HADMÉRNÖK

X. Évfolyam 2. szám - 2015. június

SZABÓ Tibor
szabo.tibor@nbsz.gov.hu

A TERRORISTÁK MODERN ESZKÖZRENDSZERE

Absztrakt

A hírekben megjelenő kibertámadások számának növekedésére csak akkor figyelünk fel, ha már a mi rendszerünket érte támadás. A terroristákat sokan a hagyományos fegyverzetben képzelik el, miközben megtámadnak egy objektumot vagy felrobbantanak egy vonatot. Kevésbé jut eszünkbe, hogy távolról, láthatatlanul férkőzik a közelünkbe, lopja el adatainkat és teszi elviselhetetlenné hétköznapjainkat. Jelen írás arra kívánja felhívni a figyelmet, hogy a terrorizmus technikai eszköztára kibővült a számítástechnikai eszközök fejlődésének köszönhetően kifinomult, komplex eszközökkel, melyek szinte mindenki számára elérhetőek a világon. Ebből adódóan bármit és bárhonnan érhet támadás a világhálón keresztül.

We are just paying attention to the increasing number of cyber-attacks that appear in the news, if our system has come under attack. Lot of people has traditional thinking of the armed terrorists, such as they attack an object or blow up a train. We are not thinking of the possibility that they can approach far away from us and invisibly steal our data and make unbearable our daily life. This article would like to draw attention to that due to the development of sophisticated computing devices, the technical tools of terrorism enlarged with complex tools that are available to almost everyone in the world. Hence, an attack can achieve anything and from anywhere over the world wide network.

Kulcsszavak: *kiberterrorizmus**,** Botnet rendszerek, sérülékenység, árak ~ cyberterrorism, Botnet systems, vulnerability, prices*

BEVEZETÉS

A hírekben megjelenő kibertámadások számának növekedésére csak akkor terelődik rá figyelmünk, ha már kompromittálták rendszerünket, számítógépes hálózatunkat vagy számítástechnikai eszközünket. A támadások céljai között gyakran a terrorizmus jellemző jegyei is felfedezhetők. A terroristákat sokan a hagyományos fegyverzetben képzelik el, miközben megtámadnak egy objektumot, túszul ejtenek embereket váltságdíjat követelve vagy felrobbantanak egy vonatot. Ritkábban jut eszünkbe az a kép róluk, hogy távolról, láthatatlanul férkőznek a közelünkbe, lopják el adatainkat és teszik elviselhetetlenné hétköznapjainkat erőszakos akcióikkal.

Jelen írás arra kívánja felhívni a figyelmet, hogy a terrorizmus technikai eszköztára napjainkra kibővült a számítástechnikai fejlődésének köszönhetően kifinomult, komplex eszközökkel, melyek szinte mindenki számára elérhetőek, beszerezhetőek vagy bérelhetőek a világon. Ebből adódóan bárkinek az eszközrendszerét érheti támadás a legváratlanabb időben és bárhonnan a világhálón keresztül.

KÖZELMÚLT ESEMÉNYEI

A híreket hallgatva vagy az újságokat, ill. hírportálokat olvasva egyre gyakrabban találkozunk számítógépes kémkedésről, számítógépes hálózat feltöréséről ill. kibertámadásról, kiberterrorizmusról és kiberháborúról szóló cikkekkel. Valóban ilyen jelentőséggel bírnak ezek az információk vagy a média esik túlzásokba a figyelem felkeltése céljából?

Egyesek túlmisztifikáltnak érzik azt, hogy a kiberterrorizmus bárkinek az életét fenyegetné, mások attól félnek, hogy egy ilyen támadás esetén az energiaellátásunk teljes kiesésével visszaesünk a kőkorszaki életszínvonalra. Az igazság a kettő között van, valamivel közelebb az utóbbi vélekedéshez. Annak érdekében, hogy egy kibertámadás tulajdonságait, lehetséges célpontjait, ill. hatását érzékelni tudjuk, nézzünk meg néhány kiragadott példát a közelmúltból, amelyeknél olyan technikákat vagy képességeket használtak, amelyek alkalmazása könnyen előfordulhat egy esetleges terrorista támadás esetén.

Izrael „megvakította” a Szíriai légvédelmet:

2007 szeptemberében egy izraeli, légi csapásmérő erő láthatatlanul átrepült – az oroszok által szállított - Szíria komplex, légvédelmi rendszerén és lebombázott egy gyanúsnak vélt, nukleáris létesítményt, amiből a légvédelem semmit nem látott. Feltételezhető, hogy egy "Suter" nevezetű számítógépes programot használtak, amely megvakította a radar rendszert. A programot az Egyesült Királyság és az Egyesült Államok fejlesztette légvédelmi hálózat „elvakítására”.

Stuxnet és a Duqu:

A Stuxnet megjelenése nyitotta ki sokaknak a szemét azzal kapcsolatban, hogy a SCADA rendszerek és a programozható logikai vezérlők (PLC) sebezhetőek. 2010-ben öt iráni létesítmény megtámadására használták a Stuxnet-et, mellyel leginkább az urándúsítás folyamatát célozták meg. Az esemény rávilágított, hogy lehetséges biztonságosnak hitt hálózatokba beszivárogni, ott adatokat módosítani és károkat okozni fizikai eszközökben.

A Duqu-t – a Stuxnet módosított változatát - 2010-ben fedezték fel. Azzal a céllal hozták létre, hogy adatokat gyűjtsenek, továbbá távoli hozzáférést biztosítsanak egy lehetséges jövőbeni támadáshoz. [1]

Valószínűleg az amerikai és/vagy izraeli kormány alkotta meg a Stuxnet-et – feltehetően jelentős pénzügyi ráfordítással. Nem is olyan régen SCADA exploit[1]-ot hoztak létre néhány óra alatt egy laboratóriumban, amelynek költségei nem haladták meg a $ 2500 dollárt. [2]

Kína kiberkémkedés:

2010 áprilisában a kínaiak elterelték 18 perc időtartamra a világ internetes forgalmának 15%-át, beleértve az Egyesült Államok kormányáét is. Az biztosított erre lehetőséget, hogy a kínai távközlési cég elhitette a világ többi internet szolgáltatójával, hogy az adatcsomagok „A" pontból „B" pontba való eljuttatásának leggyorsabb útvonala rajta keresztül vezet.[2] Mindazonáltal alkalom adódott az egyik legismertebb, közbeékelődéses (man-in-the-middle) támadás végrehajtására, amivel a nyílt kommunikáció megismerése mellett akár a titkosított csatornák közléseinek visszafejtésére is lehetőség nyílt. [3]

EGY LEHETSÉGES KIBERTÁMADÁS KELLÉKTÁRA

Már a fenti, néhány esemény és technika alkalmazása alapján is kimondható, hogy a támadási vektorok elég széles informatikai területet érinthetnek, amelyek felhasználhatók a kiberterror eszközeiként is. Az ismerethalmazunk további bővítése a manapság leginkább ismert módszerekkel teljesebb képet adhat arról, hogy milyen képességek kerülhetnek a terrorizmus kelléktárába.

DDOS (distributed denial-of-service): Túlterheléses vagy más néven szolgáltatás megtagadásos támadás, aminek eredményeképpen a feljogosított felhasználók nehezen vagy egyáltalán nem érik el a számukra biztosított szolgáltatást, információt vagy rendszert.

Reklámprogram (adware): Olyan reklámozó program, ami a felhasználó engedélye nélkül hirdet termékeket és szolgáltatásokat. Egyes esetekben kicseréli egy adott honlapon található reklám tartalmát.

Kémprogram (spyware): Olyan program, ami a felhasználó számítógépes aktivitásáról, tevékenységéről küld információt készítőjének. Működésére a rejtőzködés jellemző.

Kéretlen levelek (e-mail spam): Valós emberektől érkező, levélnek tűnő, bosszantó, rosszindulatú, álcázott üzenetek vagy reklámok. Segítségükkel a felhasználót rá lehet csalogatni hamis adathalász honlapokra.

Ál kattintás (click fraud): Aminek hatására a felhasználó akaratától eltérő honlapokat látogatat meg, ami az érintett cégeknek vagy személyeknek kereskedelmi előnyt hozó forgalmat állít elő.

Gyors folyamatos mozgás (Fast flux): Olyan DNS[3] technika, amivel el lehet rejteni adott tartománynév mögött rejlő IP címet[4] úgy, hogy gyorsan változtatják a DNS névhez tartozó IP címet. Ezáltal tűzfalakkal nehezen szűrhető ki egy rosszindulatú honlap vagy szerver IP cím alapján, mivel az folyamatosan változik.

[1] Olyan adathalmaz, program vagy parancssorozat, amely alkalmas egy szoftver vagy hardver elem biztonsági hibájának kihasználására, ami nem várt viselkedést idéz elő az érintett elemben.

[2] Ez az az útvonal, amit alapvetően minden internet adatcsomag keres az adatok minél hamarabbi célba juttatása érdekében.

[3] Domain Name System – Olyan rendszer, melynek segítségével feloldhatjuk egy adott névhez (domain név) tartozó IP címet.

[4] Internet Protocol cím– egyedi hálózati azonosító, amely alapján azonosítani tudják egymást a kommunikáló számítógépek vagy eszközök.

Teljes kipróbálás (brute forcing): Titkosított vagy jelszóval védett rendszer (FTP[5], SMTP[6], SSH[7]) ellen alkalmazott módszer. A módszer minden jelszót kikísérletezve próbál hozzáférni a rendszerhez.

Féreg (worm): A számítógépes vírushoz hasonló, de önállóan is működőképes program. Képes segítség nélkül terjeszteni önmagát más gépek sérülékenységének kihasználásával vagy akár e-mail felhasználásával is.

Félelem keltő (scareware): Olyan program, amely megrémíti a felhasználót – operációs rendszer által használt rendszerüzenet ablakot utánozva – egy nem létező vírus fertőzéssel, majd felkínál egy – egyébként nem működő – víruskeresőt megvételre. [4]

Forgalom figyelő (sniffing traffic): Figyeli a felhasználó forgalmát és kigyűjti a titkosítástól mentes, érzékeny információkat (jelszó, felhasználó név).

Billentyűzet figyelés (keylogging): A felhasználó által billentyűzeten keresztül bevitt adatokat összegyűjti és továbbítja. Ezek között gyakran szerepel felhasználó név, jelszó, bankkártya adatok.

Folyamatban lévő szavazás/játék módosítása (manipulating online polls/games): A felhasználó helyett a program vesz részt a szavazásban vagy játékban. [5]

A felsorolt kelléktár elemek egyaránt tartalmaznak adatszerző, szolgáltatás túlterhelést okozó és szervert rejtő technikákat is. Az egyes elemek egyedi és kombinált használata egyaránt tág alkalmazási teret biztosít az igénybevevőnek.

Könnyen észrevehető és egyben kihangsúlyozandó előnye a modern támadási formáknak, hogy – ellentétben a hagyományos fegyverek túlnyomó részével – nem kell jelen lenni a kiszemelt célpontnál. A támadás végrehajtása után is fedésben tud maradni a támadó. Ebből adódik, hogy nehezen állapítható meg, hogy egy nemzet vagy egy terrorszervezet áll a cselekmény mögött.

Hátránya, hogy bonyolultabb akciók esetén kitartó és részletekbe menő információszerzés szükséges, mely során folyamatosan ügyelni kell a fedett működésre. „Az információszerzés egyik alapvető módja a felderítés, amely egyidős a háborúval és a különböző katonai tevékenységekkel. Az egymással szembenálló felek mindenkor törekedtek arra, hogy a legtöbb és a lehető leghitelesebb információt gyűjtsék be a másik fél erejéről, várható tevékenységéről. Napjainkban e célra a legkülönfélébb módszereket és technikai eszközöket használják fel, melyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait.” [6]

Az információszerzés tevékenysége, az alkalmazható technikai eszközök felsorolása túlnyúlik e cikk keretein, ezért mellőzzük kifejtését.

A KIBERTERRORTÁMADÁS MEGVALÓSÍTÁSÁNAK LEHETSÉGES MÓDSZEREI ÉS ESZKÖZEI

A kelléktár egyes elemeinek:

- alkalmazásához be kell juttatni a programot az áldozat számítástechnikai eszközére, valamint fenn kell tartani a bejuttatáshoz szükséges képességet,
- alkalmazásakor tartani kell a kapcsolatot a telepített klienssel,
  a) feladat meghatározás,
  b) új program frissítése kapcsán,
- alkalmazásakor a keletkező adatokat be kell gyűjteni,
  a) fel kell dolgozni és

[5] File Transfer Protocol – Állományok átvitelére alkalmas protokoll.
[6] Simple Mail Transfer Protocol – kommunikációs protokoll elektronikus levelek továbbítására.
[7] Secure Shell – biztonságos adatkommunikációra alkalmazható hálózati protokoll.

b) el kell juttatni a megfelelő felhasználónak.

- alkalmazásakor üzemeltetni kell, és fenn kell tartani az adatgyűjtésben résztvevő szervereket.
- alkalmazásához folyamatos fejlesztéssel gondoskodni kell a rejtett működés fenntartásáról, a felfedezhetőség kizárásáról,
- alkalmazásához a hálózat elemeinek fenntartása (bérlése) és elhelyezése során ügyelni kell a visszakövethetőség megakadályozására.

A felsoroltak közül az áldozat számítástechnikai eszközére való bejuttatást és az adatgyűjtésben résztvevő szerverek üzemeltetésének jelentőségét emelném ki, mivel ezek hiányában a többi tevékenység végrehajtása szinte érdemtelenné válik. A kiemelt funkciók teljesítésére az exploit és/vagy a Botnet[8] rendszer alkalmas.

Amennyiben a kiszemelt áldozat számítástechnikai eszközére való bejuttatás sikertelen a „scarware" vagy egyéb interaktív megoldással, akkor exploit alkalmazása szükséges. A Botnet igénybevétele konkrét célpont elleni, nagy mennyiségű forgalom egy időben történő generálására továbbá tömeges adatgyűjtés alkalmával nélkülözhetetlen.

A kelléktár egyes komponenseihez kapcsolódó feladatok speciális szakembert igényelnek, ezért óriási az igény mind az állami szféra mind a bűnözői (terrorista) körök részéről ennek a tudásnak a birtoklására, ezáltal a hangsúlyos funkciók feletti dominancia megszerzésére. Ennek jól látható jelét tapasztalhattuk 2013 végén, amikor a GCHQ[9] több száz, önként jelentkező számítógépes szakértőn kívül az elítélt hackereket is besorozta kibervédelmi erőinek soraiba.[7]

A KIEMELT FUNKCIÓK MEGSZERZÉSE

Az egyes kormányzatok nyíltan, hirdetések segítségével feltölthetik személyi állományukat nagy informatikai tudással rendelkező polgárokkal, ellenben a bűnözői körök ugyanezt a módszert nem alkalmazhatják ezen a területen. Hasonló tapasztalható a kiemelt funkciók megvalósításához szükséges exploit és a Bot hálózatok megszerzése kapcsán.

1. ábra. exploit értékesítő az interneten [8]

[8] A roBot és network (hálózat) szavak kombinációja –más néven Bot hálózat. Olyan hálózat, melynek az a feladata, hogy gyorsan nagymennyiségű adatot tudjon előállítani vagy begyűjteni úgy, hogy a rendszer irányítója ismeretlen marad. A hálózat elemei olyan számítógépek, amelyek a tulajdonosuk akarata ellenére működnek együtt a rendszerrel.

[9] Government Communications Headquarters – az Egyesült Királyság titkosszolgálatainak egyike – felelős a brit kormány és a fegyveres erők információvédelméért.

Az alábbiakban felsorolt lehetőségek állnak rendelkezésre az exploit-ok megszerzésére:

- Saját erőforrás (szakember gárda, eszközrendszer) segítségével szoftverek és hardverek sérülékenységének
  a) kutatása,
  b) előállítása és forgalmazása.
- Számítógépes felhasználók által felfedezett sérülékenységek
  a) közvetlen beszerzése internet hálózaton keresztül,
  b) saját (fedő) vállalaton keresztüli beszerzése, felvásárlása.
- Hivatalos úton, szabad kereskedelemben való beszerzés.
- Világhálón elérhető, számítástechnikai eszközökön található információk alapján való előállítás vagy letöltés.

Az exploit-ok tekintetében a nemzeti rendvédelmi szolgálatok törvényes felhatalmazásuknál fogva felkereshetik a hazájukban működő számítástechnikai cégeket, melyek sérülékenységek felvásárlásával, elemzésével, esetleg feltárásával foglalkoznak. Az állami befolyás mértékétől függően el lehet érni, hogy a kiszemelt vállalkozások kiemelt hangsúllyal szolgálják a nemzet érdekeit. Ellenben léteznek olyan műhelyek, ahol az ideológia, a vallási, ill. politikai célok elérése vagy a vállalkozás gyors fellendítése, vagyis a pénzszerzés a fő mozgatórugó. Ezekben az esetekben a szervezett bűnözői körök és a terroristák is együttműködőre találhatnak.

Offering	Price
Exploit bundle rental: 24 hours 1 week 1 month	 US$25 US$125 US$400
Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player)	US$3,000 per month
Eleonore Exploit Pack v. 1.6.2 (for Microsoft Data Access Components [MDAC], IEpeers, SnapShot, HCP, JDT, JWS, PDF collab,collectEmailInfo, PDF SING, and Java Invoke(chain) 1.5/1.6; average reach of 10-25%)	US$2,500-3,000
Phoenix Exploits Kit v. 2.3.12 (for Internet Explorer [IE] 6 MDAC, Java Deserialize, Java GSB, PDF Collab/Printf, Adobe Flash Player 9 and 10, IEpeers, Java SMB, HCP, PDF/SWF, PDF Open, and PDF Lib TIFF)	US$2,200 per domain
Less popular and less effective bundle	US$25+
XSS exploit for Mail.ru: Active XSS exploit Passive XSS exploit Passive XSS exploit for Rambler.ru and Yandex.ru XSS exploit for Gmail.com	 US$50-150 US$10-35 US$10-50 US$200
SQL exploit for a site with 50,000 visitors a day	US$100
Exploit bundle crypting service: 1-time 1-month subscription (5 times)	 US$50 US$150

2. ábra. exploit árak az interneten [9]

A kormányoknak lehetősége nyílik a szabad kereskedelemben beszerezni exploit-okat, akár támadó céllal is. Erre jó példa az európai székhelyű, VUPEN[10] vállalat, ahol a legfrissebb (azaz nulladik napi) sérülékenységeket kihasználó – nem titkoltan, akár támadó jelleggel is használható – programokat értékesítenek kizárólagosan kormányok törvényileg felhatalmazott szervezetei részére. Bizonyos államok és természetesen a terrorista szervezetek korlátozó intézkedések hatálya alá tartoznak, akik részére a programok nem értékesíthetőek. A fentiek

[10] VUPEN Vulnerability Research Team (VRT) – sérülékenységeket kutató európai vállalat.

figyelembe vételével egyáltalán nem zárható ki, hogy egy terrorista csoport is hozzáfér és birtokolja a rosszindulatú számítógépes kliensek távoli bejuttatásához szükséges technológiát. Annál is inkább, mivel az interneten rövid idő leforgása alatt találhatunk több olyan céget, amely számos, nulladik napi sérülékenységet árul, elérhető áron, enyhébb korlátozásokkal. (1. ábra)

A sérülékenységek elérhetőek különböző csomagokban pl: napi, heti vagy havi időszakra. Bizonyos programcsokorra vagy akár konkrét adatbázis szoftverre vonatkozólag. (2. ábra)

Botnet rendszerek megszerzése kapcsán a következő lépések alkalmazhatóak:

- Már létező Botnet tulajdonosától a hálózat felvásárlása vagy adott feladatra való bérlése.
- Saját Bot hálózat kiépítése és fenntartása.

Amennyiben górcső alá vesszük a második esetet, szem előtt tartva azt, hogy a kelléktár egyes komponenseihez kapcsolódó feladatok speciális szakembert igényelnek, akkor könnyen beláthatjuk, hogy a fenntartás és működtetés hosszú távon nemcsak költséges és kockázatos, hanem időigényes is. Ez a megoldás inkább kormányok számára előnyösebb.

Kisebb adatgyűjtő feladatok ill. kiberterror támadások végrehajtására gazdaságosabb és előnyösebb a Bot hálózat bérlése, mivel

- a bérleti díj alacsonyabb, mint egy teljes hálózat fenntartása hosszútávon,
- a hálózatépítés fáradságos tevékenysége mellőzhető,
- a hálózati elemek tulajdonoshoz – személyi azonosítók alapján – való kötődése kisebb, mint a hálózat bérlőjéhez. Mindazonáltal a támadó személye rejtve marad.
- Több, egyidejű támadásra alternatív hálózatok is igénybe vehetők.

Amint a támadó hitelesíti magát a bérelt hálózatba, azonnal rendelkezésre áll számára az összes funkció. Például érzékeny információkat (billentyűzet leütések, belépési azonosítók, bankkártya adatok) gyűjthet az összes kompromittált gépről, nagy mennyiségű forgalmat (DDoS) állíthat elő néhány egyszerű utasítással. Mivel ilyen könnyen átvehető egy Bot hálózat irányítása, ezért elég gyakran veszik igénybe ezt a szolgáltatást az interneten keresztül. A DDoS szolgáltatással kapcsolatos bérleti díjakat a 3. ábra, míg a Bot hálózatét a 4. ábra mutatja. A Botnet bérleti árak a felére csökkentek Oroszországban a 2014. augusztusi adatok alapján. [10]

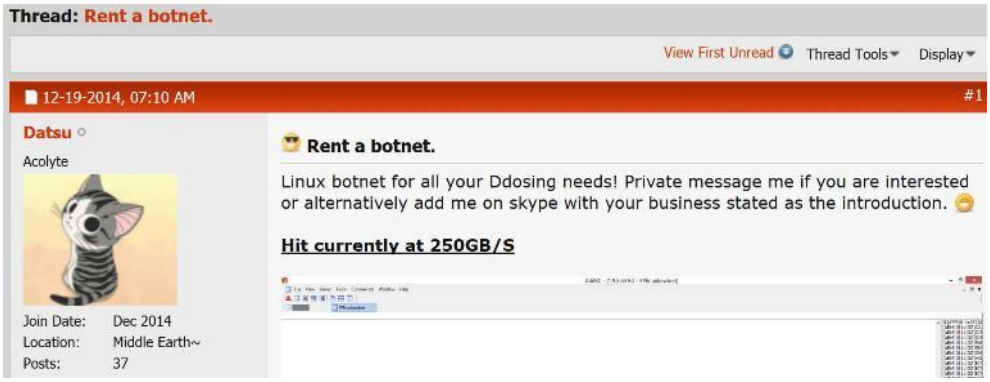
Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

3. ábra. DDoS árak az interneten [9]

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

4. ábra. Botnet bérleti árak az interneten [9]

Az árak tükrében kijelenthetjük, hogy ma már szinte bárki számára elérhető áron lehet ezeket a szolgáltatásokat bérelni. Az alábbi ábra – egy néhány perc alatt felkutatott – igen nagy sávszélességű DDoS támadási képességgel rendelkező Botnet bérleti lehetőséget ajánl a tavalyi év végén. (5. ábra)



5. ábra. Botnet bérleti lehetőség az interneten [11]

Az igen súlyos károk okozására alkalmas, bérelhető szolgáltatások tulajdonosai egyre bátrabban hirdetik szolgáltatásaikat, mivel egyre kifinomultabb módszerek (pl.: „Flash flux" eljárás)) állnak rendelkezésre a rejtőzködés területén, ezáltal biztosak lehetnek benne, hogy személyüket és tartózkodási helyüket nem fenyegeti veszély.

A ma már klasszikusnak mondható Botnet eszközrendszere, ami megfertőzött asztali számítógépekből és vezérlő szerverekből állt új, széleskörűen használt elemmel bővül napjainkban, a mobil kommunikációs eszközök új generációjával. Amellett, hogy az okos telefonok el tudják látni alapfunkciójukat (telefonálás, zene hallgatás, képek készítése) még a Bot hálózat feladatokat is képesek végrehajtani anélkül, hogy a tulajdonosnak ez nagyon szembe tűnne. A korábban már ismert, NotCompatible rosszindulatú szoftver új variánsa komplexebb technikákkal lett felvértezve, ami – az időközben mögé kiépült, - rendkívül jól működő Botnet-et hatékonyan tudja használni. [12]

Könnyen belátható, hogy az okos telefon Botnet kliensként való használata azzal a fenyegetéssel jár, hogy:

- szinte állandóan be van kapcsolva, tehát folyamatosan elérhető,
- egy főre jutó mennyisége meghaladja az asztali számítógépekét,
- egyre nagyobb sebességű mobil internet hálózat szolgálja ki, (ami a jövőben is növekszik) ezáltal – többek között – extrém sávszélességű DDoS támadások kivitelezésére válik alkalmassá.

ÖSSZEGZÉS

Cikkemben rámutattam, hogy a – mindenki által jól ismert, töretlen – számítástechnikai fejlődés eredményeként a terroristák és bűnözői körök hagyományos támadásra használt technikai eszközrendszere könnyen kibővíthető és könnyen igénybe vehető a világhálón keresztül. Köszönhető egyrészről annak, hogy az exploit-ok értékesítésében résztvevők közül csak néhány ellenőrzi a vevőt és annak szándékait a felhasználásra vonatkozólag. Másrészről nagyon gyorsan találunk olyan Botnet értékesítőt, akitől bérelhetünk erőforrásokat támadásra, mivel a komplex rejtőzködési eljárások miatt jól tudnak az értékesítők rejtőzködni.

A negyedik fejezetben szereplő árakkal felhívtam a figyelmet arra, hogy bárki számára elérhetőek ezek a szolgáltatások, tehát kibővül azoknak a köre, akik komoly károkat tudnak okozni, akár tudatlanságból is. Gondolnunk kell azokra is, akik önkényesen nevezik ki magukat egy terrorista csoport tagjának és azok nevében indítanak támadást egy fontos, kormányzati infrastruktúra ellen, akár helyrehozhatatlan károkat okozva.

Továbbá felhívtam a figyelmet arra, hogy a Bot hálózatok elemeinek a száma jelentősen megnőhet a közeljövőben azáltal, hogy a hordozható okos telefonok is részévé válnak kliensként a rendszernek. Mindazonáltal részt vehetnek a Botnet rendszerek feladat-végrehajtásában (pl.: nagyszabású túlterheléses támadásban.)

Következtetésképpen elmondható, hogy már a Botnet rendszerek kialakítását is meg kell akadályozni annak érdekében, hogy elkerüljük a NotCompatible esetét, ahol több, mint 2 éve nem sikerült a hálózatot lokalizálni és megszüntetni. Ennek érdekében át kell gondolni a hazai internet stratégiát és ki kell alakítani azokat az intézményeket, amelyek hatékonyan tudnak fellépni a Bot hálózatok ellen is, amelyek fenyegetést jelentenek a kormányzati hálózatra és a kritikus infrastruktúrákra is.

Felhasznált irodalom:

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf; (Letöltve: 2014.12.02.)

[2] Teague Newman, Tiffany Rad, ELCnetworks, John Strauchs, Strauchs: SCADA & PLC VULNERABILITIES IN CORRECTIONAL FACILITIES White Paper 2011.07.30. (Letöltve: 2014.12.15.)

[3] Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic: UPDATED: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249; (Letöltve: 2014.12.15.)

[4] http://en.wikipedia.org/wiki/Botnet (Letöltve: 2014.12.20.)

[5] https://www.honeynet.org/book/export/html/50 (Letöltve:2014.12.22)

[6] Haig Zsolt - Kovács László - Ványa László - Vass Sándor: Elektronikai hadviselés. NKE 2014, Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori iskola, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., ISBN 978-615-5305-87-0

[7] Haroon Siddique: Ex-hackers could be recruited to UK cyberdefence force http://www.theguardian.com/technology/2013/oct/22/uk-cyber-defence-force-ex-hackers-gchq (Letöltve: 2014.12.28.)

[8] http://1337day.com/ (Letöltve: 2015.01.20.)

[9] Trend Micro Incorporated Research Paper 2012 Russian Underground 101: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf (Letöltve: 2015.01.17.)

[10] Hacker Prices and Other Cybercrimes: http://www.havocscope.com/black-market-prices/hackers/ (Letöltve: 2015.01.19.)

[11] http://www.rdfrn.com/showthread.php?554-Rent-a-botnet (Letöltve: 2015.01.20.)

[12] https://blog.lookout.com/blog/2014/11/19/notcompatible/ (Letöltve: 2015.01.20.)