Az informatikai biztonság alapjai

Pintér-Huszti Andrea

2020. szeptember 6.

Tartalom

- Mártékony programok
 - Fejlett Perzisztens Fenyegetés
 - Terjedés módja: Fertőzött tartalom
 - Terjedés módja: Sebezhetőség kiaknázása
 - Terjedés módja: Pszichológiai támadás
 - Büntető rutin: Rendszer károsítása
 - Büntető rutin: Támadó ügynökök
 - Büntető rutin: Információszerzés
 - Büntető rutin: Lopakodás
 - Biztonsági intézkedések

Kártékony programok

Kártékony programok

- Malicious software = malware
- Olyan program, mely valamely rendszerbe beépülve az áldozat adatainak, szoftvereinek bizalmasságát, integritását, rendelkezésre állását veszélyezteti, vagy erkölcsi károkat okoznak, mert pénz, időt, embert kötnek le.
- Főbb kategóriák: terjedés és büntető rutin módja szerint.
- Terjedés módja szerint: vírusok(virus), férgek(worm) és trójaiak(Trojan). Büntető rutinuk szerint: botnet, adathalászat(phishing), kémprogram(spyware), gyökércsomagok (rootkit)-ek.

• Terjedés módja:

- fertőzött fájl futtatásával (vírus)
- szoftver sérülékenységeit aknázza ki (féreg)
- pszichológiai támadás (trójaiak installálása, adathalász emailek megválaszolása, spamek)
- Gazdaprogram szükségessége:
 - szükséges (vírus)
 - nem szükséges (féreg)
- Sokszorosítás:
 - nem képes önmaga megsokszorozására (trójaiak, spam email)
 - megsokszorozódik (vírus, féreg)
- Büntető rutin alapján:
 - rendszer- és adatfájlok megrongálása
 - szolgáltatás eltulajdonítása (botnet támadás esetén zombie gépek szerzése)
 - információ ellopása (jelszavak, személyes információk)

Támadói eszközrendszer (Attack Toolkit)

- Régen: egy terjedési mód egy büntető rutinnal
 Most: terjedési módok és büntető rutinok széles skálája
- Kevert támadások(blended attack) a fertőzés sebességének maximalizálása céljából többféle terjedési módot is használnak. Többségük még update mechanizmusokat is támogatnak, mely lehetővé teszi aktiválásuk után, hogy megváltoztassák terjedési módukat és büntető rutinukat.
- Az eszközrendszer, vagy crimeware(bűncselekmény+szoftver), többféle terjedési módot és büntető rutint is tartalmaz, melyet akár egy nem szakember is képes telepíteni és használni.

Zeus Crimeware Toolkit (2007):

- Személyes információk (banki információk) megszerzése a felhasználók számítógépeinek megfertőzésével.
- A legfelkapottabb aktív botnet-ek egyike. A botnet olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást.
- Többféle módon lopják el a felhasználó identitását, kontrollálják számítógépét.
- HTML kód-injektálás, minden egyes egérkattintásnál lementi a képenyőképet (virtuális billenytűzet ellen) stb.

Fejlett Perzisztens Fenyegetés

Fejlett Perzisztens Fenyegetés (Advanced Persistent Threat (APT))

Fejlett Perzisztens Fenyegetés: a fejlett, perzisztens fenyegetettségek összefoglaló neve. Kiberbűnözés, mely üzleti és politikai célpontokat célozzák meg, többféle behatoló technológia és kártékony program alkalmazásával.

Fejlett: A támadók számos eszközt használnak fel céljuk eléréséhez. Céljuk, hogy elkerüljék a célkeresztbe állított rendszert körülölelő vagy az abban működő védelmi eszközöket. A NIST (National Institute of Standards and Technology) mindezt így fogalmazta meg: a támadók alkalmazkodnak a védők erőfeszítéseihez annak érdekében, hogy azokkal szembeszállhassanak.

Fejlett Perzisztens Fenyegetés (Advanced Persistent Threat (APT))

- Perzisztens: A támadók egy jól meghatározott céllal tevékenykednek, és többnyire nem véletlenszerűen, találgatás útján próbálnak rájönni, hogy milyen sebezhetőségeket tudnak kihasználni, hanem már felkészülten, alapos felderítőmunka után lépnek akcióba. Ameddig el nem érik a céljukat (például meg nem találják az általuk keresett bizalmas adatokat), addig nem hagyják el a rendszert. Gondoskodnak arról, hogy a hozzáférésük fenntartható legyen.
- Fenyegetés: Ez esetben célzott, irányított és komplex akciókról beszélünk, amelyek komoly fenyegetést jelenthetnek az informatikai rendszerekre és az adatokra.

Fejlett Perzisztens Fenyegetés - Célok

- APT-k különböznek a többi támadástól a célpont körültekintő kiválasztása miatt. Információt gyűjt, hogy pl. megállapítsa az alkalmazott szerepét és a hozzáférés szintjét. Amennyiben ez nem vezet célra, akkor más felhasználók után kutathat, akik jobb pozícióban, több privilégiummal rendelkeznek. Nem egyszerűen feltöri a szervezet infrastruktúráját, sokkal inkább az alkalmazottakra koncentrálnak.
- pl.: Aurora, RSA, APT1, Stuxnet
- Céljuk: szellemi termék, szerzői tulajdon ellopása, biztonsági és infrastruktúrális adatok megszerzése, infrastruktúra fizikai lekapcsolása
- A speciális célpont és a perzisztens jellegük miatt a védekezés nem kivitelezhető hatékonyan csupán hagyományos biztonsági eszközök bevetésével. Védelmi intézkedés: többféle technikai védintézkedés kombinációja, oktatás.

Fejlett Perzisztens Fenyegetés - Technikák

- pszichológiai támadás
- célzott adathalász e-mail (spear-phishing e-mail): E-mailen keresztül egy meghatározott személyt, szervezetet vagy vállalatot céloz meg azzal, hogy megszerezze bizalmas adatait vagy kártékony programot installáljon számítógépére.
- drive-by-downloads: Támadás, mely egy fertőzött website-on levő kóddal kiaknázza a böngésző sérülékenységét, hogy megtámadja a felhasználó rendszerét böngészés közben.
- nulladik napi támadás (zero-day exploits): Valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás. A "nulladik napi" támadás az első vagy "nulladik" napon történik, amikor a fejlesztő még nem juttatta el a biztonsági javítást a szoftver felhasználóihoz.

APT példa: Stuxnet

- Stuxnet az első katonai féreg, mely 2010-ben bukott le egy iráni nukleáris erőmű számítógépén.
- A felfedezés óta bebizonyosodott, hogy a Stuxnet vírus az erőműre közvetlen fenyegetést nem jelentett, mert annak az urániumdúsító berendezések voltak a célpontjai. Közvetett értelemben azonban az a tény mindenképpen fenyegető, hogy egy vírus bejutott a létesítménybe.
- 2010. november 16-án Irán leállította az urándúsítóit, miután a centrifugák több mint 20%-a megsemmisült a Stuxnet tevékenysége nyomán.
- A férget úgy tervezték meg, hogy törölje magát 2012-ben.
- Négy nulladik napi támadást hajtott végre, Microsoft Windows operációs rendszerű gépeken jutott be és a Siemens Step7 mérnöki szoftvert kereste.

APT példa: Stuxnet

- Három modulja:
 - féreg, mely a támadás büntető rutinjait futtatja.
 - kapcsolat fájl, mely automatikusan futtatja a féreg másolatokat.
 - gyökércsomag, mely felelős a kártékony fájlok, processzek elrejtéséért megelőzve az esetleges lebukást.
- Stuxnet egy fertőzött USB pendrive segítségével jutott be.
- A féreg elterjedt a rendszerben.
- Stuxnet gyökércsomaggal módosította a kódot és nem várt parancsokat hajtott végre.

APT példa 2.

- Információgyűjtés bizonyos alkalmazottakkal kapcsolatosan, begyűjtött információkkal a kezükben phishing emailt küldenek a felhasználónak (cél-releváns tartalmat, például a pénzügyi osztály számára néhány tanácsot a szabályzási kontrollokat illetően).
- A támadó két különböző adathalász emailt küldött két napos periódus alatt. A két email az alkalmazottak két kisebb csoportjának szólt. Az email tárgya: "2011 Recruitment Plan" (2011-es Toborzási Terv). Az email jól meg volt szerkesztve ahhoz, hogy az alkalmazottak egyike kiszedje a levélszemét mappából, és megnyissa a csatolt excel fájlt. A táblázat egy nulladik napi támadást tartalmazott, mely egy hátsó ajtót (a távoli támadó teljes kontrollt kap) telepített egy Adobe Flash sérülékenységet kihasználva (CVE-2011-0609). Megjegyzés: az Adobe azóta orvosolta a sérülékenységet.

Terjedés módja: Fertőzött tartalom

- Program, amely saját másolatait helyezi el (megfertőzi) más, végrehajtható programokban vagy dokumentumokban.
- A vírus kód megfertőzhet alkalmazásokat, vagy rendszerfájlokat, vagy programkódokat, melyeket rendszerbetöltésnél futtat a rendszer.
- Mostanában script kód formában gyakoriak, melyek a Microsoft Word dokumentumok, Excel táblák, vagy Adobe PDF dokumentumok aktív tartalmát adják.
- A vírus kód lefutásával valamilyen kárt okoz, pl. törli az adatokat, programokat, melyet az aktuális felhasználó jogosultsága enged.

A számítógépes vírus három részből áll:

- Fertőző mechanizmus (infection vector): Mechanizmus, mellyel a vírus terjed, sokszorozódik.
- Indíték: Esemény vagy feltétel, mely meghatározza mikor aktiválódik a büntető rutin. Az ilyen a programokat logikai bombának is hívják.
- Büntető rutin: Kárt okozó tevékenységek. (pl. törlés)

Vírusok célpont szerinti csoportosítása

- Boot vírusok: A merevlemez boot szektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik.
 Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi.
- Alkalmazásvírusok: A megfertőzött állományokba beírják a saját kódjukat. Két fajtáját különböztetjük meg: hozzáfűződő (append) és felülíró (replace) vírusokat. Amennyiben egy fertőzött fájlt elindítunk, a vírus betöltődik a memóriába és megfertőzi az összes többi elindított programot.
 - A hozzáfűződő vírusok az alkalmazások végéhez fűződnek, elhelyeznek azonban a program elején egy kódot, hogy az alkalmazás indulásakor előbb ők töltődjenek be.
 - A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít, az eredeti állapot nem állítható helyre.



Vírusok célpont szerinti csoportosítása

- Macrovírusok: Elsősorban makrókat támogató dokumentumszerkesztő programokat támadnak meg (Word, Excel), általuk készített dokumentukokkal terjednek. Terjedésükhöz elegendő egy fertőzött állomány megnyitása, és a vírus már be is töltődik a memóriába, mely a későbbiekben megnyitott dokumentumokat megfertőzi. lde sorolhatók a levelező vírusok is. A csatolt fertőzött fájlok megnyitásakor aktivizálják magukat és általában a levelezési listában szereplő partnereknek írnak levelet, melyhez saját maguk másolatát is hozzáfűzik. Ha a levelezési címlistában nagyon sok partner van, akkor olyan mennyiségű levéláradat indulhat, amely megbénítja egy nagyvállalat levelezőrendszerét is.
- Összetett vírus: Többféle módon, többféle állományt képesek megfertőzni.

Vírusok csoportosítása rejtezkedési stratégiájuk szerint I.

- Titkosított vírus: Titkosítással rejti el tartalmát. Az egyik vírusrész egy véletlen titkosító kulcsot generál és titkosítja a vírust. Mivel a vírus titkosítva van különböző kulcs esetén, nem lesznek megegyező bitminták.
- Lopakodó vírus: Az antivírus programot és az operációs rendszert megkerülve a gép memóriájában maradva, a fájl méreteit, az operációs rendszer jellemzőit és a könyvtár struktúráját megváltoztatják. Látszólag tiszta állapotról szóló jelentést képesek mutatni, például a fertőzőtt állomány hossza az eredeti, tiszta állapotnak megfelelő értéket jelenít meg. Használhat gyökércsomag technikákat.
 Gyökércsomag (rootkit): Eszközök, melyeket a támadó

Győkércsomag (rootkit): Eszközök, melyeket a támadó használhat, miután megszerezte a legmagasabb felhasználói jogosultságokat.



Vírusok csoportosítása rejtezkedési stratégiájuk szerint II.

- Polimorf vírus: Bizonyos fertőzési ciklusonként képesek megjelenési formájukat változtatni. Ezzel a módszerrel a bitminta alapú felismerést lehet nehezebbé vagy lehetetlenné tenni. (pl. titkosítás, más instrukciókat szúrnak be). Azon vírusrész, mely felelős a kulcs generálásért és a titkosításért/visszafejtésért mutációs motornak hívjuk. A mutációs motor is módosul minden használat után.
- Metamorfózisra képes vírus: Minden egyes alkalommal teljesen felülírják magukat. Megváltoztatják viselkedésüket és "kinézetüket" is.

Terjedés módja: Sebezhetőség kiaknázása

Férgek - Terjedési technikák

- Kliens és szerver oldali szoftver sebezhetőségének kiaknázásával férnek hozzá más számítógépekhez.
- Használhatnak hálózati kapcsolatokat, hogy rendszerről rendszerre terjedjenek.
- Terjedhetnek megosztott médián keresztül, pl. USB drive, CD, DVD lemezek.
- E-mail vagy üzenőfal férgek makrók és script kódok segítségével terjednek e-mail csatolmány vagy Instant Messenger csatolmányain keresztül.
- Önsokszorosítóak, nincs szükségük gazdaprogramra.

Férgek - Távoli rendszerek elérése

- Terjedés során általában a következőket hajtja végre:
 - Megfelelő hozzáféréseket keres host táblákban, címtárakban vagy cserélhető médiákat keres, melyekkel más gépekhez hozzáférhetnek.
 - Ezekkel a hozzáférési mechanizmusokkal lemásolják magukat távoli rendszerre és végrehajtódnak.

Férgek - Hálózati címek keresési stratégiák

- Véletlen: A fertőzött gazdagépek (hostok) véletlen IP címet használnak. Hatalmas Internet forgalmat eredményez, mely észrevehető, így lebukhat.
- Hit-lista: A támadó összegyűjti a lehetséges sebezhető gépek címének egy hosszú listáját, és el is kezdi a lista elején levő címeket felhasználni. Minden fertőzött gép kap egy darabot a listából. Rövid ideig történik a próbálgatás, nehéz észrevenni.
- Topológiai: A támadó a már fertőzött gép információit felhasználva talál további hostokat.
- Helyi alhálózat: Tűzfal mögötti host próbál megfertőzni további hostokat a helyi hálózatban. Az alhálózat címstruktúráját használja.



Modern férgek

- Multiplatform: Többféle platformot is támadnak, főleg a népszerű UNIX variánsokat, illetve többféle népszerű dokumentumok makró és script kódjait.
- Multi-kihasználás: Többféle módú behatolási rendszer (Web szerverek, böngészők, e-mail, fájl megosztás, egyéb hálózati alkalmazások stb.)
- Ultragyors terjedés: Optimalizálják terjedésüket, hogy rövid idő alatt minél nagyobb valószínűséggel minél több sebezhető gépet próbáljanak.

Modern férgek

- Polimorf: Vírusok polimorf technikáit használja.
- Metamorf: Megváltoztatja viselkedését és "kinézetét".
- Szállítási eszközök: Ideális többféle büntetési rutin terjesztésére, pl DDOS botok, gyökércsomagok, spam e-mail generátorok, és kémprogram.
- Nulladik napi támadás: Azért, hogy maximális meglepetést és terjedést érjen el, a féregnek olyan ismeretlen sebezhetőséget kell kiaknázni, melyet a többség csak végrahajtás után ismer meg.

Mobiltelefon Férgek

- Első féreg: Cabir worm (2004), Lasco and CommWarrior (2005)
- Bluetooth vezeték nélküli hálózaton vagy MMS-en keresztül kommunikálnak.
- Célpontok az okostelefonok (applikációk intallálása), Android és iPhone rendszerek.
- Használhatatlanná teszik a telefont, adatok törlése, költséges SMS-ek küldése.
- Bár mobiltelefon férgek léteznek, de nagyobb mennyiségben fordulnak elő trójai alkalmazások, melyek magukat installálják.

Mobil kód egy program (pl. script, makró vagy más mozdítható kód), mely egy távoli rendszerről a helyire kerül, majd ott végrehajtódik a felhasználó utasítása nélkül.

- Vírusok, férgek, trójaiak számítógépre való továbbításának mechanizmusa.
- Más esetek: Kihasználva a sebezhetőségeket a mobil kód támad, pl.illetéktelen hozzáféréssel vagy megyszerzi a legnagyobb jogosultságokat.
- Népszerű szállító eszközök: Java applets, ActiveX, JavaScript és VBScript.

Drive-by-Downloads

- Cél: Felhasználói alkalmazások hibáinak (bug) kihasználása.
- Drive-by-Downloads:
 - Böngésző sebezhetőségét használja ki. A felhasználó egy a támadó által kontrollált weboldalt megnéz, a felhasználó tudta nélkül a böngésző bug-ját kihasználva letölt és installál egy kártékony programot.
 - A támadó feltérképezi áldozatát, összegyűjti azon web oldalakat, melyeket gyakran látogat. Megvizsgálja ezen oldalakat, a sebezhetőekkel szemben drive-by-download támadást indít és vár míg az áldozat meglátogatja az oldalt. Más felhasználókra nem biztos, hogy hat.

Kliens oldali sebezhetőség

- Malvertising: A támadó fizet, hogy hírdetések jelenjenek meg a célpont weboldalakon. A hírdetések kártékony programot tartalmaznak. A weboldalak látogatóit fertőzik meg.
- E-mail kliensek bug-jainak kihasználása: pl. Klez mass-mailing worm (2001) a Microsoft's Outlook és Outlook Express programokat támadta, hogy automatikusan végrehajtódjon.
- PDF-olvasó bug-jainak kihasználása: PDF-olvasó (sokszor kiegészítő modulok révén, multimédiás tartalmak megjelenítése) kártékony programot installál, amikor PDF dokumentumot nézünk. Ezek a dokumentumok e-mail spammel terjednek, vagy célzott adathalász támadással.

Kattintáseltérítéses támadás (Clickjacking)I.

- A támadó célja összegyűjteni a fertőzőtt felhasználói klikkeket.
- pl.: "Akaratlan lájkolás": Funkciógombnak (jóváhagyás, eltávolítás, bezárás stb.) álcázott like gombok formájában a felhasználók üzenőfalára kikerülnek az üzenetek.
- Ráveszik a felhasználót, hogy tegyen bizonyos dolgokat, pl. kártékony tartalmat lájkolhatunk, és az így becsempészett rosszindulatú kódok villámgyorsan elterjednek az ismerőseink között, vagy egy weboldalt kell megnéznie stb., így installálnak kártékony programokat.
- Pl. Adobe Flash vagy JavaScript segítségével lehet nyomógombokat beszúrni.



Kattintáseltérítéses támadás (Clickjacking)II.

- Tipikus támadás az átlátszó rétegek alkalmazása, ráveszik a felhasználót, hogy kattintson egy linkre vagy gombra.
- Az iFrame technológiával megoldható, hogy egy láthatatlan, az egész ablakot beborító Like gombot húzzunk az oldalunk tartalma fölé, ahol bárhová klikkel a látogató, ha éppen be van jelentkezve Facebookra, azonnal megjelenik az üzenőfalán, hogy neki tetszett az oldal.
- Billenytű lenyomásokat is megszerezhetik. Jól megtervezett stíluslapok, iframe-ek, szöveges beviteli mezők félrevezethetik a felhasználót, aki az átlásztó rétegen adja meg jelszavát stb. a támadónak.

Terjedés módja: Pszichológiai támadás

Pszichológiai támadás - Spam e-mail

- Ötlet: "átverni" és rávenni a felhasználókat, hogy saját rendszerüket veszélyeztessék vagy kiadjanak személyes információkat.
- A felhasználó megnéz vagy válaszol egy SPAM e-mailre, vagy megengedi, hogy felinstallálódjon vagy lefusson egy trójai program vagy script kód.
- A felhasználó aktív részvétele szükséges.
- Spam e-mail: Mai becslések szerint az e-mail forgalom 90% vagy annál több spam e-mail.
- Ez a jelentős növekedés fellendítette a anti-spam ipart, mely igyekszik detektálni és kiszűrni a spam e-maileket.



Spam e-mail

- Kis része a spam-eknek legális mail szerverekről küldődnek ki, nagy részük botnet-eken keresztül mennek, felhasználva a fertőzött (zombie) gépeket.
- A spamek nagy része csak reklám.
- Másrészük valamilyen kártékony programot hordoz:
 Csatolmány tartalmaz egy trójait vagy script kódot, melynek futtatásával megfertőzzük a rendszert.
- Spamek használhatók még adathalászatra is (spear phishing emails), tipikusan átirányítják a felhasználót egy a támadó által kontrollált weblapra, mely valamely valós szolgáltatás tükrözése.

Trójai lovak

- A trójai ló egy olyan kártékony program, mely magukat hasznos programnak álcázzák de képesek a háttérben segíteni egyéb ártó szándékú programok bejutását, és működését a számítógépen.
- Nem sokszorozódnak.
- Mivel hasznos programnak mutatják magukat, ezért leggyakrabban a felhasználó tölti azt le fertőzött honlapokról a számítógépére. Emellett terjedhetnek e-mailben, vagy adathordozókon is.
- Többségük tartalmazza a hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a célszámítógéphez.
- Büntető rutinok: valamely más kártékony program telepítése, kémprogramok, botnet.



Trójai lovak - Modellek

Három modell:

- A program továbbra is folytatja eredeti funkcióját, de rajta kívül még valamilyen büntető rutint is futtat.
- A program továbbra is folytatja eredeti funkcióját, de módosítja annak működését, hogy végrehajtsa a büntető rutint (pl. login program gyűjti a jelszavakat)
- Teljes mértékben lecseréli az eredeti program funkcióját.

Mobiltelefon trójaiak

- 2004-ben jelent meg elsőnek: Skuller
- Célpont: okostelefonok, Android és Apple iPhone. A trójaiak általában az alkalmazás áruházakból tölthetőek le. (pl. Good Weather időjárás előrejelző alkalmazás Google Play áruházban(2017), már visszavonták, büntető rutin: banki adatok ellopása, képernyő lezárása, feloldása)
- Több olyan mobil trójai (Ztorg, Gorpo, Leech) is van, mely root jogosultságokat használ. Az ilyen trójaikkal megfertőzött eszközök általában hálózatba szervezik magukat egyfajta reklám botnetet alkotva, amelyet a hackerek különféle reklámprogram (adware-ek) telepítésére használnak. Röviddel azután, hogy rootolják az eszközt a trójaik letöltenek és telepítenek egy hátsó ajtót. Majd letölt és aktivál két modult, amely képes letölteni, telepíteni és elindítani alkalmazásokat.

Büntető rutin szerinti csoportosítás

Büntető rutinok

- Büntető rutin: tevékenységek, melyek végrehajtódnak a fertőzött rendszeren
- Vannak olyan kártékony programok, melyeknek nincs büntető rutinjuk, céljuk a terjedés.
- Általában van büntető rutinjuk.
- Kategóriák:
 - Rendszer károsítása: adat megsemmisítése, fizikai károkozás, logikai bomba
 - Támadó ügynökök: Botok, zombik
 - Információ lopás: billentyűzetfigyelők (keyloggers), adathalászat (phishing), kémprogramok (spyware)
 - Lopakodás: hátsóajtó (backdoor), gyökércsomag (rootkit)



Büntető rutin: Rendszer károsítása

Adatok megsemmisítése

- 1998, Csernobíl vírus: Windows-95 és 98-as vírus. Ahogy az indítási feltétel teljesül, törli az adatokat a merevlemez első megabájtjának bitjeit 0-ra állítva, komoly kárt okozva a teljes fáilrendszerben.
- 2001, Klez mass-levelező féreg: Windows-95-től XP-ig terjedő rendszerek. E-mailen keresztül terjed, másolatokat készít és küld önmagáról a címtárban levő email címekre. A merevlemezen levő antivírus programot és fájlokat törli.
- Ransomware: Lezárja a felhasználó fájljait, blokkolja az áldozat hozzáférését a számítógéphez, az okozott károk visszafordításáért minden esetben váltságdíjat követel, képesek lehetnek az áldozat érzékeny személyes adatainak megszerzésére (jelszavak), a védelmi szoftverek (antivírus, Anti-Spyware stb.) leállítására, megtévesztő figyelmeztetések megjelenítésére és más kéretlen tevékenységekre is. Gyakran "drive-by-downloads" útján terjednek.

Ransomware fajtái I.

- Fájltitkosító ransomware: Ez a ransomware változat főként trójai vírusok, email mellékletek, népszerű programok (Adobe Flash, Microsoft Office...stb) sebezhetőségeit kihasználva terjed. A rendszerbe jutva gyors sebességgel megkeresi és titkosítja a személyes fájlokat.
- Nem titkosító ransomware: Ez a típusú ransomware a teljes rendszert lezárja. Valamilyen bűnüldöző hatóság üzenetének adja ki magát (FBI, CIA, Nemzeti Nyomozó Iroda, Rendőrség) megkeresi az illegális fájlokat (torrentről vagy egyéb fájlmegosztó oldalról származó fájlok). Megtalált fájlokat mind bizonyítékként sorolja fel. Továbbá tájékoztatja az áldozatot arról, hogy ha nem fizeti ki a követelt büntetést, akár börtönbe is kerülhet.

Ransomware fajtái II.

 Böngészőlezáró ransomware: Egy Javascript segítségével egyszerűen blokkolja a böngészőket, és figyelmeztető üzenetet jelenít meg. Többnyire illegális tevékenységeket sorol fel, és a börtönbüntetés elkerülése érdekében büntetés megfizetését kéri.

Ransomware példák

WannaCry féreg - 2017. május

- Windows operációs rendszer EternalBlue nevű biztonsági résén keresztül (is) támad.
- Titkosítja az adatokat, Bitcoin-ban kéri a váltságdíjat.
- A sérülékenységeket kihasználó kód (EternalBlue kódnéven) a ShadowBrokers néven ismertté vált csoport által került ki az Internetre 2017. április 14-én, és a Microsoft március 14-ével javította az MS17-010 javítócsomag részeként.
- Az első jelek leginkább egy spear-phishing kampányra utalnak, amelyben JavaScript és PowerShell kódot alkalmazó makrókkal ellátott MS Office dokumentumot terjesztenek csatolmányként.

Ransomware példák

Petya - 2016. március végén jelent meg

- A támadó egy hitelesnek tűnő e-mailt küld, ami állásra való jelentkezésnek tűnik. Ebben útmutató is van a kapcsolódó önéletrajz letöltéséhez, egy Dropbox-fiókon keresztül.
- Az önéletrajz a ransomware, amely azonnal tönkreteszi a bootrekordot, és kikényszeríti az összeomlást. Az újrainduláskor egy üzenet jelenik meg, amely szerint hibajavításokra van szükség, a folyamat több órába telhet. Ekkor a teljes meghajtót titkosítja a kártevő. A következő rendszerbetöltés alkalmával már a szomorú üzenet várja a felhasználót: fizessen váltságdíjat a Tor böngészőn keresztül, vagy mindene oda van. A váltságdíj hét nap után duplázódik.
- Átveszi az uralmat a rendszerbetöltési folyamat fölött, és a teljes gépet zárolja. Saját magukat nem terjesztik, a megtámadott rendszerben komoly problémákat okozhatnak.

NE fizesse ki a követelt váltságdíjat, mert ez nem segít.

Fizikai sérülés

- A büntető rutin fizikai eszközöket károsít meg.
- Csernobil vírus nemcsak az adatokat károsítja, de megpróbálja újraírni a BIOS kódot. A rendszer addig használhatatlan, míg a BIOS chip nincs újraprogramozva vagy kicserélve.
- Stuxnet féreg ipari működtető rendszert céloz meg. A féreg az eredeti rendszer kódját módosítja, mely a berendezés meghibásodását eredményezi.

Logikai Bomba

- Logikai bombák, mint büntető rutinok egy adott feltétel teljesülésével vagy valamely esemény bekövetkeztével "robbannak" (hajtják végre rutinjukat).
- Indíték: Bizonyos fájlok megléte vagy hiánya, valamely dátum vagy a hét valamely napjának bekövetkezte, vagy egy szoftver verzió konfigurálása, vagy valamely speciális felhasználó belépése stb.
- "Robbanás": adatok vagy teljes fájlok módosítása vagy törlése, rendszer leállása, illetve más károk okozása.

Büntető rutin: Támadó ügynökök

Támadó ügynökök

- Büntető rutin: A kártékony kód (vírusok, trójaiak) módosítja a rendszert úgy, hogy a támadó irányítása alá vehesse, használhassa annak erőforrásait.
- A számítógépet zombie számítógépeknek hívjuk.
- A zombi számítógépek hálózatba kötve, koordináltan működhetnek. Ezt a hálózatot botnetnek nevezzük.
- Ezek a büntető rutinok a fertőzött rendszer integritását és rendelkezésre állását támadják.

Zombik használata I.

- Elosztott szolgáltatásmegtagadással járó támadás (Distributed denial-of-service (DDoS)): A DDoS támadás számítógépes rendszerekre vagy azok hálózatára irányul, azzal a céllal, hogy azok szolgáltatását teljesen vagy részlegesen megbénítsa, eltérítése a helyes működési módjától.
- Spam-ek küldése: Botnet zombik ezrei segítségével komoly mennyiségű kéretlen e-mailt lehet kiküldeni.
- Forgalomfigyelés: Zombikat a hálózati forgalom megfigyelésére is használhatjuk. Figyelik a rajtuk átmenő érdekes nyílt üzeneteket. Érzékeny információk megszerzése a cél (pl. felhasználói nevek és jelszavak).
- Billenytűzetfigyelés: A fertőzőtt gépek figyelik a billyentyűzet használatát és kinyerik az érzékeny adatokat.
- Kártékony programok terjesztése: Botnetek alkalmasak új botok terjesztésére, melyek képesek valamely új fájl HTTP-n, FTP-n keresztül történő letöltésére, majd futtatására:

Zombik használata II.

- Reklámok elhelyezése: Botnetek alkalmasak pénzszerzésre is. Vegyünk egy hamis Web site-ot, mely rengeteg reklámot tartalmaz. Vannak cégek, melyek fizetnek a reklámok megjelenítése, illetve a rájuk történő kattintások után. A támadók zombi gépekkel oldalakat látogattatnak és klikkeltetnek. Fejlesztett változat: a bot eltéríti a böngésző kezdőoldalát, így minden egyes alkalommal, ha a böngészőt megnyitják, gyűjtik a látogatottságot, klikkeket. Az adware-ek általában kapcsolódó eszköztárakat, más adware-eket és egyéb nemkívánatos, harmadik felektől származó programokat is hirdetnek. A felhasználók internetes tevékenységeinek megfigyelése, az érdeklődési körök, a leggyakrabban látogatott weboldalak, a beírt adatok stb. begyűjtése. A megfigyelt adatokat távoli szerverre továbbítják.
- Online szavazások/játékok manipulálása: Mivel minden botnak saját IP címe van, minden egyes szavazat számít?

Büntető rutin: Információszerzés

- A kártékony program a fertőzött gépeken tárolt adatokat gyűjti össze, melyeket a támadó felhasznál.
- Az adatok bizalmasságát támadják.
- Kategóriák:
 - Hitelesítő adatok (credential) ellopása, billenytűzetfigyelés, kémprogramok
 - Adathalászat és személyazonosság ellopása
 - Felderítés, kémkedés

Hitelesítő adatok (credential) ellopása, billenytűzetfigyelés, kémprogramok

- Billentyűzetfigyelők összegyűjtik a billentyűlenyomásokat, hogy a támadó érzékeny adatokat szerezzen be.
- Mivel az összes szöveget begyűjtik, szükséges egy "beépített" szűrő, mely csak a megadott kulcsszóhoz kapcsolódó adatokat továbbítja.
- Néhány bank alkalmazás átállt a grafikus appletek alkalmazására.
- Válaszul a támadók általánosabb kémprogram büntető rutint használnak: böngésző előzmények figyelése, web oldalak éltérítése a támadó által kontrolláltakra, és a böngésző és bizonyos web oldalak között kicserélt adatok dinamikus változtatása.
- Valamennyi személyes adatok megszerzésére irányulnak.

Adathalászat és személyazonosság ellopása

- A felhasználó belépési adatainak megszerzésére irányuló másik megoldás, egy a támadó által kontrollált web oldalra mutató link elhelyezése egy kéretlen e-mailben.
- Ez általában valamilyen sürgős üzenetben jelenik meg, mely a felhasználói fiók aktiválására kér.
- Adathalászat: pszichológiai támadással kihasználják a felhasználók bizalmát úgy, hogy valamely megbízható felet személyesítenek meg.

- A támadó bizonyos típusú információt szeretne megtudni.
- Operation Aurora 2009-ben egy trójait használt, hogy hozzáférjen (esetlegesen módosítsa is) high tech és biztonsági cégek forráskódjaihoz.
- A Stuxnet féreg 2010-ben összegyűtött számos hardver és szoftver konfigurációk részleteit, hogy meghatározza hogy tudná -e a célpontokat támadni.
- Célzott adathalászattal ipari kémkedéseket vagy más felderítéseket végeznek.

- Komolyabb változata: célzott adathalászat(spear-phishing) attack). Leveleket küldenek, egy olyan cég/személy nevében, akiben a címzettek megbíznak.
- Talán 5-10 jól kiválasztott embernek küldik csak ki, a támadók tanulmányozzák a kiszemelt célpontokat, mint pl. azok LinkedIn vagy Facebook fiókjainak átolvasásával, vagy az általuk nyilvános blog-okon, fórumokon közölt üzeneteik vizsgálatával.
- Egy nagyon testre szabott levelet készítenek, amely az érintett célpontok számára relevánsnak tűnhet. Így az egyének nagyobb valószínűséggel válnak a támadás áldozataivá.
- A támadó kifejezetten a felhasználót, vagy a cégét akarja támadni, bizalmas információkhoz igyekeznek hozzáférni, mint pl. a cég üzleti titkai, az érzékeny technológiai tervek, vagy bizalmas kormányzati kommunikáció. Lehet hogy egy másik embert/céget akarnak elérni rajtunk keresztül:

Büntető rutin: Lopakodás

Lopakodás: Hátsóajtó (Backdoor)

- Lopakodó büntető rutinok: A kártékony programok azon rutinjai, melyekkel elrejtik jelenlétüket és hozzáférésüket a fertőzött gépeken.
- Ez a rutin a rendszer integritását célozza.
- Hátsóajtó: A program egy titkos belépési pontja, mely lehetővé teszi, hogy a belépési pont ismerője a biztonságos hitelesítés nélkül kapjon hozzáférést.
- Programozók legálisan használták a hátsóajtókat program tesztelésre. A hátsóajtók veszélyessé válnak, ha a tisztességtelen programozók illetéktelen hozzáférésre használják.
- A védelmi intézkedések szoftverfejlesztésekre és szoftver updatekre irányulnak.



Lopakodás: Gyökércsomag (Rootkit)

- A gyökércsomagok egy programcsomag, mely installálása után fedett hozzáférést biztosít, tart fent a már fertőzött géphez adminisztrátori (root) jogosultságokkal. Hátsóajtó hozzáférést biztosítanak trójaiak számára úgy, hogy fontos rendszer fájlokat módosítanak.
- Az operációs rendszer valamennyi funkciójához és szolgáltatásához hozzáférést ad.
- Adminisztrátori jogosultsággal, a támadónak teljes kontrollja van a rendszer felett, felrakhat, módosíthat programokat, fájlokat, processzeket monitorozhat, küldhet, fogadhat hálózati forgalmat és hátsóajtó hozzáférést kaphat.
- A gyökércsomag elrejti ezeket a mechanizmusokat.



Gyökércsomag jellemzői

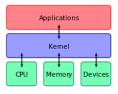
- Perzisztens: A gyökércsomag perzisztens helyen tárol kódot, pl. registry-ben és a kódot a felhasználó részvétele nélkül futtatja le.
- Memória alapú: Nincs perzisztens kód, tehát újraindítást nem éli túl. Mivel csak a memóriában van, nehezebb detektálni.

Gyökércsomag jellemzői

- Felhasználói (user) módú: Felhasználói szinten működik az operációs rendszerben. Lehallgatja az API hívásokat és módosítja kapott választ. Pl. ha egy alkalmazás egy könyvtár listázását kéri, a lista, amit megkap nem tartalmaz olyan bejegyzéseket, melyek a rootkittal kapcsolatos fájlok beazonosítását segítik.
- Kernel módú: A gyökércsomag úgy rejti el jelenlétét, hogy módosítja a kernelt.

Kernel módú rootkitek

- A rendszermag (kernel) az operációs rendszer alapja (magja), amely felelős a hardver erőforrásainak kezeléséért (beleértve a memóriát és a processzort is).
- A korai rootkitek felhasználói módúak voltak. A változtatásokat detektálni lehetett kernel kódokkal.
- A következő generációs rootkitek egy szinttel lejjebb kerültek, kernel szintű változtatásokat hajtottak végre.
- A felhasználói szintű programok a kernellel rendszerhívásokon keresztül teremt kapcsolatot. A kernel szintű rootkitek rejtőzködéséhez az elsődleges célpontok a rendszerhívások.





00000000000000**0000000**000000000

Kernel módú rootkit technikák

- Linux esetében minden egyes rendszerhíváshoz egy azonosító van rendelve.
- A kernel egy rendszerhívási táblázatot kezel, minden egyes rendszerhíváshoz tartozik egy rekord. Minden rekord tartalmaz egy a megfelelő rutinra mutató mutatót.
- Három technika:
 - Rendszerhívási tábla módosítása: A támadó a tárolt rendszerhívások címeit módosítja, átirányítva a rendszerhívás mutatóját a legális rutinról a rootkit rutinjára.

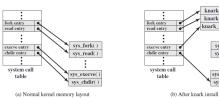


Figure 6.4 System Call Table Modification by Rootkit



knark_fork()

knark execve(

sys fork()

sys read()

svs execve()

svs chdir(

00000000000000**00000000**0000000000

Kernel módú rootkit technikák

Másik két technika:

- Rendszerhívási tábla célpontainak módosítása: A támadó a legális rendszerhívási rutint írja felül a kártékony kóddal. A tábla nem változik.
- Rendszerhívási tábla átirányítása: A támadó a rendszerhívási táblára vonatkozó hivatkozásokat átirányítja egy másik kernel memóriabeli táblára.

Biztonsági intézkedések

Biztonsági intézkedések: Megelőzés

- Valamennyi biztonsági intézkedést "antivírus" mechanizmusnak hívunk, mivel elsőnek tipikusan a vírusok írtására jöttek létre.
- Ideális megoldás: megelőzés. Elsőnek ne engedjük, hogy a kártékony program a rendszerünkbe bejusson. Ha bejutott, blokkljuk, ne módosíthassa a rendszert.
- Férgek, vírusok, trójaiak terjedésének megelőzése:
 - **Sérülékenység csökkentése**: Összes javítócsomag (patch) alkalmazása, a felszínre került programhibák orvosolására.
 - Fenyegetés csökkentése: A rendszer adataihoz, fájljaihoz megfelelő hozzáférés-vezérlés beállítása.
- Pszichológiai támadás megakadályozható megfelelő felhasználói felvilágosítással és oktatással.



Pszichológiai támadás

 A UK Payment Council nem rég jelentette be, hogy a 2010-es évben elkövetett online banki csalások 22%-kal csökkentek annak ellenére, hogy az adathalászattal kapcsolatos visszaélések 21%-kal növekedtek a vizsgált időszakban. A helyzet változott. A pénzügyi szektornak hét évébe telt egy új védelmi rendszer kifejlesztése a phishing vagy trójai típusú social engineering támadások ellen.

- Külső adatmentés, szalagos mentés: offline, szalagos mentési rendszer esetén a lementett adatokat a szalagos technológiából fakadóan a zsaroló vírus nem képes titkosítani, TÁROLJUK a havi mentéseket fizikailag is biztonságos külső helyen.
- Folyamatos frissítések, többrétegű vírusvédelem: többrétegű védelemmel ellátott vírusírtó, frissítése, tűzfal
- Szabályozás kialakítása és betarttatása
- Oktatás, tudatosítás: Ismeretlen feladótól érkezett e-mailekben ne nyissuk meg a mellékletet, főleg ha ez tömörített állomány. Munkahelyünkön figyelmeztessük azon kollégáinkat a veszélyekre, akik főleg külső irányból kapják leveleik többségét (pl. pénzügyi vagy HR osztály). A felhasználóknak ismerniük kell a vírus működését és terjedését, valamint azokat a technikákat, amelyeket a kártékony kód alkalmaz.

Ha a megelőzés nem sikeres:

- Detektálás: Ha a kártékony kód már megfertőzte a rendszert, határozzuk meg a helyét.
- Azonosítás: Ha detektáltuk, azonosítsuk be a kártékony kódot, mely megfertőzte a rendszerünket.
- Eltávolítás: Ahogy azonosítottuk, távolítsuk el a kártékony kód nyomait valamennyi fertőzött állományból, hogy ne terjedjen tovább.

Ha sikerült detektálni, de se azonosítani, se eltávolítani nem tudjuk, akkor töltsünk be a tiszta backup verziót.

Antivírus szoftver I.

Négy generáció:

- Első generációs: egyszerű szkennerek: a kártékony program valamennyi másolatában ugyanaz a struktúra és bitminta kell, hogy legyen. Másik típus a program állományok méretét tárolja és figyeli azok változását.
- Második generációs: heurisztikus szkennerek: A szkenner a kártékony kódhoz kapcsolható programkód részleteket keresi. (pl. polimorf vírusok esetén a titkosítási részből próbálják kinyerni a kulcsot. Másik megoldás az adatintágritás vizsgálata. Egy ellenőrzőösszeg (hash vérték, MAC) adható meg minden egyes programhoz. Ha a kártékony kód módosítja a programot az ellenőrzőösszeg változtatása nélkül, akkor a változás detektálható. A kulcs külön tárolandó.

Antivírus szoftver II.

- Harmadik generációs: aktivitást figyelők: olyan programok, melyek a kártékony kód tevékenységét figyelik, nem a fertőzött programbeli struktúráját. Elegendő néhány tipikus kártékony kód tevékenységet felismerni.
- Negyedik generációs: teljes védelem: Ezek a programcsomagok többféle antivírus megoldást alkalmaznak.
- Fejlett antivírus szoftverek: általános visszafejtés (generic decryption (GD)): Ha egy polimorf vírust tartalmazó fájlt futtatunk, a vírusnak vissza kell fejtenie magát. Az általános visszafejtő szkenner detektálja ezt.

Antivírus szoftver III.

Fejlett antivírus szoftverek: Viselkedés-blokkoló szoftver

- Viselkedés-blokkoló szoftver valós időben figyeli a kártékony programok működését és megpróbálja blokkolni mielőtt komoly károkat okoz.
- A következő eseményeket figyeli:
 - Fájlok módosítására, törlésére, megnyitására irányuló próbálkozások;
 - Merevlemez formatálása vagy más javíthatatlan művelet;
 - Indítási beállítások módosítása;
 - Futtatható tartalmak küldése e-mailen vagy messenger-en keresztül;
 - Hálózati kommunikáció kezdeményezése;
- A kártékony kód már el kezdi működését mielőtt a tevekénységét detektáljuk.



Antivírus szoftver IV.

Rootkit védelmi intézkedések:

- A gyökércsomagokat nehéz detektálni és megsemmisíteni főleg, ha kernel módúról van szó.
- Javítócsomagok (patch), update-k használata. Admin jelszavak megváltoztatása.
- Ha egy kernel szintű rootkitet detektálunk az egyetlen és megbízható megoldás, ha teljes operációs rendszert újrarakjuk.