Illetéktelen hozzáférés után

speciális fenyegetések kezelése

Új kihívás van keletkezőben

A végpontok biztonsága egy kulcsfontosságú tényező a tárgyalóterem szintjén. A C szintű informatikusok és biztonsági vezetők 71%-a még 2015 novemberében is a végpontokat tartotta a leginkább sebezhetőnek[1]. Ez a probléma jelenleg is egyre súlyosabbá válik, mivel egyre gyakoribbá válnak a szellemi tulajdont és nagy jelentőségű üzleti információkat megcélzó, kifinomult támadások. A hagyományos védekezés hatástalan a jelenséggel szemben, és a biztonsági vezetők 70%-a nem bízik a meglévő biztonsági rendszerekben. Új megközelítésre van tehát szükség.

Miközben a kártevőirtó szoftvereket továbbra is a tömegével gyártott, kiberbűnözéssel kapcsolatos kártékony szoftverekre tervezik, egy újfajta, sokkal kifinomultabb, célzott fenyegetés jelent meg. A Stuxnethez és a Reginhez hasonló, állami fejlesztésű kiberfegyverek nyilvánosságra kerülése óta alig múlik el nap anélkül, hogy egy újabb jelentős vállalatot vagy kormányzati hálózatot támadás érne. Csak 2015-ben 2 122 illetéktelen hozzáférést igazoltak vissza hiteles forrásból, ami az egyik forrás szerint éves viszonylatban 40%-os növekedést jelent a nagyvállalatok ellen irányuló célzott támadások terén. Az államilag támogatott és politikailag motivált hackercsoportok, mint a Strontium, jellemzően a vállalati és kormányzati szellemi tulajdon, valamint az ügyfélnyilvántartások ellen indítanak támadásokat.

Ez a rohamos emelkedés részben annak köszönhető, hogy a kártevőirtó és hibajavító csomagok nehezen tudják megállítani ezeket a támadásokat. Az elszánt támadók könnyűszerrel megkerülik a kártékony szoftverek ellen kifejlesztett védelmet azzal a megoldással, hogy egyáltalán nem használnak ilyen szoftvereket. Ez a helyzet az esetek nagyjából 60%-ában[2], amikor az operációs rendszer (OS) jogszerű kezelésével, illetve tolltesztelő eszközök használatával érik el céljukat, egyszerű pszichológiai manipulációt alkalmazva a felhasználók megtévesztésére, akik így hozzáférést és jogosultságokat biztosítanak számukra. Egy másik ilyen módszer a nulladik napi biztonsági hibák kihasználása, melyek segítségével a támadók az operációs rendszeren és az alkalmazásokon keresztül észrevétlenül hozzáférhetnek a hálózathoz. A statisztikák ijesztőek: 2014-ben a legjelentősebb nulladik napi biztonsági hibákat összesen 295 napon keresztül használták ki a támadók, mielőtt sikerült a hibákat kijavítani[3]. Miközben a támadóknak mindössze néhány percébe került a hálózathoz hozzáférni, a biztonsági csapatoknak átlagban 221 napig kellett dolgozniuk ahhoz, hogy egyáltalán felfedezzék a hozzáférést. Egy felmérés alapján a vezetők jelentős többsége, 81%-a nem a kártevőirtó szoftverekre alapozza a speciális támadások elleni védelmet[4].

---

[1] promisec Blog: Endpoint Security Infographic

[2] Verizon jelentés: Verizon 2016 Data Breach Investigations Report

[3] Symantec jelentés: 2016 Symantec Internet Security Threat Report

[4] promisec Blog: Endpoint Security Infographic

Ahogy a támadások száma évről évre növekszik, egyre több kereskedelmi vállalat fedezi fel, hogy illetéktelen személyek férnek hozzá az adataikhoz. Míg korábban a támadók leginkább a nagy horderejű célpontokat támadták, manapság a kis és közepes méretű kereskedelmi szereplők is változatos támadásoknak vannak kitéve, a politikai szabotázstól az ipari kémkedésig.

Az illetéktelen hozzáférés utáni teendők

A kártevőirtó végpontmegoldások, mint például a Windows Defender az adatforgalom őreként az illetéktelen hozzáférés előtti megközelítésre koncentrálnak, kivizsgálva a beérkező fájlokat és a memóriát kártékony tartalmakat illetően, valós időben kivédve a támadásokat. Ugyanakkor, ahogy a fentiek is mutatják, ezek az egyébként igen fejlett megoldások nem biztosítanak száz százalékos védelmet, így a jelentős anyagi háttérrel és kifinomult szoftverekkel rendelkező támadók sikeresen használhatják ki a nulladik napi biztonsági hibákat, a pszichológiai manipulációt és az egyébként nem kártékony eszközöket a hozzáférés, jogosultságok és irányítás megszerzésére. Ennek következtében új megközelítésre van szükség az illetéktelen hozzáférést követő szakaszban a korábbi szakaszokban alkalmazott biztonsági megoldások kiegészítésére.

Az illetéktelen hozzáférés előtti szakasztól eltérően az illetéktelen hozzáférés utáni megoldások azt feltételezik, hogy a hálózatba már betörtek, ezért fedélzeti adatrögzítőként és helyszínelőként működnek. A biztonsági eseményeket figyelik a végponton, és a nagyméretű összefüggés- és anomáliaészlelési algoritmusok előnyeit kihasználva riasztást küldenek a folyamatban lévő támadásokról. Az illetéktelen hozzáférés utáni védelem azt használja ki, hogy a behatolás után a támadónak több különböző műveletet kell végrehajtania, mint amilyen a hálózat felderítése, az elrejtőzés, az értékes erőforrások keresése és az információk kinyerése. Az illetéktelen hozzáférés utáni védelem megfelelő információkat és eszközöket kínál a biztonsági csapatoknak az egyébként észlelhetetlen támadások beazonosítására, kivizsgálására és elhárítására. Ezzel a módszerrel bezárul az illetéktelen hozzáférés előtti védelmet biztosító kártevőirtó szoftverekkel és egyéb megelőzési eszközökkel kezdődő kör, mivel a megoldás beviszi a rendszerbe a korábban nem észlelt jelzéseket és mintákat. Ennek következtében kiválóan kiegészíti az illetéktelen hozzáférést megelőző biztonsági rendszert.

Ez az új illetéktelen hozzáférés utáni megközelítés globális elismertséget szerzett, és egy teljes új szegmens épült rá a biztonsági piacon belül, melyet a Gartner Endpoint Detection and Response (EDR – végpontészlelés és -elhárítás), az IDC

[5] Gartner Report: Market Guide for Endpoint Detection and Response Solutions

[6] IDC-tanulmány: Worldwide Specialized Threat Analysis and Protection Market Shares, 2014: Rapidly Evolving Security Defenses

Specialized Threat Analysis and Protection (STAP – speciális fenyegetéselemzés és védelem) néven említ. A vállalkozásoknak ajánlatos a végpontvédelmi és fenyegetés-megelőzési csomagjaikat kiegészíteni fejlettebb, nem aláírásalapú fenyegetésekre koncentráló észlelési és elhárítási technológiákkal[5], melyek képesek a hagyományos biztonsági technológiákkal történő észlelést kikerülni képes fenyegetések elemzésére[6].

Az előrejelzések szerint 2019-re 3 milliárd USD értékre bővülő, 27,6%-os összetett éves növekedési ütemmel rendelkező biztonsági piacra folyamatosan érkeznek az új szereplők, köztük olyan nagy nevekkel, mint a Symantec és a Dell, de olyan sikeres új vállalkozásokkal is, mint a FireEye, Bit9 és CrowdStrike, mely utóbbi 2015-ben több mint 100 millió USD támogatást kapott a Google-től[7]. A kérdésekre válaszoló C szintű informatikai vezetők 82%-a szerint mélyebb végpontelemzési készségekre volna szükség az illetéktelen hozzáférések észleléséhez és elhárításához[8].

Az illetéktelen hozzáférés utáni Windows-megoldás

A Windows 10 évfordulós frissítésével a Windows saját megoldást kínál az illetéktelen hozzáférés utáni védelemre Windows Defender Advanced Threat Protection (ATP) néven, mely a Windows Defender, SmartScreen és az operációs rendszer biztonságát fokozó változatos szolgáltatások egyesítésével létrehozott végpontbiztonsági rendszert egészíti ki. A kifejezetten speciális támadások észlelésére és elhárítására kifejlesztett új szolgáltatás a Windows 10 rendszerbe integrált mély viselkedésérzékelő és a háttérben elhelyezkedő, hatékony biztonsági elemzőfelhő előnyeit kombinálva lehetővé teszi a vállalkozásoknak a hálózataik ellen irányuló, célzott és kifinomult támadások észlelését, kivizsgálását és elhárítását.

A Windows Defender ATP a következőket kínálja a vállalkozásoknak:

- Speciális támadásészlelés – viselkedésalapú és anomáliaelemzés használata riasztások kidolgozásához az összes vállalati végponton keresztül. A hasonló szolgáltatások közül a Microsoft hatékony biztonsági elemzési és veszélyfelismerő képességeinek köszönhetően kiemelkedő védelmi rendszer a Windows Defender, a Bing, az IE és az Office 365 előnyeit egyesítve világszerte több mint egymilliárd végpontnak biztosít láthatóságot.

- Kivizsgálás és válasz – egy biztonsági műveleti konzol, amely könnyen használható megoldást kínál a vállalkozások számára a riasztások kivizsgálására, a támadásra utaló, hálózaton belüli jelzések aktív felderítésére, az egyes gépek kriminalisztikai vizsgálatára, a támadók nyomon követésére a hálózatba bekötött gépeken keresztül, valamint részletes, szervezeti szintű fájlhelyigény-felmérés készítésére.

---

[7] Financial Times: http://www.ft.com/cms/s/0/dd7ba860-2965-11e5-8613-e7aedbb7bdb7.html

[8] promisec Blog: Endpoint Security Infographic

• Veszélyfelismerés – belső és külső jelentések és jelzések ismert támadókról és jelentős támadásokról (például a Strontium), amelyeket egy belső, szakértőkből álló biztonsági csapat (biztonsági kutatólaboratórium) hagy jóvá, és külső hozzájárulásokkal bővít.

1. ábra: A Windows Defender ATP a Windows 10 illetéktelen hozzáférés előtti és utáni biztonsági rendszerében

• Integrált megoldás – A Windows Defender ATP integrálja a Windows Defender szolgáltatásból érkező jelzéseket, felfedve a korábban nem észlelt fenyegetéseket, és hozzájárulva annak megakadályozásához, hogy a probléma szétterjedjen a teljes vállalati hálózaton.

Windows 10 védelmi rendszer

Az egyre kifinomultabbá váló, célzott támadások növekvő fenyegetése ellen kulcsfontosságú feladat továbbfejleszteni az illetéktelen hozzáférés utáni stratégiát, az egyre összetettebbé váló hálózati ökoszisztéma megfelelő védelme érdekében. A Windows Defender ATP átfogó illetéktelen hozzáférés utáni megoldást kínál, amellyel a biztonsági csapatok megbízható riasztásokat építhetnek ki azokra az esetekre, amikor az illetéktelen hozzáférés előtti védelem csődöt mond. A Windows 10 végpontbiztonsági rendszere a végpontok teljes spektrumát lefedi, az eszközvédelemtől a hozzáférés-észlelésig, megbízhatóbb védelmet kínálva a vállalati hálózatoknak a kifinomult, speciális támadások ellen.