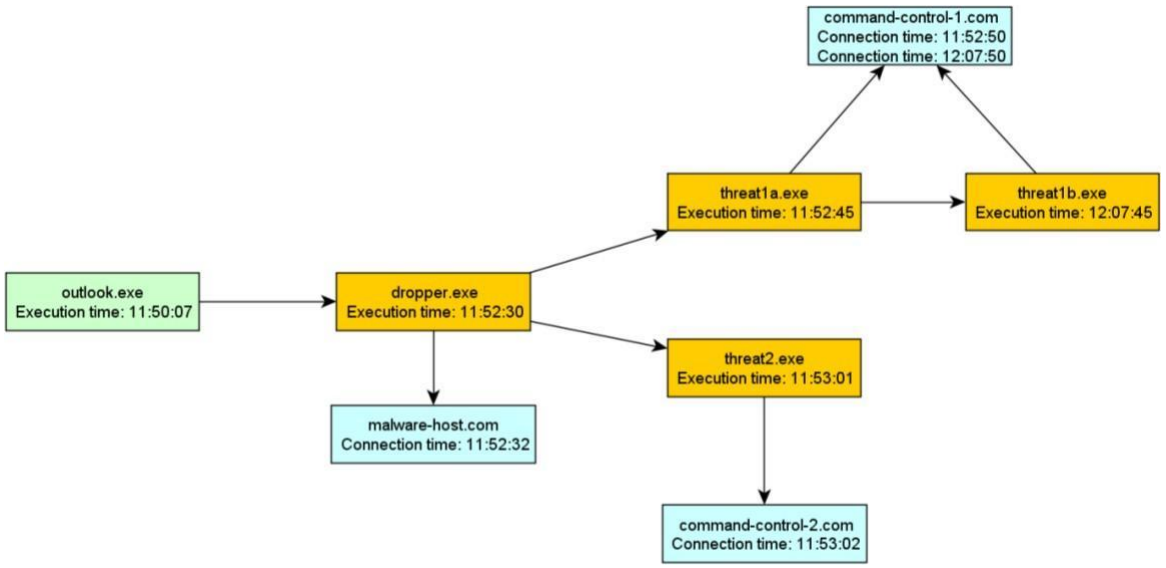
A hagyományos végpontbiztonsági szoftverekben a műveleteket csak akkor hasonlítják össze az IOC-listákkal, amikor a művelet megtörténik. Például egy fájl végrehajtása előtt összehasonlításra kerül az ismert rosszindulatú fájlok listájával. Vagy ha egy folyamat csatlakozik egy gazdagéphez, a gazdagépet a rendszer az ismert C&C-k listájához hasonlítja. Ha a gazdagépet rosszindulatúként azonosítják, akkor az egész folyamatot rosszindulatúként észleli.

A fő probléma azonban az, hogy a biztonsági gyártó IOC azonosítási folyamatai ismét reaktívak – azután indulnak el, hogy a gyártók elkezdik elemezni a fenyegetést, ami nyilvánvalóan csak a

fenyegetés tényleges megjelenése után történhet meg. Még akkor is, ha ez automatizált, és nagyon rövid időn belül végrehajtódik, az időeltolódás továbbra is jelentős a rosszindulatú programok megjelenése és a reakció között. Egyszerűen fogalmazva: a biztonsági gyártók gyakran túl későn tudnak cselekedni, ha hagyományos módszerekre támaszkodnak.

A BEAST védelmi modulban a műveletek (viselkedés) egy helyi gráfadatbázisban kerülnek tárolásra. Ezért ebben az adatbázisban mindent össze lehet hasonlítani a G DATA által azonosított IOC-kkal, még azok létrejötte után is. **És mivel a grafikon-adatbázis minden, a IOC-hez kapcsolódó műveletet is tartalmaz, ezek a műveletek is visszaállíthatók, ami hatékonyan lehetővé teszi a rosszindulatú programok visszamenőleges eltávolítását.**

Ez különösen fontos, ha egy rendszert feltörtek, de még nem indítottak el olyan rosszindulatú műveleteket, amelyek kiváltották volna a hagyományos magatartásalapú észlelési modul riasztását. Ennek szemléltetésére képzeljük el a következő egyszerűsített viselkedési grafikont:



A példában először az Outlook levelezőprogramban egy fertőzött melléklet nyílik meg. Ezért az „outlook.exe” folyamat létrehozza és végrehajtja a „dropper.exe” nevű fájlt. Az új folyamat ezután csatlakozik a „malware-host.com” webhelyhez, hogy letöltse és végrehajtsa a további rosszindulatú bináris fájlokat („threat1a.exe”, „threat2.exe”). Mindkettő csatlakozik a megfelelő C&C szerveréhez („command-control-1.com”, „command-control-2.com”). Körülbelül 15 perc elteltével a „threat1a.exe” parancsot kap a bináris fájl frissítésére a „threat1b.exe” fájlra, amely ezt követően szintén kapcsolatot létesít ugyanahhoz a C&C szerverhez.

Ha például a G DATA a „command-control-2.com” szervert vagy a „dropper.exe” bináris fájlt IOC-ként azonosítja, a BEAST – még órákkal a fertőzés után is – egyszerűen végigsétálhat a gráfon, megkeresve és eltávolítva minden, a fertőzéshez kapcsolódó állományt.

Két megjegyzés: először is, a Windows rendszerleíró adatbázisában történt bármilyen változás rögzítésre kerül, és visszaforgatható; másodszor, mivel az outlook.exe egy ismert jóindulatú végrehajtható fájl, így nem kerül eltávolításra.

Mi a különbség a mostani magatartásalapú védelemhez képest?

A meglévő, évek óta elérhető magatartásalapú védelem alapvetően minden műveletet észlel, amelyet egy folyamat hajt végre. Minden egyes művelethez egy adott numerikus „rosszaság” értéket rendel. Ezután összeadja az összes értéket, és ha az egy bizonyos küszöbértéket túllép, a folyamatot rosszindulatúnak minősíti.

A magatartásalapú védelem (behavior blocker) tehát alapvetően folyamatközpontú, míg a BEAST az egész rendszerről áttekintést kap. Továbbá, mivel a magatartásalapú védelem csak számszerűen összesíti a műveletek „rosszaság” értékét, nem lehetséges a műveletek bizonyos kombinációit rosszindulatúként észlelni. Ez megnehezíti a rosszindulatú viselkedésminták konkrét észlelését.

Amikor egy művelethez új vagy magasabb „rosszaság” értéket rendelnek a magatartásalapú védelemben, az hamis pozitív riasztásokat válthat ki. Emiatt korábban nehézkessé vált az új fenyegetésekre való gyors reagálás. És még ha óvatosak és alaposak vagyunk is, valahányszor egy művelethez új vagy magasabb „rosszaság” értéket rendelünk egy új fenyegetés észlelése érdekében, olyankor óriási a kockázata annak, hogy hamis pozitív riasztásokat váltunk ki.

Ezzel szemben a BEAST esetében az észlelések a rosszindulatú tevékenységek nagyon specifikus kombinációin alapulnak. Ezért könnyebb új szabályokat felvenni, miközben a védelem általánosságban kevésbé lesz hajlamos a hamis pozitív riasztásokra.

Ezenkívül az IOC-k retrospektív összehasonlítása és az utólagos eltávolítás csak a BEAST technológiánál lehetséges.

Miért van szükségünk BEAST-re, ha már van G DATA DeepRay?

A DeepRay védelmi technológiánk egy másik védelmi réteg, amelynek erőssége abban rejlik, hogy képes átnézni a csomagolókat, lehetővé téve számunkra a rosszindulatú programmagok (központi komponensek) azonosítását. A rosszindulatú programmagok kezdeti azonosítása azonban manuális folyamat. A legelterjedtebb kártevőcsaládok esetében ez egy kezelhető feladat.

Ennek ellenére a BEAST még ezeknél is segít kitölteni a DeepRay észleléséig tartó időhézagot abban az esetben, ha a rosszindulatú program a magjában megváltozik. De a legelterjedtebb kártevőcsaládok mellett van egy nagy halom rosszindulatú programcsalád is, amelyek egyetlen családként ugyan nem túl elterjedtek, de egymással összeadva hatalmas mennyiségű fertőzést okoznak. És ha kisszámú terjedésnek az az oka, hogy ezeket a családokat célzott támadásokhoz használják fel, akkor azok különösen veszélyesek.

Mivel a BEAST nem egy adott rosszindulatú programmag azonosítására támaszkodik, hanem a rosszindulatú viselkedés általános megfigyelésére, segít enyhíteni ezeket a fenyegetéseket, és így további biztonsági réteget ad.