Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- Áttekintés
- Javítócsomag
- Mentések
- Adathalászat

A WannaCry tanulságai

Áttekintés

Az utóbbi időszakban borzasztó hírek láttak napvilágot egy új „WannaCry” nevű kibertámadásról. Több mint 200.000 számítógépet fertőzött meg a „WannaCry”, zárolva a különféle intézmények, beleértve az Egyesült Királyság kórházainak az adatait. Számos oka van, amiért ez a támadás ilyen jelentős figyelmet kapott. Elsőként az, hogy a Windows számítógépek egy ismert sérülékenységét támadva terjed gyorsan számítógépről számítógépre. Másodszor, a támadás egy zsarolóvírusnak nevezett kártékony kód volt, mely azt jelenti, hogy ha egyszer megfertőzi a gépünket, akkor minden fájlunkat titkosítja, ezzel elérhetetlenné téve számunkra a saját adatainkat. Az adataink visszaállítása a biztonsági mentésekből lehetséges, vagy úgy, ha fizetünk a zsarolóknak 300$ váltságdíjat, az adataink dekódolásáért. A harmadik és legfontosabb, hogy ennek a támadásnak soha nem szabadott volna megtörténnie. A Windows számítógépeknek azon gyengesége, amit kihasznált a „WannaCry”, már ismert volt a Microsoft számára, aki hónapokkal ezelőtt ki is adott javítást a sérülékenységre vonatkozóan. Számos szervezet nem telepítette a javítást, vagy még mindig olyan operációs rendszert használ, mint például a Windows XP, ami már olyan régi, hogy nem érhetőek el hozzá javítócsomagok. Mutatunk 3 egyszerű lépést, aminek következményeként biztosak lehetünk benne, hogy az ilyen támadások, mint a „WannaCry” nem fertőzik meg az eszközeinket.

A szerzőről

Dr. Johannes Ullrich a SANS Technológiai Intézet kutatási dékánja és aDShield.org alapítója. Ő felelős a **SANS Internet Storm** nevű Központért, mely az aktuális kiberbiztonsági fenyegetéseket figyeli. Web alkalmazás Biztonságot (**DEV522**), Illetéktelen behatolást (**SEC503**) valamint and IPv6-t (**SEC546**) oktat.

Javítócsomag

Legelőször is győződjünk meg arról, hogy naprakészek a számítógépeink, mobil eszközeink, applikációink és minden, ami az internethez kapcsolódik. A kiberbűnözők folyamatosan új sérülékenységeket keresnek az eszközeinken használt szoftverekben. Amikor felfedezik a sérülékenységeket, akkor speciális programokat használnak, hogy feltörjék az általunk használt eszközöket. Eközben az eszközeinkhez szoftvereket gyártó cégek keményen dolgoznak azon, hogy frissítések kiadásával helyrehozzák ezeket a sérülékenységeket. Ezen frissítéseknek a számítógépeinkre és eszközeinkre történő telepítésével sokkal nehezebbé tesszük azok feltörését és ez az, ami annyira frusztráló a WannaCry terjedésével kapcsolatban. A Microsoft már több mint 2 hónapja közzétette azokat a frissítéseket, melyek javítják a sérülékenységet és megállíthatják ezt a támadást. Ha a szervezetek naprakészen tartották volna a számítógépeiket, akkor ez a támadás soha nem valósulhatott volna meg. Annak érdekében, hogy biztosítsuk az eszközeink naprakészségét, engedélyezzük az automatikus frissítéseket. Ez a szabály alkalmazandó szinte bármely technológia esetében ami kapcsolódik a hálózathoz, nem csak a

A WannaCry tanulságai

számítógépek, és a mobil eszközök, hanem az internethez kapcsolódó TV-k, otthoni routerek, játékkonzolok illetve majd egyszer talán az autóink esetében egyaránt. Ha az operációs rendszereink vagy eszközeink olyan régiek, mint pl. a Windows XP, hogy a gyártó azt már nem támogatja biztonsági frissítésekkel, akkor cseréljük le őket újakra, melyek támogatottak.

Annak érdekében, hogy megvédjük magunkat az olyan támadásoktól, mint a WannaCry három egyszerű lépést kell tennünk: mindig frissítsük a számítógépünket, legyünk óvatosak az adathalász támadásokkal és készítsünk biztonsági mentéseket a számítógépünkről.

Biztonsági Mentések

Néhány esetben a naprakész rendszereket is megfertőzhetik az olyan kibertámadások, mint a zsarolóvírus. A második módszer a saját védelmünk érdekében az adatainkról történő biztonsági mentések készítése. A biztonsági mentés az adataink másolata, amit nem a mobileszközeinken vagy a számítógépünkön tárolunk. Amikor értékes adatot veszítünk el, akkor visszaállíthatjuk azt a biztonsági mentéseinkből. Sajnos sokan nem készítenek rendszeres biztonsági mentéseket, annak ellenére sem, hogy ez egyszerű és olcsó megoldás. Két módja van az adatok mentésének: fizikai adathordozó vagy felhő alapú tárolás. Mindkét megközelítésnek megvannak az előnyei és hátrányai. Alkalmazható mindkét megközelítés egyszerre ha bizonytalanok vagyunk abban, hogy melyik módszert válasszuk.

A fizikai adathordozók, mint a külső USB meghajtó vagy az otthonainkban illetve irodánkban elhelyezett hálózati meghajtók a mi felügyeletünk alá tartozó eszközök. A saját fizikai adathordozó előnye hogy nagyon gyorsan hozzáférhetünk a biztonsági mentésünkhöz és visszaállíthatunk nagy mennyiségű adatot. A hátránya ennek a megoldásnak, hogy ha zsarolóvírussal fertőződünk meg akkor elképzelhető, hogy a fertőzés átterjed a biztonsági mentéseinkre is. Ha fizikai adathordozót használunk a biztonsági mentéshez, akkor azt az eszközünktől leválasztva, biztonságos helyen tároljuk. Figyeljünk rá, hogy a biztonsági mentéseket tároló adathordozókat megfelelően felcímkézzük. A felhő alapú megoldások olyan online szolgáltatások, melyek az interneten mentik és tárolják a fájljainkat. Általában úgy működik, hogy feltelepítünk egy programot a számítógépünkre, amely mindenről gondoskodik. A felhőszolgáltatások előnye az egyszerűségük. Továbbá, ha zsarolóvírussal fertőződünk meg, akkor az általában nem fér hozzá a felhő alapú mentéseinkhez. A hátránya, hogy hosszabb ideig tarthat a nagyobb mennyiségű adat mentése és visszaállítása. Bizonyosodjunk meg a felhő alapú biztonsági mentések esetében a személyes adatok védelméről és biztonságáról, hogy biztosít e olyan erős biztonsági szolgáltatásokat, mint például az adatok titkosítása és az autentikáció.

Adathalászat

Végül, a rosszindulatú támadók mindig frissítik és változtatják a támadási módszereiket. A kiberbűnözők gyakran alkalmaznak egy másik, adathalászat nevű támadási típust, hogy megtámadják és megfertőzzék az áldozatokat. Az adathalászat

A WannaCry tanulságai

során a kiberbűnözők egy olyan csali emailt küldenek, mellyel megpróbálnak rávenni egy fertőzött melléklet, vagy egy rosszindulatú weboldal megnyitására. Ha ezt megtesszük, akkor a számítógépünk megfertőződik. A „WannaCry" ugyan nem használta ezt a támadási módszert, azonban ez egy gyakran használt módszer számos egyéb típusú támadáshoz, beleértve a legtöbb fajta zsarolóvírust is. Azok a kiberbűnözők, akik a WannaCry-t fejlesztették kétségtelenül frissíteni fogják a támadási módszerüket az elkövetkező hónapokban és új technikákat fognak alkalmazni - mint az adathalászat - ahhoz, hogy még több számítógépet fertőzzenek meg. Annak érdekében, hogy megvédjük magunkat az ilyen email alapú támadásoktól a józanészre kell hallgatni. Ha egy email vagy üzenet furcsa, gyanús vagy túl szép ahhoz, hogy igaz legyen - akkor az valószínűleg támadás.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Mi a káros szoftver:	https://securingthehuman.sans.org/ouch/2016#march2016
Zsarolóvírus:	https://securingthehuman.sans.org/ouch/2016#august2016
Biztonsági mentések:	https://securingthehuman.sans.org/ouch/2015#august2015
Adathalászat:	https://securingthehuman.sans.org/ouch/2015#december2015
A felhő biztonságos használata:	https://securingthehuman.sans.org/ouch/2016#november2016

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita