PARIPA beszámoló

Ransomware és egyéb kártékony kódok elleni védekezés

(2017/2018 1. félév)

Készítette: Tamás Csongor BIFAPW

Konzulenseim: Bencsáth Boldizsár dr. (CrySyS Lab), Guba Viktor (Nemzeti Infokommunikációs Szolgáltató zrt.)

Ismertető a programról

A PARIPA (PARtnerségben az IPArral) program 2017 őszén indult el a BME-n. Célja, hogy szűkítse a szakadékot az egyetemi oktatás és az ipari igények között. A részt vevő diákok tapasztalatot szerezhetnek az iparban való munkavállalásban és a program részét képző ÖNKÉP (ÖNKÉPző) műhelyen vendég előadókon keresztül betekintést nyerhetnek az egyetemi oktatásban háttérbe szoruló, de az iparban nélkülözhetetlen és kulcs fontosságú „soft skill”-ek működésébe. A részt vevő cégek kapcsolatba kerülnek az egyetemmel, így lehetőségük van magukhoz csábítani érdeklődő, fiatal tehetségeket, ami a versenyben maradásuk záloga. Végezetül az egyetem a cégeken keresztül pénzt áramoltat az oktatásba, melynek segítségével fejlesztheti működését.

A programban részt vevő cégek és egyetemi kutatók által közösen megfogalmazott és kitűzött témákra pályázhattak az érdeklődő hallgatók. A feladatok hallgatókhoz rendelését követően a diákok egyetemi és céges témavezetőik folyamatos koordinálásával megkezdték munkájukat a megnyert témákban.

Én a „Ransomware és egyéb kártékony kódok elleni védekezés” témát nyertem el a NISZ zrt. kiírásában. Konzulenseim Bencsáth Boldizsár dr. a BME-n működő CrySyS laboratóriumból és Guba Viktor a NISZ zrt.-től.

Téma fontossága

Napjainkra majdnem a Föld népességének fele rendelkezik internet eléréssel valamilyen eszközről. Ennek két legnépszerűbb alkalmazása a World Wide Web és az emailek. Mindkettő kiváló eszközt nyújt a támadóknak a fertőzés terjesztésére.

Elsőként tekintsünk vissza 2017 tavaszára. Május 12-én indult útjára a WannaCry, minden idők eddigi legtöbb fertőzésért felelős zsarolóvírusa. Közel 700 000-re becsülik a fertőzések számát világszerte. „Sikerének” egy oka, hogy sok malware-rel ellentétben a WannaCry-nak nem volt földrajzi célpontja, akit tudott, megfertőzött. Terjedésre az EtarnalBlue névre keresztelt Windows exploitot használta, mely a Microsoft Szerver Message Block alkalmazás-rétegbeli protokoll hibáját használta ki. Ezen keresztül a WannaCrynak lehetősége volt egy fertőzött számítógépről szkennelni a helyi hálózat többi tagját és nyitott

TCP 445-ös portokon keresztül lemásolhatta saját kódját a cél eszközre. Ekkor keresést indított és titkosított minden fájlt, aminek kiterjesztése egy a kijelölt 176-ból, majd felajánlotta, hogy bitcoinban fizetett $300 fejében visszaszolgáltatja a fájlokat. Így összesen közel $59000-nak megfelelő bitcoin gyűlt össze a támadók számláján. A támadást megállítani egy killswitch-csel lehetett, ami egy, majd később egy második és harmadik domain beregisztrálásából állt.

Másodikként a június 26-án útnak induló exPetr másik nevén NotPetya zsarolóvírust kell megemlíteni. Ez nagyságrendileg 2000 cég megfertőzéséért felel, köztük található a Nurofen, a Durex, a Maersk illetve a FedEx is összesen több mint $9 000 000 elmaradt haszonnal. Terjedéséhez EtarnalBlue-t, EternelRomance-t valamint a fertőzött gépekről ellopott bejelentkezési információkat használta. Egy gépre jutva vár 10-60 percet, majd reboot-olja a rendszert. Ekkor titkosítja a Master Fájl Tablet valamit felülírja a Master Boot Record-ot egy saját betöltővel, ami felszólít a ransome kifizetésére. Ez azonban csak egy álca, a támadók a kifizetés után sem képesek visszaállítani az áldozat számítógépének eredeti állapotát.

Végül tekintsük rá a dolgozat írásakor (2017 december) nem egészen két hónapos programra, a BadRabbitre. Ez a ransomware kb. 200 orosz és néhány ukrán fertőzésért felel. Terjedésre hasonló módszereket használ, mint az exPetr. Ahhoz hasonlóan felülírja a Master Boot Record-ot, azonban ez egy valódi ransomware, a váltságdíj kifizetése után helyreállítja a gép állapotát.

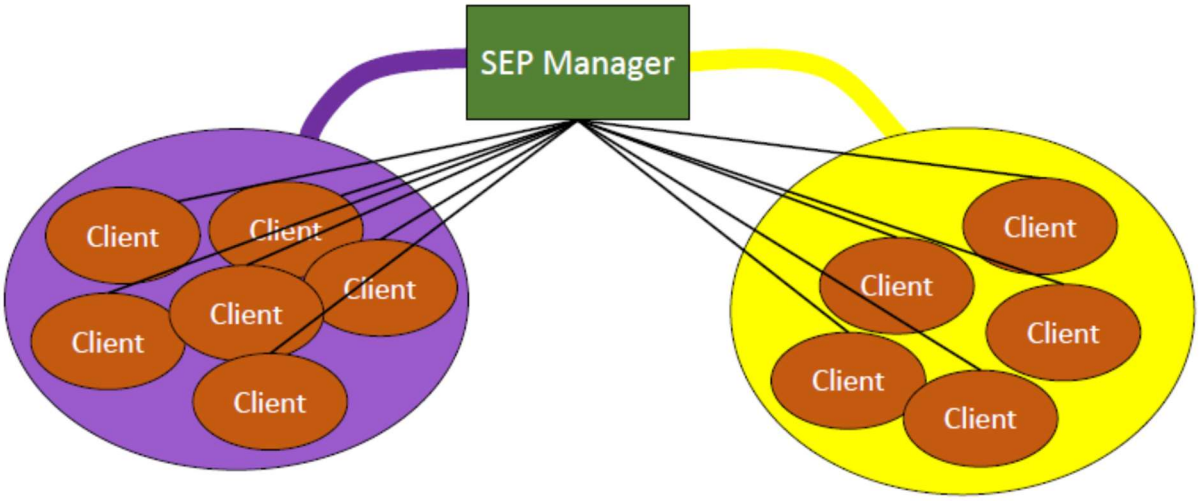
Ezek a közelmúltbeli események hangsúlyozzák a téma és a kutatás fontosságát. Sőt, egy állami szektorban működő cég számára, mint a NISZ zrt. kiemelten fontos az ehhez hasonló támadásokra való megfelelő felkészülés. A munkámat ebben a szellemben folytattam.

A munka kezdete

Munkám során a Symantec Endpoint Protection (továbbiakban SEP) szoftverrel ismerkedtem meg. Ez egy komplex védelmi program főként Windows rendszerekre kialakítva, mely számos eszközzel igyekszik megvédeni a felhasználót a fertőzésektől.

A program architektúrája két komponensből áll. Ezek a SEP Manager és a SEP Client. A SEP Manager egy szerver gépen fut és lehetőség szerint folyamatos összeköttetéssel bír a

Symantec szerverei valamint az összes általa felügyelt kliens felé. Az architektúrát az 1. ábra szemlélteti.



1. ábra. Symantec Endpoint architektúra vázlata

A Manager kapcsolatban áll az összes általa felügyelt klienssel. Ezen a kapcsolaton keresztül a Manager teljhatalommal bír a kliensek felett. A klienseket csoportokba szervezhetjük és a csoportokra eltérő szabályokat, működési mintákat vezethetünk be, amit aztán a csoport tagjain érvényesíthetünk.

Tekintsük sorra, hogy az egyes elérhető eszközök milyen védekezési lehetőségeket nyújtanak számunkra. Ezek kapcsolatát szemlélteti a 2. ábra.

A SEP legfontosabb, központi védelmi rendszere a Virus and Spyware Protection, Ebben négy eszköz található: Auto-Protect, Download Protection, SONAR, Early Launch Anti-Malware Driver. A munka tapasztalata alapján ezek közül az Auto-Protect végzi a legtöbb munkát. Ez minden fájl hozzáférési, másolási, írási kísérlet során működésbe lép és szkenneli a részt vevő objektumokat, az aktuális vírus definíciós adatbázis alapján. A Download Protection karanténba helyez minden olyan letöltött fájlt, amit a Symantec felhasználók kártékonynak vélnek, de erről még nem bizonyosodtak meg. A SONAR valós idejű védelmet igyekszik nyújtani a még nem felfedezett, de vélhetően kártékony kódok ellen. Végül az Early Launch Anti-Malware Driver a rendszer indításakor még a harmadik fél által készített illesztőprogramok betöltése előtt működésbe lép és igyekszik kiszűrni az ide beékelődő kártevőket.

	Fájl név	Fájl hash	Fájl tartalom	Tűzfal szabályok	Fájl hozzáférési kísérletek	Hálózati forgalom
Virus and Spyware Protection	✓	✓			✓	✓
Firewall				✓		
Intrusion Prevention						✓
Application and Device Control	✓	✓			✓	
Host Integrity						
LiveUpdate						
Exceptions						
Memory Exploit Mitigation					✓	✓

2. ábra. Eszközök és védekezési módszerek kapcsolata

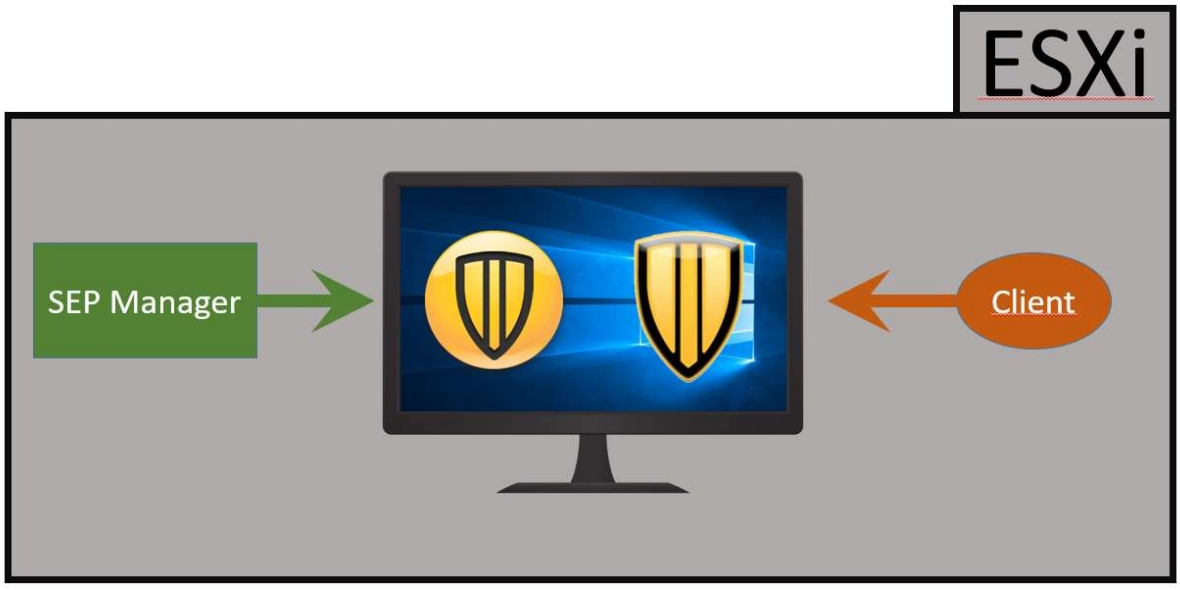
Ezek közül csak a Firewall, Intrusion Prevention és Application and Device Control eszközökben tudunk megfogalmazni saját szabályokat. Látszik, hogy így a fájl tartalma szerinti védekezés kiesik a hatókörünkből.

A környezet megismerése után konzulensemmel, Dr. Bencsáth Boldizsárral kitűztük a féléves feladatot: „Virtuális gépeken tesztelem a meglévő szabályokat néhány malware-en. Ha találok olyat, ami átjut az eddigi védelmen, akkor megpróbálok rá szabályt írni, hogy a jövőben ez ne történjen meg.” Így egyaránt megismerkedem kártevőkkel, támadási és védekezési formákkal is.

Környezet kialakítása

A feladat teljesítéséhez először fel kellett állítani egy teszt környezetet. Erre a legalkalmasabb konstrukciót virtuális gépekkel hozhatjuk létre, hiszen, itt teljes befolyásunk van a rendszer felett és sokkal rugalmasabb, mint egy fizikai architektúra. Hovatovább, egy fertőzés esetén percek alatt visszaállíthatjuk a virtuális gépet egy korábban elmentett állapotba és jelen helyzetből folytathatjuk a munkát.

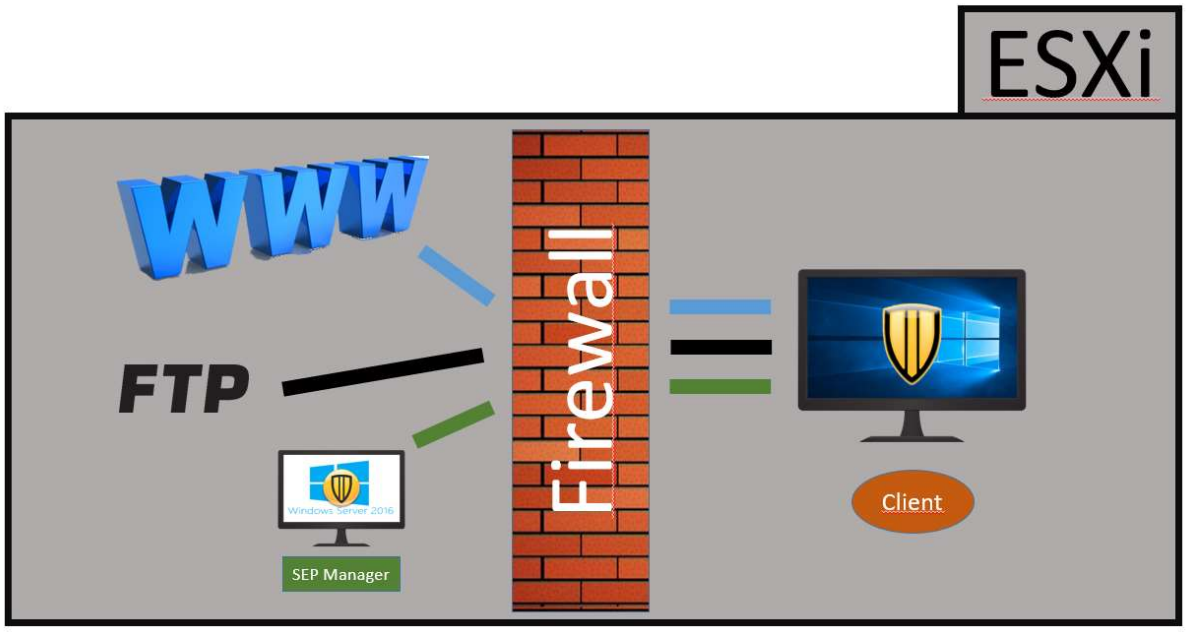
A környezet kialakításához lehetőségem nyílt használni egy tanszéki ESXi rendszert. Kezdetben ezen létrehoztunk egy Windows 10-es virtuális gépet. Azért ezt az operációs rendszert választottam, mert a SEP számos funkciója csak Windowsos környezetben működik, ebből is a 8-as verziótól kezdve. Továbbá szükség esetén így bármikor lehetőség nyílik a Windows Defender használatára. Az architektúrát a 3. ábra szemlélteti.



2. ábra. A környezet első verziójának felépítése

Először feltelepítettem a Managert, melyből lehetőség nyílik a kliens programot telepítő fájl generálására. Ezzel a módszerrel a klienst is feltelepítettem a gépre (3. ábra), mely automatikusan kapcsolódott a szerverhez. Így mind a két szoftver azonos gépen futott, ami rövidesen problémássá is vált. Megesett, hogy rebootoláskor egyik program sem tudott elindulni. Ennek okára csak találgatásaim vannak. Egyik, hogy később kiderült, hogy a Manager nem támogat semmilyen asztali operációs rendszert, másik, hogy a kliens egy eszköze blokkolta a Manager egyik komponensének elindulását. Később felvetődhetett volna az a probléma, hogy egy, a Manageren kialakított szabály, melyet a kliens érvényesít, megakadályozza a szerverrel való kommunikációt, vagy annak helyes működését, így lehetetlenné válik jelen szabály eltávolítása is.

Ebből kifolyólag jónak láttam változtatni ezen: létrehoztam egy Windows Szerver 2016-os gépet, melyre feltelepítettem a Managert és a Windows 10-es gépet pedig alaphelyzetbe állítottam és újratelepítettem rá a kliens programot. Ezt szemlélteti a 4. ábra.



3. ábra. A környezet második verziójának felépítése

A klienst áthelyeztük egy „belső” hálózatba, melyet egy tűzfal választ el a „külvilágtól”. Erre azért van szükség, mert a munka során fennáll a fertőzés veszélye, így viszont kontrollálhatjuk a kliens hálózati forgalmát, megakadályozhatjuk a terjedést. A külvilággal való kapcsolattartásra, fájlok mozgatására összekapcsoltuk mind a klienst mind a szervert egy FTP szerverrel. Ezen keresztül juttathatunk mintákat a kliens gépre.

Munkám során használtam a Far Managert, mely egy nagy funkcionalitású fájl kezelő program, Wireshark hálózati protokoll analizátor programot valamint a Sysinternals Suite-ből a Process Explorert.

Próba

A környezet kialakítása után végeztem egy próbát, hogy megfelelően működik-e a rendszer. Először megvizsgáltam, hogy a kliens gépről tudok-e kommunikálni az FTP szerverrel. Ennek működését mutatja az 5. ábra.

```
c:\PARIPA>ftp 10.105.1.97
Connected to 10.105.1.97.
220 ProFTPD 1.3.5 Server (Debian) [::ffff:10.105.1.97]
200 UTF8 set to on
User (10.105.1.97:(none)): sfd
331 Password required for sfd
Password:
530 Login incorrect.
Login failed.
ftp> quit
221 Goodbye.
```

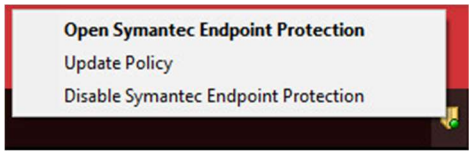
4. ábra. Kapcsolódás az FTP szerverhez

Majd létrehoztam egy új tűzfal szabályt Block FTP néven, mely blokkol minden olyan ki- és bemenő TCP forgalmat, aminél a távoli cím a 20-as vagy 21-es port. Ez látható az 6. ábrán.

...	E...	Name	Action	Application	Host	Service	Log	Severity
1	✔	Block FTP	Block	Any	Any	TCP:[Remote=20,21]	Write to Traffic Log	5-Major

5. ábra. Tűzfal szabály az FTP kapcsolatok blokkolására

Ezt követően a klienssel lekérdeztem a legfrissebb szabályokat (7. ábra), majd újra kapcsolódni próbáltam (8. ábra), de ekkor már nem sikerült.



7. ábra. Szabályok frissítése a klienssen

```
c:\PARIPA>ftp 10.105.1.97
^C
```

6. ábra. Sikertelen kapcsolódást az FTP szerverhez

A szabály alkalmazásáról készült egy napló bejegyzés is (9.ábra), mely mutatja, hogy tényleg az újonnan létrehozott szabály akadályozta meg a kapcsolódást.

Date and Time	Action	Severity	Direction	Protocol	Remote Host	Remote Port	Remote MAC	Local Host	Local MAC
12/9/2017 11:05...	Blocked	5	Outgoing	TCP	10.105.1.97	21	00-0C-29-44-3...	10.105.36...	00-0C-29-44-5...

Loc...	Application	User	User Domain	Location	Occurr...	Begin Time
58660	C:\Windows\System32\ftp.exe	user	DESKTOP-QJTLPK3	Default	2	12/9/2017 11:05...

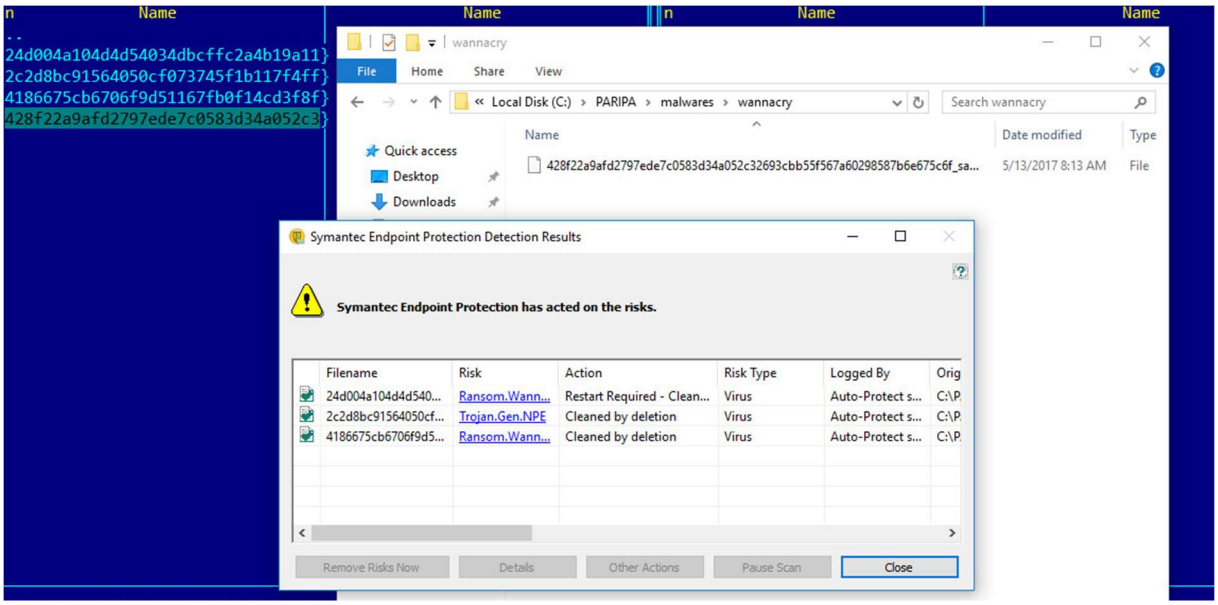
End Time	Rule
12/9/2017 11:05...	Block FTP

8. ábra. Napló bejegyzés a blokkolt FTP kapcsolatról

Tesztek

Következhetett néhány minta tesztelése. Először a tűzfallal blokkoltam minden hálózati forgalmat, majd engedélyeztem a kapcsolatot az FTP szerverrel. Ezek a kapcsolaton keresztül juttattam a mintákat a gépre.

Elsőként négy WannaCry mintát másoltam át. Ez látható a 10. ábrán. Hármat rögvest felismert és eltávolított az Auto-Protect, de a negyediket nem. Ezt azért nem, mert ez egy kulccsal védett .zip fájl, vagyis a helyes kicsomagoláshoz mindenképp szükség van a kulcsra. Kicsomagolva, az ebben található további két mintát is eltávolította az Auto-Protect.



9. ábra. WannaCry minták kliensre másolása és az Auto-Protect figyelmeztetése

Másodikként egy CryptoLocker mintát másoltam át, ezt is eltávolította a Symantec.

Harmadikként sok CosmicDuke-ot próbáltam ki, ezek közt már volt négy olyan, amit az Auto-Protect nem ismert fel. Kettőnek alaposabban utána jártam. Az elsőt elindítva megpróbálja feloldatni a tangentialreality.com domaint, de nem jár sikerrel, hiszen az ilyen forgalom blokkolva van. Másik számítógépen feloldva Non-exsistent domain választ kapunk.

A második a store.extremesportsevents.net-et próbálja feloldani. Ez már egy létező domain. Securelist.com weboldalon szintén felfedezték ezt a két malware verziót, vélhetően a fent említett domaineket használták Command & Control szervereknek (11 ábra).

Update 2:

MD5	7fcf05f7773dc3714ebad1a9b28ea8b9
Size	28160 bytes
Compilation timestamp	Fri Mar 07 10:04:58 2014
C&C	hxxp://tangentialreality.com/cache/template/yoo_cache.php

We have observed another similar Trojan, although not on the C&Cs directly:

MD5	edf7a81dab0bf0520bfb8204a010b730, ba57f95eba99722ebdeae433fc168d72 (dropped)
Size	700K, 28160 (dropped)
Compilation timestamps	Sat Dec 14 18:44:11 2013 (top) Fri Jan 10 12:59:36 2014 (dropped)
C&C	hxxp://store.extremesportsevents.net/index.php?i=62B...[snip]

10. ábra. Felismert CosmicDuke minták a securelist.com oldalon

Mivel ezeket a mintákat nem ismerte fel a Symantec, ezért kiszámoltam ezen fájlok MD5-ös hash-ét és létrehoztam egy új szabályt az Application Control eszközben, mellyel blokkoltam minden olyan programot, ami futtatni szeretné ezeket a fájlokat. A szabályok frissítését követően nem is sikerült futtatni ezeket a fájlokat.

Konklúzió

A félév során sikerült kialakítani egy egyszerű teszt környezetet, ahol a további munka folyhat. A teszteknek nincs nagy jelentőségük, megfelelő mintahalmazzal akár egy program is önállóan végezhetné őket. Azonban mégis hasznos volt, mert így megismerkedtem a szóban forgó kártevőkkel és védekezési lehetőségekkel, ESXi-vel, VPN-nel, tűzfalakkal és nem utolsó sorban a Symantec Endpoint Protection-nel. Ezt az alapot szeretném tovább szélesíteni a következő félév során, minél több akadály leküzdésével.

Források

BME HIT. (dátum nélk.). *https://www.hit.bme.hu/page/paripa*.

CrySyS. (2014. július 3). *http://blog.crysys.hu/2014/07/miniduke-2-cosmicduke/*.

CrySyS. (dátum nélk.). *http://crysys.hu/*.

Kaspersky. (2014. július 3). *https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/*.

Kaspersky. (2017. október 24). *https://securelist.com/bad-rabbit-ransomware/82851/*.

Kaspersky. (2017. június 28). *https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/*.

Kaspersky. (2017. június 27). *https://securelist.com/schroedingers-petya/78870/*.

Kaspersky. (2017. may 15). *https://securelist.com/wannacry-faq-what-you-need-to-know-today/78411/*.

Kaspersky. (2017. június 27). *https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/*.

Kaspersky. (dátum nélk.). *https://www.kaspersky.com/blog/tag/notpetya/*.

Malwarebytes. (2017. október 24). *https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/*.

NISZ zrt. (dátum nélk.). *http://www.nisz.hu/*.

Symantec. (2017. október 25). *https://www.symantec.com/connect/blogs/badrabbit-new-strain-ransomware-hits-russia-and-ukraine*.