NAGY ZOLTÁN ANDRÁS – MEZEI KITTI

A ZSAROLÓVÍRUS ÉS A BOTNET VÍRUS MINT NAPJAINK KÉT LEGVESZÉLYESEBB SZÁMÍTÓGÉPES VÍRUSA

1. Bevezetés

Napjaink a számítógép felhasználási lehetőségek bővülésével a különböző rosszindulatú programok (malware-ek, pl. vírusok) átalakultak. Új célok érdekében, új felhasználási formára születnek. Az Internet lehetőségei teremtik meg, hogy a vírusok kifejhessék nemkívánatos hatásukat és azt, hogy robbanásszerűen elterjedhetnek a világhálón. A tanulmányban két különösen veszélyes malware-fajtával kívánunk foglalkozni, az egyik a napjainkban elterjedt zsarolóvírusokat, illetőleg a számítástechnikai rendszerek (pl. akár kritikus infrastruktúrák) működésének megakadályozására, megbénítására alkalmas terheléses támadáshoz szükséges botnet-vírusokat mutatjuk be, egyben felhívva a figyelmet számítógépeink sebezhetőségére, a védekezés szükségességére.

2. A túlterheléses támadásokról általában

A túlterheléses, avagy szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételére – innen a szolgáltatásmegtagadással járó elnevezés is -, amelynek a leggyakoribb formája a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövekedett adatforgalommal.[1]

Az elnevezés a támadás angol megfelelőjének rövidítéséből ered, amely során az említett támadás egyetlen számítógéptől származik, több közbeiktatott gép nélkül: Denial of Service (rövidítve: DoS). Amennyiben a támadás összetettebb, mert összekapcsolt rendszerek csoportjától, egyszerre sok – lehetőleg minél több - helyről indul, akkor használatos a Distributed Denial of Service (rövidítve: DDoS), vagyis az elosztott szolgáltatásmegtagadással járó támadás elnevezés. Ebben az esetben feladatot nem egyetlen eszköz végzi el, mint a DoS-támadásnál, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő – eszközök (pl. asztali gépek, mobiltelefonok, vagy routerek stb.) párhuzamosan.[2]

A technikai alapja leegyszerűsítve a következőképpen néz ki: amikor a felhasználó az Internethez kapcsolódik, akkor egyben az ún. hozzáférést biztosító szolgáltató szerveréhez is, amellyel adatcsomagokat váltanak egymással. Közben megtörténik

[1] http://www.cert-hungary.hu/ddos [2017.01.06.]; Kezdetben 100 Gbps támadások voltak megfigyelhetők, napjainkra ez már a 300 Gbps-ot is meghaladhatja, sőt állítólag 600 Gbps támadásra is sor került és ezek 24 óránál tovább is tarthatnak. Europol: The Internet Organised Crime Assessment. 2016. 35. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Letöltés ideje: 2017.01.11.)

[2] Gyányi Sándor: Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem. PhD értekezés. Budapest, 2011. 88. o.

mindkettőjük azonosítása (ügyfél személye, jogosultsága, a keresett weboldal azonosítása, a szerver azonosítása stb.), majd ez a szerver a keresett weboldal szerverére irányítja a felhasználót. A támadás esetében pedig a célzott szerverre – egyszerre – ezer-, vagy tízezer számra érkeznek adatcsomagok, amelyekre a szervernek – időrendi sorrendben – válaszolni kellene. A DDoS-támadás során a támadó egy hálózatot alkotó számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, azoknak válaszolására, ezzel akár a rendszer teljes leállását is eredményezhetik, azonban a funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik.[3]

A felhasználó tudta nélkül megfertőzött számítógépeket, amelyek távolról irányíthatók „zombi"-nak nevezik. Másik elnevezésük a robot és network szavak összevonásából eredő „botnet", amely a több bot összekapcsolásával keletkezett hálózatot jelenti. A botnet irányítóját, aki kiosztja a feladatot a fertőzött eszközöknek, „botmaster"-nek, illetve több irányító esetén „botherder"-nek hívják. A botnet tagjait a fertőzött zombi számítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnet-akciókat „controller"-nek hívjuk. A controller általában az ún. „drop server"-re csatlakozik, amely a botnet által gyűjtött adatok tárolására szolgáló tárhelyet jelenti, ami hozzáférhető a botnet tagjai és a botmaster részére is. A botmaster és botnet közti kapcsolatot és az utasítások eljuttatását biztosító kommunikációs útvonal az ún. Command&Control (C&C) csatorna.[4] A botnetek alkalmasak a DDoS támadások indításán kívül spamküldésre, adathalászatra,[5] hálózat-figyelésre, billentyűzet-figyelésre, illetve az internetes reklámokhoz a klikkelések begyűjtésére.

Bármely felhasználó számítógépe bármikor válhat könnyedén „zombigéppé". A számítógépek a számítógépes hálózatra történő csatlakozással már ki vannak téve a veszélynek, a kockázat pedig különösen megnövekedett az új mobilinformatikai és Internet of Things (IoT)[6] eszközök elterjedésével, főleg azért, mert utóbbinak még nincs megfelelően biztosított informatikai védelme és a többségük magánszemélyek használatban van, akik a biztonsági frissítésekkel hajlamosak nem foglalkozni.[7]

Az első bot, 1999-ben PrettyPart féreg néven jelent meg, ami egy IRC (Internet Relay Chat) szerverhez csatlakozva távolról vezérelte a fertőzött számítógépeket. Napjainkban a botnetek a technológiai fejlődésnek köszönhetően már megosztott hálózatokon, fájlmegosztó rendszereken, peer-to-peer (P2P) hálózatokon, HTTP

[3] Nagy Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (szerk.): Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. 2016. 487. o.

[4] Gyányi: i.m. 89. o.

[5] A botnetek képesek nagy mennyiségű személyes vagy egyéb titkos adat megszerzésére. Általában jól ismert cégek – főleg bankok, pénzintézetek – nevében e-mail üzeneteket küldenek, melyekben azt kérik a felhasználótól, hogy lépjen be elektronikus úton fiókjába. A levél általában egy linket is tartalmaz, hogy az áldozat könnyebben eljuthasson a honlapra. A link azonban nem a cég weblapjára mutat, hanem egy ahhoz kísértetiesen hasonlító – esetleg kívülről nem is megkülönböztethető – ál-honlapra, mely többnyire a botnet valamely tagján fut.

[6] http://www.digitalhungary.hu/e-volution/Mi-is-az-az-IoT/2202/ (Letötlés ideje: 2017.01.05.): „Az 'Internet of Things', vagy rövidítve 'IoT' magyarul a 'dolgok (tárgyak) internete', mellyel a mindennapjainkban használt eszközök (például háztartási gépek, autók, mérőórák, pénztárgépek, stb.), az interneten keresztül is elérhetőek, és képesek egymással akár önállóan is kommunikálni. Ennek a kommunikációnak a motorja az ún. M2M (machine-to-machine) technológia, ami olyan adatáramlást jelent, mely emberi közreműködés nélkül, gépek között zajlik. A kommunikáció minden olyan gép között létrejöhet, amely a megfelelő technológiával (érzékelőkkel, chipekkel) van ellátva ahhoz, hogy bekapcsolható legyen a rendszerbe."

[7] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (Letötlés ideje: 2017.01.05.)

weblapokon, illetve akár közösségi oldalakon mint a Facebook, Twitter, Reddit-en keresztül is terjedhetnek.

Új trendként jelent meg, hogy a DDoS támadások könnyű indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, szoftvereket mint egy szolgáltatásként bérelni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5 $ és 1000 $ közötti áron -, vagy akár vásárolni lehet manapság a fekete online piacokon és fórumokon keresztül (pl. Alphabay és Exploit), amik az ún. Deep Weben keresztül érhetőek el és közös jellemzőjük, hogy nehezen lenyomozhatók. A hackerek gyakran nem egyértelműen hirdetik a szolgáltatásukat, hanem a „stressers" vagy „booters" elnevezést használják. A szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, mert csak a célpontot kell kiválasztaniuk, egy egérkattintás az egész, sőt sokszor a végrehajtáshoz technikai segítséget is kapnak. Ezek a szolgáltatások és eszközök kiberfegyvernek minősülnek, ezért velük szemben szigorú és azonnali fellépés szükséges, különösen figyelembe véve az egyre növekvő népszerűségüket és széleskörű elérhetőségüket.[8]

Érdemes felhívni a figyelmet a hazai helyzetre. A magyarországi botnet fertőzöttségre figyelmeztető 2015-ös Symantec tanulmány szerint Magyarország a bot fertőzött számítógépek számát tekintve a 6. legfertőzöttebb ország a világon – Kína, USA, Tajvan, Törökország és Olaszország előz meg minket – és 2. helyet foglalja el az európai országok között.[9]

3. A túlterheléses támadások motivációja

A túlterheléses támadásokat sokszor anyagi haszonszerzés céljából indítják. Ezeket a támadásokat egyre többször zsarolás vagy ún. „védelmi pénz" követelése során használják fel, amit az áldozatoktól online fizetés - általában Bitcoin - formájában követelnek. Az elkövetők gyakran olyan cégek weblapjait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. online casinok, energia-, pénzügyi szféra).

2016-ban az Europol sikeres akciót hajtott végre és letartóztatta a zsarolásokban élen járó DD4BC Team hacker csoportnak a kulcsfontosságú tagjait, akik számos DDoS támadást indítottak európai cégekkel szemben.

Az általuk alkalmazott zsaroló séma a következőképpen néz ki: felmérik a célpont hálózati sérülékenységét, majd kisebb DDoS-támadásokat indítanak a céggel szemben, ezt követően a további támadások indításának elkerülése érdekében Bitcoin formájában fizetséget kérnek a cégtől. Abban az esetben, ha az áldozat ennek a követelésnek nem tesz eleget, akkor további, erőteljesebb támadásokat indítanak a cég weblapjával szemben, amely annak a teljes elérhetetlenségéhez is vezethet. Azonban nem javasolt, hogy fizessenek a zsarolóknak, mert a támadók célja a haszonszerzés, valamint nincs garancia fizetség esetén sem a támadás elkerülésére. DD4BC csapatnak a módszere egyre elterjedtebbé vált és már „copycat" hacker csoportok is megjelentek, akik másolják őket.[10]

[8] James Scott–Drew Spaniel: Rise of the machines: The DYN attack was just a practice run. 2016. 7-12. o.
[9]https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf (Letötlés ideje: 2017.01.05.)
[10] https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 (Letöltés ideje: 2017.01.18.)
http://news.softpedia.com/news/members-of-dd4bc-the-group-that-blackmailed-companies-with-ddos-attacks-arrested-by-Europol-498797.shtml (Letöltés ideje: 2017.01.18.)
http://neih.gov.hu/zsarolo-ddos (Letöltés ideje: 2017.01.21.)

Az anyagi haszonszerzésen kívül gyakori a gazdasági célzat, ami az üzleti versenytársak technológiai folyamatai ellen intézett támadásokban nyilvánul meg. A támadók általában tudatosan, jól időzítve olyan időpontokat választanak a támadásokhoz, amikor az adott cég nagyobb bevételre számíthat - így nagyobb kárt is tudnak okozni - pl. ilyen a Cyber Monday, Black Friday vagy a karácsony. A weboldalak működésének a megszakítása költséges terhet jelent bármely weboldal üzembentartójának legyen szó kis- és középvállalkozásról vagy nagyobb cégről. A támadással járó pénzügyi veszteség esetenként különbözhet és nem kizárt, hogy az adott vállalkozás működésére hosszútávon is hatással lehet. Ez megnyilvánulhat a kieső és pótolhatatlan bevételben, illetve akár presztízsveszteséget is okozhat, mivel az ügyfelek nem tudják elérni a támadással célzott cég honlapját, sem igénybe venni a cég által kínált szolgáltatást, ezért inkább a konkurens vállalkozásokat választják és lemorzsolódnak az adott cégtől (pl. a pénzügyi ágazaton belül, különösen az értéktőzsde, értékpapír kereskedés piacán ez pillanatok alatt súlyos és hatalmas kárt okozhat).[11]

A túlterheléses támadások hátterében politikai vagy ideológiai indíttatás is állhat, amit az ún. hacktivizmus elnevezéssel illetek. A hactivista nem egy csalárd hacker, aki személyes információkat szeretne megszerezni vagy egyéb kárt okozna, hanem tevékenységével az a célja, hogy felhívja a figyelmet valamely fontos politikai vagy társadalmi ügyre. Számára a hacktivizmus egy Internet által biztosított stratégia, amely lehetővé teszi a polgári engedetlenség gyakorlását (pl. DDoS támadások indításával, a weboldal felülírásával azaz „defacement”-tel, adatlopással, illetve azok későbbi nyilvánosságra hozatalával, vagy egyéb virtuális szabotázs akciókkal).[12]

Az egyik legismertebb hacktivista csoport, az Anonymous[13], akiknek a támadásai rendszerint valamilyen közös ügyet szolgálnak. A csoport nevében intéztek már támadást amerikai, izraeli, tunéziai és ugandai kormányszervezetek weblapjai, gyerekpornográf tartalmú oldalak, szélsőségesen rasszista szervezetekkel szemben (mint például a Westboro Baptist Church), de nagyvállalatok is váltak már célpontjukká. A másik ismert csoport a LulzSec, akiknek hasonló támadásaik voltak ugyanúgy kormányzati (pl. CIA webszervere ellen intézett túlterheléses támadás) és nagyvállalati rendszerek ellen (pl. a Sony Playstation online szolgáltatásait tették elérhetetlenné, illetve több százezer regisztrált felhasználó adatait, fontosabb rendszerleírásokat tették nyilvánossá).[14] További példa a politikai célzatú támadásokra az USA elnök választásának kampány időszaka, amikor Trump és Clinton oldalait sorozatos támadások érték. Magyarországi érintettségű ügy is volt, amikor a Belügyminisztérium kormányzati rendszereinek az egyes nyilvánosanan elérhető szolgáltatásait jelentős mértékű túlterheléses támadás tette időszakosan elérhetetlenné.[15]

[11] Urcuyo: i.m. 302-303. o. Forrás: http://hirek.prim.hu/cikk/125744/ (Letötlés ideje: 2017.06.23.)
[12] https://www.techopedia.com/definition/2410/hacktivism (Letötlés ideje: 2017.01.21.)
[13] Török Szilárd: Anonymous a világban és Magyarországon. Felderítő Szemle. 2014. március XIII. évfolyam I. szám. 192. o.: Az Anonymous egy nemzetközi hacker csoport, amely formálisan 2003-tól létezik és 2008 óta indít támadásokat. Több, egymástól független sejtből áll, a világ számos országában vannak aktivistái. A csoport megalakulását a „4chan” internetes oldalhoz kötik.
[14] Török: i.m. 196. o.
[15] www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast (Letöltés ideje: 2017.01.21.)

4. A zsarolóvírusokról általában

A malware-t[16] zsarolási célzattal már az 1990-es években használták. A zsarolóvírusok megjelenése az otthoni számítógépek elterjedésével egyidős: 1989-ben floppy lemezen érkezett az első hasonló kártevő. Joseph Popp biológus programot írt, amely címében az AIDS-re vonatkozó információkat tartalmazta. Ez azonban valójában egy "trójai faló" program volt. Az "AIDS Information Disk" számítógépbe történő betöltése után arra szólította fel a felhasználót, hogy küldjön pénzt egy privát panamai postafiók címére. Ennek fejében Popp küldött (volna) egy újabb szoftvercsomagot. Ellenkező esetben a lemezen rögzített program 90. hozzáférést (újraindítást) követően tönkreteszi, pontosabban a felhasználó számítógépében rögzített adatállományát titkosítja. Az inkriminált lemezeket Popp angliai és panamai címekről 20 ezer (!) címzettnek küldte el, amelyekből Magyarországra is érkezett két (?) lemez.[17]

A zsarolóvírus (ransomware) modern változata már online terjed, az elővigyázatlan felhasználók telepítik számítógépeikre. A program a számítógépen levő adatállományt letitkosítja, így a felhasználó nem fér adataihoz, könyvtáraihoz. A titkosítás feloldását pénzösszeg megfizetésétől teszi függővé. Az elkövető kilétének megismerése szinte lehetetlen, hiszen a „váltságdíjat" virtuális valutában, Bitcoinban vagy valamely altcoinban kéri. A pénz kifizetése sem garancia arra, hogy a zsaroló a titkosítást feloldja. De előfordulhat, hogy a váltságdíj fejében titkosított adatállomány egyrészét teszi ismét elérhetővé, majd további követelésekkel áll elő. Az elkövetők célja az anyagi haszonszerzés, ezért általában ezek nem célzott támadások, azonban 2016-ban megfigyelhető volt egy tendencia, amely során sorozatos támadások a kórházakat érintette. Például a Hollywood Presbyterian Hospital Medical Center 17 000 $ értékű Bitcoint fizettet ki, mert a vírus napokig megbénította a kórház működését. Részben ennek a támadásnak köszönhető, hogy Kalifornia állam Büntető törvénykönyvébe önálló bűncselekményként jelent meg a ransomware felhasználása.[18] A magánvállalkozások, amelyek nagyobb összeget is képesek fizetni, könnyedén válhatnak szintén a zsarolóvírusok áldozataivá.

2017-ben a WannaCry zsarolóvírus söpört végig a világon, amely a Windows sebezhetőségét használta ki. A vírus e-mailek mellékleteiben és fertőzött linkek megnyitásával terjedt, s azért tudott ilyen léptékben rendszereket megfertőzni, mert féregként viselkedve egy lokális hálózatban elég volt, ha egyetlen felhasználó óvatlanul rákattintott a fertőzött fájlra, és máris átterjedt a rendszer többi gépére is. A legrosszabb helyzet Nagy-Brittanában volt, ahol a National Health Service gépeit teljes egészében blokkolta a vírus. Oroszországban a Belügyminisztérium, és a Sperbank volt érintett, míg Németországban a Deutsche Bahn vasútvállalat gépeit támadták, a kijelzőkön megjelent a

[16] A malware gyűjtőfogalom, e körbe vonhatók a vírusok (rootkitek, trójai, zsarolóvírusok), „férgek", logikai bombák és más kárt okozó programokat, illetőleg a spyware-eket, mint kémprogramokat, ezek azok a programok, amelyek a számítógépes munkafolyamatot, elektronikus adatot, a számítástechnikai eszközöket károsítja. A malware kifejezés valamilyen rosszindulatú programot jelent, amely a malicious software angol szavak összetételéből származik.

[17] http://www.origo.hu/techbazis/20170421-floppyn-erkezett-a-vilag-elso-zsarolovirusa.html (Letöltés ideje: 2017.05.21.)

[18] https://www.barkly.com/hospital-ransomware-healthcare (Letöltés ideje: 2017.05.21.)
https://blog.barkly.com/hospital-ransomware-attacks (Letöltés ideje: 2017.05.21.)
https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/ (Letöltés ideje: 2017.05.21.)

vírus üzenete. Az Egyesült Államokban a FedEx csomagküldő cég gépei váltak a vírus áldozataivá.[19]

5. A hazai szabályozás

Az Európai Unióban az Európai Parlament és Tanács 2013/40/EU irányelve hívta fel először a figyelmet a botnetekre mint kiemelt veszélyforrásokra. Általuk egyre veszélyesebb, ismétlődő és átfogó támadásokat tudnak végrehajtani, melyek gyakran kulcsfontosságú információs rendszereket is érintenek. Az irányelvnek megfelelően a magyar Büntető Törvénykönyv - 2012. évi C törvény - értelmében a túlterheléses támadás végrehajtása a 423. § szerint az információs rendszer vagy adat megsértésének minősül és a 2) bekezdés szerint büntetendő, aki a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve, megváltoztat, töröl vagy hozzáférhetetlenné tesz. A minősített eset valósul meg, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint. A DDoS támadás során a támadó sok száz vagy több ezer felhasználó gépei felhasználásával kísérel meg kapcsolatot létesíteni a megtámadott számítógéppel. E sok száz vagy ezer zombigép egy botnet hálózatot alkot, amelyet a támadó vezérel. Az egyszerre küldött nagy mennyiségű adatkérés és továbbítás bénítja a támadott számítógépet és rajta keresztül az információs rendszert.[20] A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a támadást közérdekű üzem ellen követik el.

A zsarolóvírus alkalmazása esetében hasonlóan az információs rendszer vagy adat megsértése bűncselekmény valósul meg, de 2) bekezdésének b) pontja szerint büntetendő információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő és a minősített esetek ugyanúgy alakulnak, mint a túlterheléses támadásnál.

[19] http://www.hirado.hu/2017/05/15/vilagszerte-terjed-a-virusfertozes/ [2017.05.21.]

[20] Nagy Zoltán András: XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények. Magyar Büntetőjog: Különös rész. Osiris Kiadó, Budapest 2014. 598. o.