Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2011. III. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető....3
Szoftver sérülékenységek....4
Informatikai biztonság a vállalati szféra szemszögéből 2011....5
A vállalati szféra hardver-ellátottsága....6
A vállalati szféra szoftver-ellátottsága....7
Hálózatok és internet-használat a vállalati szférában....8
Költségvetés, stratégia, fejlődés....9
Internetbiztonsági incidensek....11
DDoS támadások 2011. második negyedévében....12
DDoS és tiltakozás....12
DDoS támadások a közösségi médiában....13
Kereskedelmi DDoS támadások....13
DDoS támadások eloszlása országok szerint....14
A megtámadott weboldalak eloszlása online aktivitás szerint....15
A DDoS támadások típusai....16
A DDoS botnetek aktivitása az idő függvényében....17
Következtetés....17
A routing tábla birtoklása – Új OSPF támadások
Blackhat USA 2011....18
Kapcsolódó tanulmányok....20
Új támadások....21
Álcázott LSA....21
Hamis távoli szomszédosság....24
Konklúziók....27
Káros szoftverek az mobil készülékek világában....28
Trendek és tendenciák....28
Célpontok....29
Célkeresztben az Android....30
Tudatosítás....31
Kitekintés a kiber-bűnözéssel kapcsolatos nemzetközi jogi, nemzetközi büntetőjogi környezetre....32
Cyber Crime Convention – Budapest, a múlt és a jelen....32
Az Europol....32
Nemzetközi bűnügyi jogsegély intézménye az internetes bűncselekmények területén....33
A büntetőeljárás átadása....34
A büntetőeljárás átvétele....34
A Nemzetközi Büntetőjog, a nemzetközi felelősségre vonás szabályai....34
A VirusBuster Kft. összefoglalója 2011 harmadik negyedévének IT biztonsági trendjeiről....35
Államok rémálmai....35
Bűn....37
...és a bűnhődés....37
Spamesnek áll a világ?....39
Kiemelkedő kártevők....40
Folt hátán folt....42
A VirusBuster Kft.-ről....43
Elérhetőségeink....44

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2011. harmadik negyedéves jelentését, amely a negyedév legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a VirusBuster Kft. informatikai biztonsági trendjeiről szóló összefoglalóját. A jelentésben a főszerep ismét a hálózatbiztonságé.

A jelentés betekintést nyújt az informatikai biztonság berkeibe, jelen kiadványunkban a vállalati szektor szemszögéből.

Egy-egy cikk erejéig kitérünk az okostelefonok térhódítása által ránk leselkedő veszélyekre, a kiberbűnözés nemzetközi jogi hátterére, az OSPF támadások világába is betekintünk.

A Nemzeti Hálózatbiztonsági Központ továbbra is eredményesen működteti szakmai közönségének és partnereinek szóló IT biztonsági oldalát a Tech.cert-hungary.hu-t.

Az oldalon a látogató megtalálhatja a legfrissebb szoftversérülékenységi és riasztási információkat, valamint a TechBlog hírfolyam naponta frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven.

Mindenkor fontos megemlítenünk, hogy a jelentésben szereplő adatok, értékek és kimutatások a PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ, mint Nemzeti Kapcsolati Pont hazai és nemzetközi kapcsolatai által szolgáltatott hiteles és aktuális információkon alapszanak.

Bízunk abban, hogy ezzel a jelentéssel egy megbízható és naprakész ismeretanyagot tart a kezében, amely hatékonyan támogatja majd az Ön munkáját és a legtöbb informatikai és internetbiztonságban érintett szervezetnek is segítséget nyújt a védelmi stratégiai felkészülésben.

A Puskás Tivadar Közalapítvány - Nemzeti Hálózatbiztonsági Központ (CERT-Hungary) nevében:

Dr. Angyal Zoltán
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
hálózatbiztonsági igazgató

Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
nemzetközi képviselő

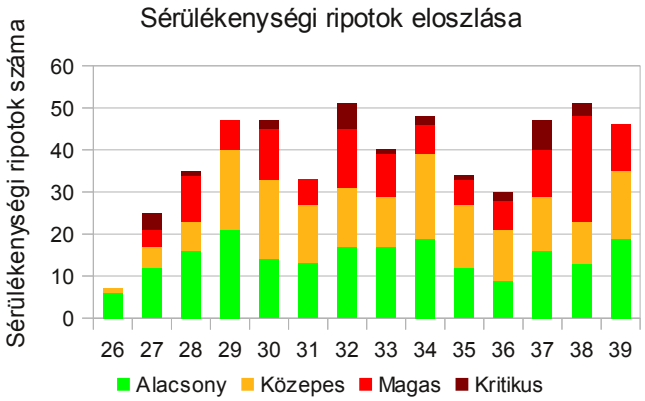
Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

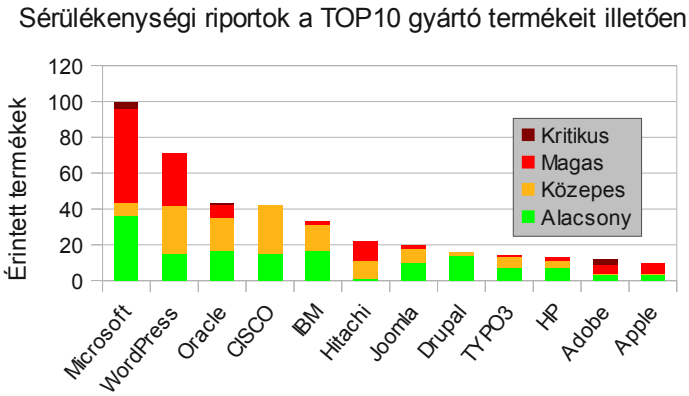
Szoftver sérülékenységek

Szoftversérülékenység minden olyan szoftver gyengeség vagy hiba, amelyet kihasználva egy rosszindulatú támadó megsértheti az informatikai rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** 2011. harmadik negyedéve során **541 db szoftver-sérülékenységi információt** publikált, amelyekből 204 db alacsony, 177 db közepes, 131 db magas és 29 db kritikus kockázati besorolású.



Jelen periódusban összességében 8%-al több sérülékenységi publikáció került kiadásra, mint az előző negyedévben, továbbá a magas és/vagy kritikus sérülékenységek száma is 25%-al nőtt

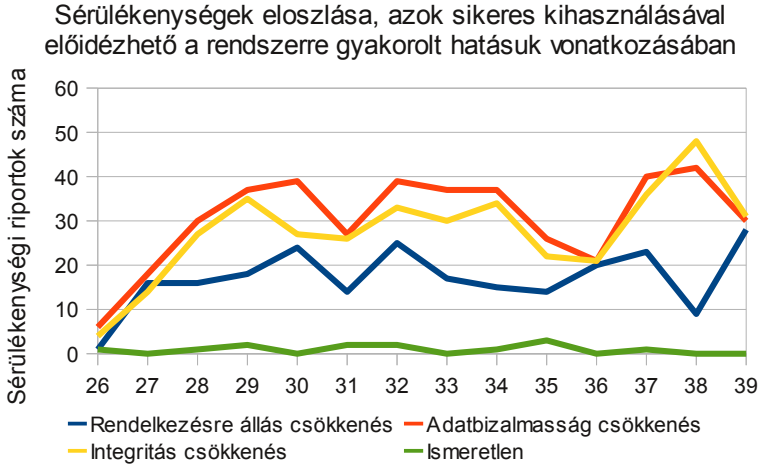


A sérülékenységek által érintett gyártók tekintetében igaz ugyan, hogy a Microsoft áll az élen, de az előző negyedévhez képest 2011 harmadik negyedévében 30%-al kevesebb termék került regisztrálásra az egyes sérülékenységek kapcsán. Viszont ezen termékek több mint felére nézve a feltárt biztonsági rések magas és/vagy kritikus kockázatot jelentenek.

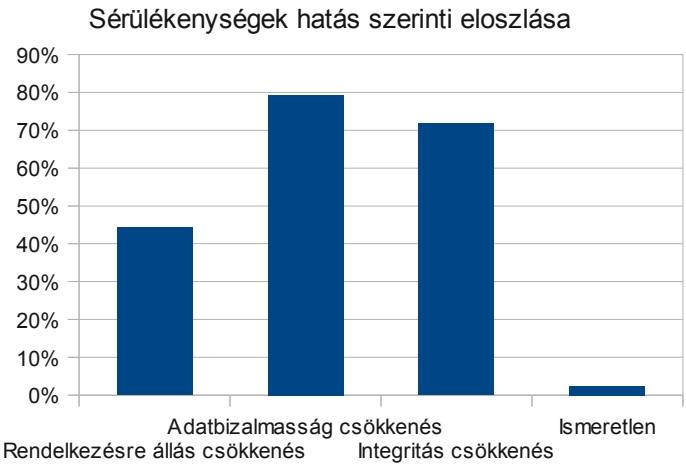
Igaz ugyan, hogy a kimutatás a TOP10-es lista és ezt az Adobe és az Apple zárja a 11. és 12. helyen, de úgy gondoltuk, hogy érdemes figyelmet szentelni az említett gyártók termékeiben feltárt biztonsági hibákra is, hiszen a negyedévben, az említett gyártók termékei kapcsán felfedezett sérülékenységek többsége magas és/vagy kritikus kockázatú – Adobe termékek esetében 75%, Apple termékek esetében 60%.

A sebezhetőségek értékelésénél fontos az is, hogy a biztonságon belül mit fenyegetnek, azaz milyen nem kívánt beavatkozást tesznek lehetővé a támadók számára. Ennek alapján a felhasználók jobban képet alkothatnak arról, hogy az egyes általuk használt termékekben felfedezett biztonsági hiányosságok esetében gyakorlatilag, milyen veszélyekkel kell szembenézni.

A bizalmasságot fenyegető veszélyek kiaknázásával információt nyerhetnek a támadók a számítógépeinkről, a sértetlenség (integritás) sérülésével a támadó módosíthatja adatainkat, programjainkat, míg az elérhetőségre vonatkozó támadásokkal a gépünk normál üzemszerű működését akadályozhatják meg a támadók (ideértve a programjaink törlését és a gépek más célú felhasználását – botnet hálózathoz való csatlakoztatását is).



A feltárt sérülékenységek jelentette veszélyek komplexitása ebben a negyedévben is meglehetősen magas, hiszen egy sérülékenység jellemzően több területre jelentett veszélyt, egyben a bizalmasságot, a sértetlenséget és az elérhetőséget is.



Ezért is nagyon fontos egy naprakész komplex vállalati védelmi rendszer használata, mely legalább az ismert fenyegetések, rosszindulatú támadások ellen védelmet nyújt.

Egy ilyen rendszer használata mellett fontos annak folyamatos aktualizálása és frissítése a rendszerünk hatásos védekezési képességének megőrzése miatt.

Informatikai biztonság a vállalati szféra szemszögéből 2011.

Az informatikai sérülékenységek, informatikai biztonsági kérdések meghatározó módon hatnak a nemzetgazdaság három fő csoportjára, a háztartásokra, a vállalati szektorra és a közszférára is. Azonban minden célcsoport mást és mást tapasztal ezekből a kockázatokból, incidensekből, valamint nem mellékesen más a felkészültségük egy esetlegesen bekövetkező incidens megoldására.

A harmadik negyedév fókuszcsoportja a vállalati szféra, mely a hazai, kissé zilált szerkezet miatt különösen sokrétű terület. Éppúgy megtalálhatók a valódi IC T-tudatossággal működő nagyvállalatok, mint a fejlesztéseiket szűkösen mérő, sok esetben a mindennapi piacon maradással küzdő vagy éppen feltörekvő közepesek és a rengeteg kis- és mikrovállalkozás, amelyek számarányukban óriási súlyt képviselnek, viselkedésükben, ismeretszintjükben és az általuk alkalmazott technológiákat tekintve pedig sok esetben nem is a vállalatokhoz, hanem a lakossági felhasználók jellegzetességeihez állnak közelebb.

A piacon van továbbá számos állami nagyvállalat, amelyek stratégiai erőforrások fölött – közlekedés, energiaipar, közszolgáltatások, közművek, stb. – diszponálnak. Ők, bár a vállalati szférához tartoznak, inkább az előző félévben elemzett kormányzati szektorral mutatnak rokonságot döntéshozatali folyamataik, beruházásaik, gondolkodásmódjuk következtében.

Természetesen e szektor biztonsága is kiemelten fontos a nemzetgazdaság teljesítményének fenntartása érdekében. Bár látszólag ez a szektor bír a legtöbb szakértelemmel és erőforrással az informatikai, biztonsági problémák leküzdésére, azért bőven akadnak hiányosságok, nem beszélve az új technológiák – felhő alapú rendszerek, mobil informatika, okostelefonok, stb. – által generált mindig új kihívásokról, kockázatokról, megoldandó feladatokról.

A vállalati szféra hardver-ellátottsága

A vállalati szféra működéséhez elengedhetetlen a megfelelő szintű IT-infrastruktúra jelenléte. A vállalati adatvagyon a cégek legfontosabb erőforrását képezi. Ennek megfelelő kezelése megőrzése és védelme stratégiai fontosságú a folyamatos szervezeti működés fenntartása érdekében.

A BellResearch elemzői a Magyar Infokommunikációs Jelentés legutóbbi adatai[1] alapján megállapították, hogy az ellátottsági mutatók az elmúlt egy évben nem változtak számottevően, a mikrocégek egy része továbbra sem használ számítógépet; a fejlődés inkább a mobilitás terén érhető tetten.

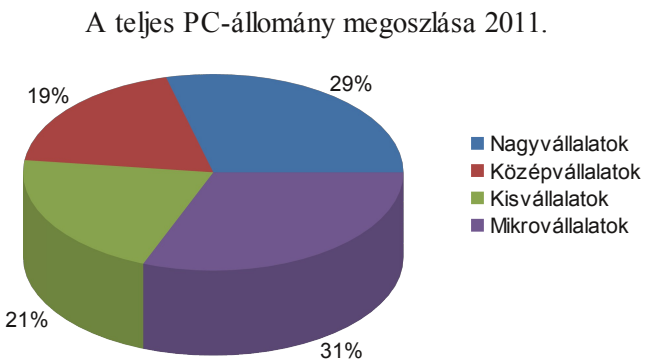
A személyi számítógép az IT-infrastruktúra alapja - s mivel minden megoldás és további eszköz erre épül, a PC-ellátottság szintje kulcsfontosságú a vállalatok fejlettsége, különösen a lemaradók szempontjából.

A PC-penetrációs mutató – azaz a legalább egy géppel rendelkezőknek az összes szervezetre vetített hányada – a legalább 10 fős cégek körében 2008 óta 100 százalékos, ekkor zárkóztak fel ugyanis a kisvállalatok, a nagyobb szervezetek gyakorlatilag teljes ellátottságának szintjére. Ezen a téren a mikrovállalati szegmens tartogathat(na) némi fejlődési potenciált, ugyanis az 1-9 főt alkalmazó vállalkozásoknak csak kicsivel több, mint négyötödénél találunk PC-t.

Ez azt jelenti, hogy 36 ezer hazai mikrovállalkozás még mindig nem használ számítógépet, aminek a legfőbb oka az igény hiánya. Az érintett döntéshozók úgy vélik, nincs szükségük PC-re az üzletmenet szempontjából, hogy az internetről ne is beszéljünk. Nem túl örvendetes, hogy túlnyomó többségük egyelőre beszerzést sem tervez. Az elmúlt évek adatai alapján rajzolt trend szintén a stagnálást támasztja alá. A penetrációs hányados a mikrovállalati körben alig mozdult felfelé.

A négy vállalati szegmens viszonylag kiegyenlített mértékben osztozik a teljes gépállományon, noha alapsokasági arányuk, illetve az egy cégre jutó átlagos géppark mérete nagyságrendekkel tér el egymástól. A kevesebb, mint fél százalékot kitevő, mintegy ezer nagyvállalatnál üzemel a PC-k 29 százaléka (cégenként körülbelül 360 géppel), míg a 205 ezer mikrovállalatnál összesen az állomány harmada (átlag 2-3 PC-vel, már ahol van); a fennmaradó 40 százalékon a kis- és közepes vállalatok osztoznak.

A teljes üzleti PC-állomány négyötöde asztali eszköz, de évről évre nagyobb teret hódítanak a hordozható számítógépek is - egyre inkább helyettesítő jelleggel. A legnagyobb arányban, közel egyharmad részben a mikrovállalkozások gép-parkjában vannak jelen a laptopok, jócskán megelőzve a többi szegmenst, ahol egyötöd körüli az arány. Ennek okai sokrétűek: a mobilitási megfontolások mellett sok esetben szerepet kap az üzleti alkalmazás melletti privát használat lehetősége is.



1 Bellresearch: Magyar Infokommunikációs Jelentés 2010.

Az év során az általános visszaesés ellenére a legnagyobb beszállítók statisztikái alapján a vállalati PC- értékesítések növekedtek. A vállalati szegmens is lassan, de fokozatosan mozdul a mobil eszközök egyre kiterjedtebb használata felé.

A trend egyértelműen a mobilizáció irányába mutat, hiszen évről évre nő a hordozható számítógépek eladásának aránya. A tapasztalatok szerint jelentős a mikrovállalatok szerepe a hordozható számítógépek arányának növekedésében, hiszen többségük notebookot választ asztali PC helyett, viszont sokszor a lakosságnak szánt eszközöket vásárolják, figyelmen kívül hagyva annak esetleges hátrányait egy vállalati notebookkal szemben.

A vállalati szféra szoftver-ellátottsága

Az operációs rendszerek tekintetében a verziókövetési gyakorlat erősen konzervatív; szerveroldalon már inkább megjelentek a szabadszoftverek.

A Magyar Infokommunikációs Jelentés adatai szerint a Microsoft kliens oldalon továbbra is rendíthetetlenül őrzi pozícióját, és az elmúlt egy év változásai a Windows 7 erősödésével foglalhatók össze. Bár továbbra is a kissé már korosodó XP áll az élen mind elterjedtségét, mind az installált bázison mért részesedését tekintve, a legújabb verzió a hazai cégeknél már megelőzi a Vistát.

A vállalatoknál az általános célú irodai szoftverek esetében hasonlóan erős Microsoft-elköteleződés figyelhető meg - mutatnak rá a kutatók. Ugyan az OpenOffice mint a legerősebb, szabad szoftverként hozzáférhető versenytárs a legalább 10 fős magyarországi cégek bő ötödénél megtalálható, ma tipikusan csak kiegészítő, és nem helyettesítő jelleggel alkalmazzák azt.

Az irodai szoftvert használó, legalább 10 főt foglalkoztató vállalati sokaság mindössze 5 százaléka cserélte le a megszokott MS-logós programcsomagokat, és tért át teljes egészében a ma már Oracle-felségterületnek számító szoftver használatára. A verziókövetésre komolyabb hangsúlyt korábban sem helyező vállalati vezetők továbbra is tipikusan két generációval korábbi szoftvereket licencelnek. Így ma a legszélesebb körben használt verzió az MS Office 2003-as és a 2007-es; részesedését tekintve a legelőkelőbb helyen pedig az Office 2003-as áll.

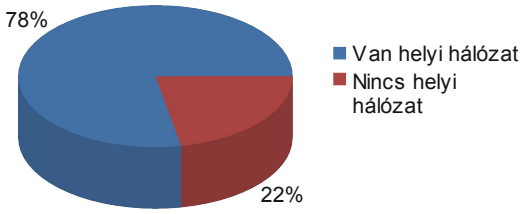
Szerveroldalon már jóval heterogénebb képet láthatunk. A márkázott termékek közül ugyan itt is a Windows Serverek szerepelnek a legjobban, de a különböző Linux-disztribúciók azért összességében számottevő részesedést tudhatnak magukénak. A legelterjedtebb rendszernek számító Windows Server 2003 44 százalékos, míg a legerősebb pozíciót birtokló Linux-variáns, a Debian mindössze 12 százalékos penetrációt tud felmutatni. A kutatók rámutattak, hogy valamilyen Windows Server-terméket a vállalkozások mintegy háromnegyede használ, a Linuxok összesített adata 28 százalék.

A tipikusan nagygépes környezetbe szánt Unixok elterjedtsége egyedül a nagyvállalati szegmensben tekinthető számottevőnek, bár az ott mért 12 százalékos penetrációja érzékelteti a többség számára költséghatékonyabb x86-os platformok erős dominanciáját. Ma a vállalati informatikusoknak a kérdés a gyakorlatban a Linux és/vagy Windows Server formájában tehető fel. A válasz a nagyobb szervezeteknél inkább a vegyes alkalmazás, a kis- és középvállalati szektorban pedig az egységesítés jegyében az egyik "vonal" preferálása.

Hálózatok és internet-használat a vállalati szférában

A legalább két darab, asztali vagy hordozható személyi számítógéppel – azaz olyan gépparkkal, amelyen már értelmezhető a helyi hálózat fogalma – rendelkező hazai cégek mintegy 78 százaléka kapcsolja össze PC-it. A 250 fő feletti nagyvállalatok esetében teljes az ellátottság, és az 50 fő feletti körben is közelíti ezt a szintet. Számottevő lemaradást az előbbi szegmensekénél általában lényegesen kisebb PC-állományt használó kis- és mikrovállalatok esetében tapasztalhatunk, ahol a penetrációs mutató a 2-nél több PC-t használó vállalati körben 74, illetve 54 százalékra tehető.

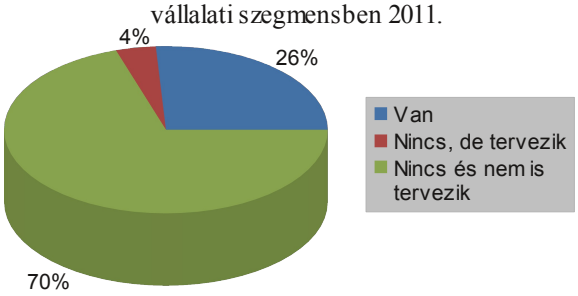
LAN penetráció a 10 fősnél nagyobb, 2 PC-nél többet használó szegmensben 2011.



Az eredmények azt tükrözik, hogy a LAN-ellátottsági mutató, illetve a helyi hálózattal rendelkező hazai cégek száma évről évre emelkedik ugyan, de csak igen kis mértékben és egyre lassuló ütemben.

A LAN-ok komplexitása a vállalatmérettel párhuzamosan nő. A szerver–kliens hálózatok, a dedikált kiszolgálók alkalmazása az 50 fő feletti szegmensben általánosnak tekinthető: a nagyvállalatok körében gyakorlatilag teljes az ellátottság, és a mutató értéke a középvállalatoknál is jóval meghaladja a 90 százalékot. A kisvállalatok körében azonban a cégek negyedénél, míg az 1–9 fős mikrovállalati szegmensben az esetek többségében csak alapvető funkciókat lehetővé tevő peer-to-peer hálózati architektúrát használnak, dedikált kiszolgálók nélkül.

A WLAN elterjedtsége a 10 főnél többet foglalkoztató vállalati szegmensben 2011.



A vezeték nélküli helyi hálózati infrastruktúrát tekintve az elmúlt évek mérsékelt növekedése után jelentős mozgás érzékelhető a piacon, a 10 fő feletti szegmensben már minden negyedik, PC-vel rendelkező cégnél van ilyen megoldás. Az elterjedtség a vállalatmérettel egyenes arányban áll, és az egy évvel korábbihoz képest valamennyi szegmensben számottevő, az informatikai döntés-hozók akkori terveit is meghaladó mértékben nőtt.

Az e téren élenjáró nagyvállalati körben a cégek közel 60 százaléka, de a kisvállalatok egyötöde is használ ilyen megoldást. Vagyis már nemcsak az általában egyéb szempontokból is fejlettebb top cégek részéről mutatkozik nyitottság a vezeték nélküli technológiára, hanem a kisebb szervezetek jó része is felismeri a technológia előnyeit.

Az internet helyzetét vizsgálva, a penetráció fejlődése a hazai cégek és intézmények körében az utóbbi időszakban lelassult, illetve az elmúlt egy évben megtorpant. A legalább egy főt foglalkoztató magyarországi vállalatok 78 százaléka használ valamilyen internetkapcsolatot, míg 10 fő fölött megközelítőleg teljes az ellátottság.

Ám az, hogy a cégnél van internet-hozzáférés, még nem jelenti azt, hogy minden dolgozó el is éri a világhálót – emlékeztet a magyar BellResearch. Számos munkakörben erre nincs is szükség, esetleg a műszaki lehetőség hiányzik, de az is előfordul, hogy a vezetők csak kiemelt beosztású dolgozóknak adják meg az internethasználat lehetőségét. A hazai kutatók szerint tavaly a vállalati alkalmazottak közel kétharmada semmilyen formában nem fért hozzá munkahelyén a világhálóhoz; az internet használatát közvetlenül nem igénylő munkakörökben a menedzsment gyakran korlátozza, sőt egyenesen tiltja a világhálós szörfözést.

A nagyobb vállalatok körében mindeközben folytatódik a fejlődés. A hozzáférések száma nő, amiben nagy szerepe van a mobil szélessávnak. Az internetet használó vállalatok részéről érzékelhető az igény a magasabb sávszélességre és az egyre robusztusabb internetkapcsolatokra, valamint az SLA jellegű prémiumszolgáltatásokra is; a piacnak potenciális hajtóerőt a hostolt, menedzselt szolgáltatások terjedése, kritikus jelentőségűvé válása adhat.

Költségvetés, stratégia, fejlődés

Hardvereket az e téren érintett szervezetek 45%-a szerez be számítástechnikai szaküzletből, ami a teljes üzleti piacra vonatkozó rangsorban magasan az első helyet jelenti. Ez a csatorna a költségvetési szférában a leggyakoribb (51%), de a nagyvállalatoknál sem számít igazán ritkának, minden negyedik cégnél előfordul. Az egyes üzleti szegmensek beszerzési-vásárlási gyakorlata között azonban jelentősek az eltérések.

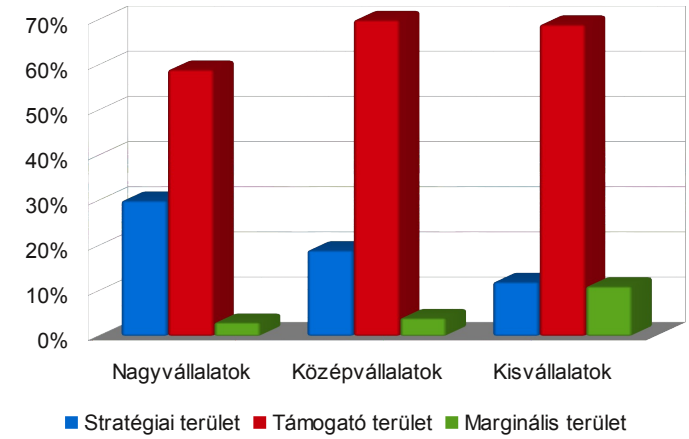
Az egyéb beszerzési megoldások közül a gyártótól vagy márkakereskedőtől, illetve a rendszerintegrátoron vagy informatikai cégen keresztüli vásárlások számítanak elterjedtnek. Ezek a vállalatméret növekedésével arányosan válnak egyre gyakoribbá, a 250 fő feletti nagyvállalati szegmensben pedig dominálnak, ahol a cégek mintegy fele közvetlenül, a harmada pedig partneren keresztül szerez be ilyen módon hardvereket. Ebben a körben az anyavállalatok központosított beszerzései is érdemi szerephez jutnak (23%).

A nemzetközi gyakorlatban egyre fontosabbá váló elektronikus beszerzési csatornák, az internetes áruházak és piacterek használata Magyarországra még kevéssé gyűrűzött be. A hazai szervezetek csupán 5 százaléka használ ilyen megoldásokat hardvervásárláskor - és ez alól a nagyvállalatok sem jelentenek kivételt. Az alacsonynak mondható hazai penetrációs adatok azt vetítik előre, hogy e téren az igazi áttörés még akár évekig is elhúzódhat - prognosztizálják a kutatók -, noha a beszerzésekben az internet, mint információs és kommunikációs csatorna szerepe egyébként folyamatosan nő.

Noha felértékelődő szerepét mindenki elismeri, a hazai cégek nagy többsége csak kiszolgáló területként tekint az informatikára; a nagyvállalatok élen járása a szemléletben és a fejlesztési fókuszokban is megmutatkozik.

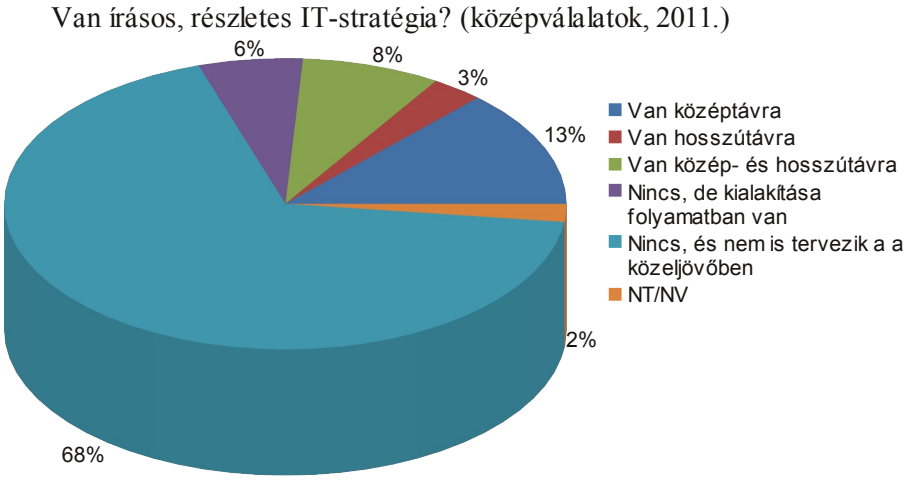
Az informatika mára a hazai cégek túlnyomó többsége számára megkerülhetetlenné vált a hatékonyság, illetve a legtöbb helyen egyáltalán a működés és a normál üzletmenet fenntartása szempontjából.

Az infokommunikáció szerepe a cégeknél 2011. (százalék)



A vállalat viszonyulása az infokommunikációhoz sok mindent meghatároz a célok kijelölésétől a fejlesztési prioritásokon és büdzséken át a mérhetőségig és az értékelésig. A kutatási eredmények tanúsága szerint az IT működésre és üzleti folyamatokra gyakorolt hatását a 10 fő feletti körben a szereplők meghatározónak tekintik a versenyképesség- és hatékonyságnövelés, a költségcsökkentés vagy akár a munkavállalói elégedettség szempontjából, és azzal is egyetértettek a döntéshozók, hogy az IT szerepe egyre inkább felértékelődik.

Mindezek mellett a hazai cégek 71 százaléka csak az alaptevékenységet támogató, kiszolgáló funkcióként tekint az informatikára. Stratégiai szerepet leginkább a nagyvállalati szegmensben kap az infokommunikáció; az IT-stratégia és IT-költségvetés írásba foglalása is itt a leggyakoribb. A kisvállalatoknál ugyanez az arány csak 14 százalék, e körben ugyanennyien marginális területként kezelik az IT-t.



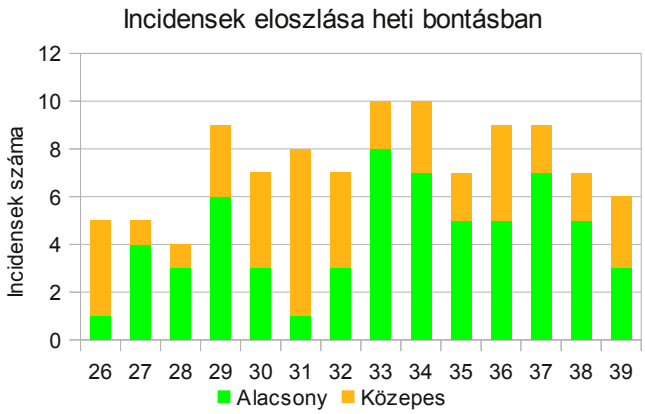
A nagyvállalati szféra és a kisebb méretű cégek közötti szakadék jelen van a beruházások célja tekintetében is. Máig a legtöbb projekt infrastrukturális fókuszú: PC-k és szerverek beszerzését vagy hálózati fejlesztéseket jelent. Az üzleti célokat szem előtt tartó, inkább a megvalósítandó funkciókra, és nem az IT elemi építőköveire koncentráló beruházások elsősorban a nagyok sajátosságai. Kivételt talán az internetes jelenlétet biztosító megoldások jelentenek: a vállalati webes aktivitásokat fokozó erőfeszítések - nyilván más-más szinten megvalósítva - a kisebb cégek számára is releváns területnek számítanak. A vállalaton belül az érintett részlegek között az első helyen az értékesítést, a felső vezetést és a pénzügyet találjuk.

Internetbiztonsági incidensek

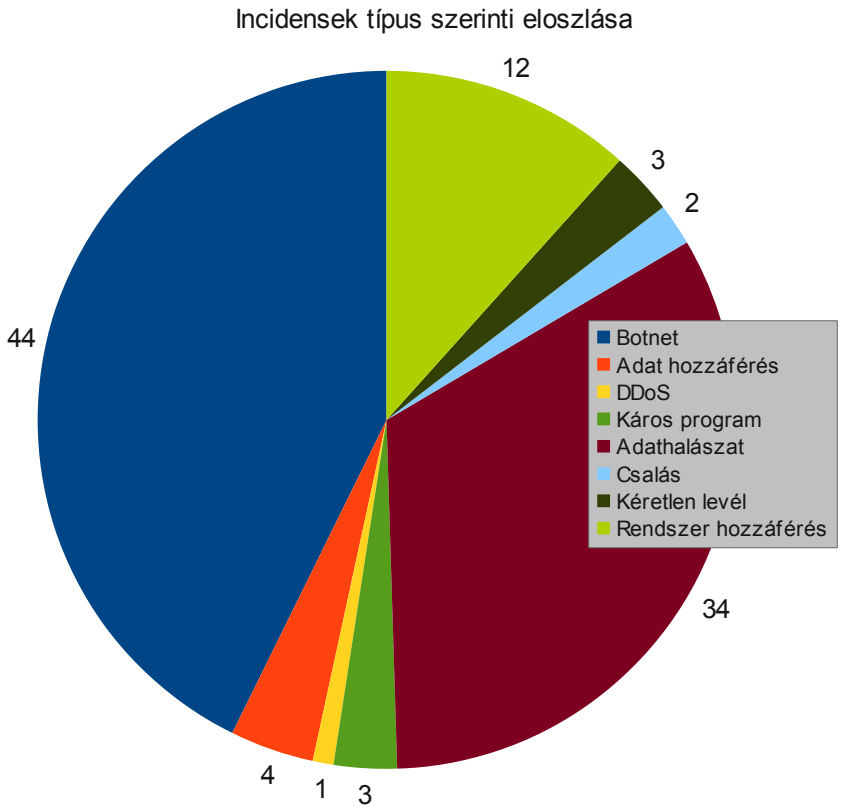
Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2011. harmadik negyedéve során összesen **103 db incidens bejelentést** regisztrált és kezelt, ebből 61 db alacsony és 42 db közepes kockázati besorolású.

A **Nemzeti Hálózatbiztonsági Központ** a hatékony incidens-kezelés érdekében **24 órás ügyeletet működtet** az év minden napján. Az ügyelet feladata az egyes incidensek kapcsán adandó válasz-intézkedések megtétele.



Az incidensek típus szerinti eloszlását tekintve, a megszokott trend változatlanul fennáll, hiszen 2011 harmadik negyedévében is túlnyomó többségében botnet hálózatok részét képező fertőzött gépek és adathalász tevékenység kapcsán érkezett, melyek összességében háromnegyedét teszik ki a periódusban kezelt incidenseknek, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket.



A botnet hálózatokat érintő és az adathalász oldalakat riportoló bejelentések mellet a harmadik helyen az illetéktelen rendszer hozzáférési kísérletek állnak. A rendszer hozzáférési kísérletekről beérkező bejelentések kapcsán érdemes megemlíteni, hogy Központunkhoz nem csak kísérletekről, de valós kompromittálódásról, illetve adatokhoz való illetéktelen hozzáférésről is érkeztek bejelentések. Ezek többsége email és FTP hozzáférési adatokat érintett, melyekkel összefüggésben összesen 120 szálon folyt incidenskezelés.

A bejelentések többsége külföldi partner-szervezetektől érkeztek és több mint 85%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben.

DDoS támadások 2011. második negyedévében

Napjainkban egyre gyakrabban lehet olvasni az online és a nyomtatott médiában is személyek, gyártók, cégek, valamint weboldalak elleni internetes támadásokról, amelyek következtében nem a weboldalak tartalmát módosították a támadók, hanem egyszerűen a kiszemelt célpontot elérhetetlenné tették DDoS (elosztott szolgáltatás megtagadás - Distributed Denial of Service) támadások által. A támadások következtében az érintettek hírneve csorbult vagy anyagi kárt szenvedtek el. Egyes támadókat letartóztattak vagy elítéltek, míg más támadók kiléte után még mindig nyomozások folynak. A cikkben felsorolt adatok a Kaspersky Lab botnet monitoring rendszeréből és a Kaspersky DDoS Prevention rendszeréből származnak.

Néhány fő adat a második negyedévből:

- A Kaspersky DDoS Prevention által visszavert legerőteljesebb támadás: 500 Mbps volt.
- A Kaspersky DDoS Prevention által visszavert átlagos támadás: 70 Mbps volt.
- A leghosszabb DDoS támadás ideje: 60 nap 1 óra 21 perc és 9 másodperc volt.
- A legnagyobb számú DDoS támadás egyetlen oldal ellen: 218 volt.

DDoS és tiltakozás

Az elosztott szolgáltatás megtagadásos (DDoS - Distributed Denial of Service) támadásokat már nem csak egyszerűen a profit szerzésért hajtják végre. A kiberbűnözők egyre inkább kormányzati forrásokat vagy nagy cégek weboldalait veszik célba, hogy megmutassák tudásukat, demonstrálják erejüket vagy egyes esetekben tiltakozásuknak adjanak hangot. Ezek pontosan azon fajtái a támadásoknak, amelyek a legnagyobb nyilvánosságot kapják a médiában.

2011. második negyedévének legaktívabb hacker csoportja a LulzSec és az Anonymous volt. DDoS támadásokat szerveztek kormányzati weboldalak ellen az Amerikai Egyesült Államokban, az Egyesült Királyságban, Spanyolországban, Törökországban, Iránban és néhány más országban. A hackereknek átmenetileg sikerült zavarokat okozni az oldalak működésében, mint például a www.cia.gov (Central Intelligence Agency - CIA - az amerikai Központi Hírszerző Ügynökség) és a www.soca.gov.uk (British Serious Organized Crime Agency - SOCA) weboldalai esetében. Ez azt mutatja, hogy még a kormányzati weboldalak védelméért felelős ügynökségek sem „immunisak” a DDoS támadásokra.

A kormányzati weboldalak ellen indított támadások igen kockázatosak, ugyanis azok azonnal magukra vonják a bűnüldöző hatóságok figyelmét. 2011. második negyedévében, például az Anonymous csoport több mint 30 tagját letartóztatták kormányzati oldalak ellen indított DDoS támadások gyanúja miatt. A hatóságok nyomozása során valószínűleg további letartóztatások lesznek, azonban a letartóztatott bűnözők nem mindegyike lesz elítélve, mert a DDoS támadásokban való részvétel számos országban nem számít illegális tevékenységnek.

A második negyedévben egy nagyvállalat volt kitéve komoly támadásnak, amely a Sony volt. Március végén a Sony jogi eljárást indított több hacker ellen, akiket azzal vádoltak, hogy feltörték a népszerű PlayStation 3 konzol firmware-jét[2]. Tiltakozásul, hogy a Sony üldözi a hackereket, az Anonymous DDoS támadást indított, amely egy időre megbénította a PlayStationnetwork.com weboldalt. De ez csak a jéghegy csúcsa volt. A Sony szerint a DDoS támadások alatt a PSN szolgáltatás szervereit törték fel és 77 millió felhasználó adatát tulajdonították el. Ez az akció a Sony hírnevét erősen csorbította.

2 (gyári beépített szoftver) egy olyan szoftverfajta, amely a hardvereszközbe van beépítve, és a hardver működtetéséhez szükséges legalapvetőbb feladatokat látja el (esetleg figyeli az eszköz állapotát, arról információkat nyújt a külvilágnak) - http://hu.wikipedia.org/wiki/Firmware

DDoS támadások a közösségi médiában

2011. második negyedévében az orosz internet felhasználók biztosan emlékeznek a LiveJournal ellen indított támadás sorozatra. A weboldal népszerű a háziasszonyok, a fotósok, a pilóták sőt a politikusok körében, akik blog bejegyzéseket írnak. A Kaspersky botnet monitoring rendszerének adatai szerint, a LiveJournal ellen intézett masszív támadások a politikai természetű folyóiratok célbavételével kezdődtek, különösen a korrupcióellenességéről ismert politikai aktivista, Alexey Navalny ellen.

A Kaspersky botnet monitoring rendszere az Optima nevű botnet tevékenységét követte, amelyet a LiveJournal elleni DDoS támadáshoz használtak. Március 23. és április 1. közötti időszakban az Optima parancsokat kapott, hogy támadjon meg korrupcióellenes oldalakat, mint a http://rospil.info, a http://www.rutoplivo.ru és a http://navalny.livejournal.com, továbbá egy bútorgyártó weboldalt a http://www.kredo-m.ru-t. Bizonyos napokon csak a http://navalny.livejournal.com volt a támadás célpontja. Április elején a botnet parancsot kapott arra, hogy kezdeményezzen támadást a LiveJournal-on fellelhető olyan weboldalcímek ellen, amelyek többnyire népszerű blogger-ekhez tartoznak.

Az Optima nevű botnetet már 2010. vége óta ismerik a piacon. A kód típusa alapján kijelenthető, hogy az Optima botokat oroszul beszélő kártékony szoftver írók fejlesztették és ezt többnyire orosz nyelvű fórumokon értékesítették. Nehéz meghatározni a botnet méretét, mert erősen szegmentált. Ugyanakkor, a Kaspersky monitoring rendszere több esetben is azt rögzítette, hogy az Optima botok a LiveJournal weboldalt támadták úgy, hogy parancsot kaptak más kártékony kódot tartalmazó program letöltésére. Ez azt sugallja, hogy az Optima botnethez több tízezer gép tartozik, mivel az ilyen letöltési mechanizmusok kis méretű botnet hálózat esetén nem gazdaságosak.

Nem egyértelmű a LiveJournal ellen indított támadás motivációja, mivel senki sem vállalta a felelősséget. Így amíg a támadás mögött meghúzódó kiberbűnözőket nem azonosítják, addig nehéz lesz megmondani, hogy a támadásokat megrendelésre követték el vagy csak egyszerűen erődemonstráció volt.

Egyre gyakoribb a közösségi médiát ért DDoS támadások száma, mivel ezek az oldalak és szolgáltatásaik közvetlen információ cserét tesznek lehetővé több tízezer felhasználó számára. Így ezek blokkolása, még ha rövid időre is, csak DDoS támadások segítségével érhető el.

A Kaspersky szakemberei a jövőben további növekedést jósolnak az ilyen típusú támadások számosságában.

Kereskedelmi DDoS támadások

A bűnözők továbbra is aktívan használják a DDoS támadásokat. A támadások mögött meghúzódó cél a szervezetek zsarolása, de ezeket a támadásokat a szervezetek ritkán hozzák nyilvánosságra, vagy ha nyilvánosságra is hozzák, akkor legtöbbször már csak a nyomozás elindításáról érkezik információ.

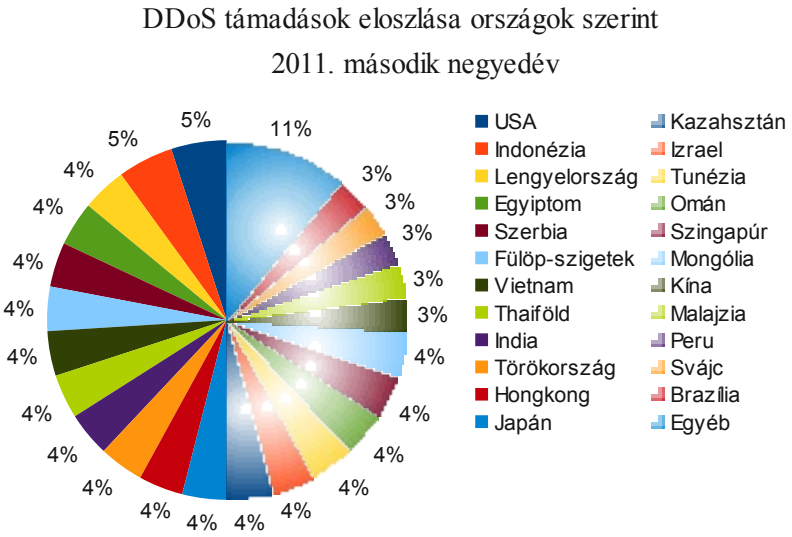
Áprilisban egy düsseldorfi bíróság ítéletet hozott egy kiberbűnöző ügyében, aki megpróbált zsarolni hat német fogadóirodát a 2010-es labdarúgó világbajnokság alatt. A vádlott a megszokott módszereket használta: megfélemlítés, próbálkozásos támadás (trial attack) az áldozat weboldalán, és egy üzenet, amely egy váltságdíj követelést tartalmazott. A hatból három fogadóiroda beleegyezett abba, hogy fizetnek a támadó részére. A fogadóirodák szerint a pár órára leállított weboldal jelentős anyagi kárt okozott - a nagyobb fogadóirodák számára 25-40 ezer eurót, míg a kisebbek számára 5-6 ezer eurót. Meglepő módon a csaló csak 2000 eurót követelt, melyet U-cash utalvány formájában kapott meg. Ez olyan módszer, amely a jól ismert GpCode trójai program megalkotója már használt.

A bíróság a vádlottat közel három év börtönre ítélte, amely az első alkalom a német jog történelmében, hogy valakit azért ítéltek börtönbüntetésre, mert DDoS támadást szervezett. Az ország bíróságai most már az ilyen támadásokat számítógépes szabotázsként minősítik, amely akár 10 év börtönnel is büntethető.

Júniusban, az orosz igazságszolgáltatási rendszer is foglalkozott a DDoS támadások tárgyával. Június 24-én egy moszkvai bíróság Pavel Vrublevsky letartóztatását szentesítette, aki Oroszország legnagyobb internetes fizetési szolgáltatójának, a ChronoPay-nek tulajdonosa. Vrublevsky-t azzal vádolták, hogy DDoS támadást szervezett egy versenytárs cég, az Assist ellen, annak érdekében, hogy aláássák esélyeit egy tender kapcsán, amely egy jövedelmező szerződés volt, az Aeroflot (Oroszország legnagyobb légitársasága) kifizetéseinek feldolgozására. A nyomozóhatóságokhoz közel álló források szerint Vrublevsky neve is felmerült, mint lehetséges tulajdonosa az Rx-Promotion cégnek, amely gyógyszeripari spamek terjesztésére szakosodott.

DDoS támadások eloszlása országok szerint

A statisztikák szerint 2011. második negyedévében a DDoS támadások forgalmának 89%-a 23 országban generálódott. A DDoS források eloszlása meglehetősen egyenletes ezen országok között, amelyek 3-5%-ot tesznek ki.



A legtöbb támadás az Egyesült Államokból és Indonéziából érkezett, mindkét ország 5-5%-ot tesz ki az összes DDoS támadás forgalmából.

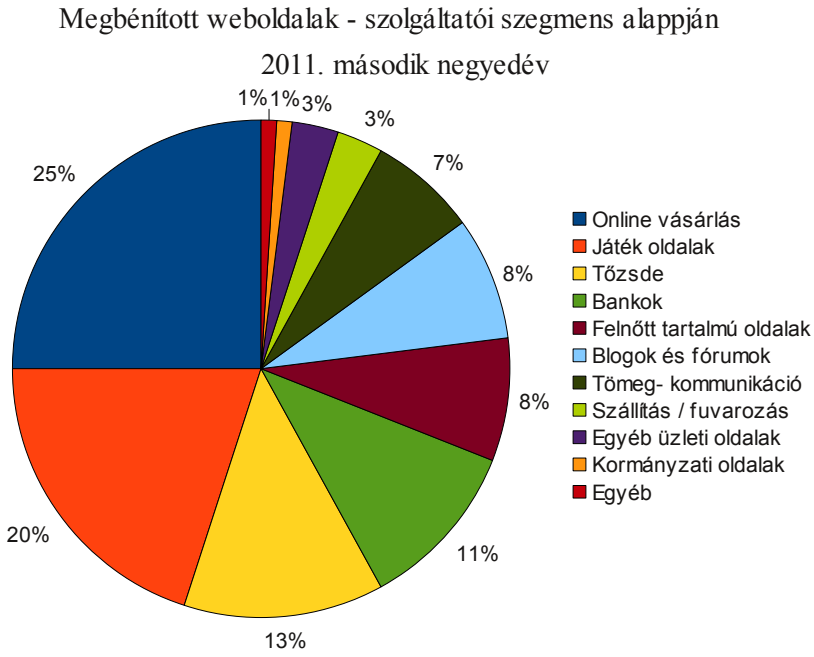
Az Egyesült Államok vezető pozíciója abból származik, hogy az országban szinte mindenki rendelkezik számítógéppel. Tavaly az amerikai bűnüldöző szervek sikeres anti-botnet kampánya, számos botnet felszámolását eredményezte. Nem kizárt, hogy a kiberbűnözők megpróbálják visszaállítani az elveszett botnetek kapacitását és így a DDoS támadások száma növekedni fog.

A DDoS forgalom ranglistáján Indonézia vezető helyéhez, a nagy számban megfertőzött számítógépek vezettek. 2011. második negyedévében szinte minden második gép (48%) ki volt téve helyi kártevő (malware) fertőzési kísérletnek a Kaspersky Security Network, Kaspersky Lab's globálisan-elosztott fenyegetettség monitoring hálózat indonéz szegmensében. A blokkolt helyi fertőzési kísérletek ilyen magas százaléka a védtelen számítógépek nagy számosságában mutatkozik, amelyeket kártevők terjesztéséhez használnak fel.

Azok az országok felelősek az összes DDoS forgalom kevesebb mint 3%-áért, melyek esetében magas az egy főre jutó számítógépek száma és ezzel együtt az informatikai biztonság (Japán, Hong Kong, Szingapúr), valamint azok ahol az egy főre jutó számítógépek száma lényegesen alacsonyabb, de a vírusvédelem messze nem tökéletes (India, Vietnám, Oman, Egyiptom, Fülöp-szigetek, stb.).

A megtámadott weboldalak eloszlása online aktivitás szerint

A második negyedévben, az online kereskedelmi oldalak, beleértve e-üzletek, aukciós oldalak, adás-vételellel foglalkozó oldalak stb., egyre inkább kerülnek a kiberbűnözők célpontjába. Az említett kategóriákba tartozó weboldalak az összes támadás egynegyedét szenvedték el. Ez aligha meglepő, hiszen az online kereskedelem nagymértékben függ a weboldal rendelkezésre állásától és minden kiesett óra a profit és a kliensek elvesztését okozza. Ez magyarázza, hogy miért ezeket a weboldalakat támadják legtöbbször – ezen támadások mögött általában a versenytársak vagy egy egyszerű zsarolás húzódik meg.



A második legnépszerűbb célpontok a játékokkal összefüggő weboldalak voltak. Mivel a Kaspersky Lab monitoring rendszere azt mutatja, hogy legtöbb támadást az EVE Online és az ehhez kapcsolódó oldalak szenvedték el. Ez az űr-témájú MMORPG[3] játék 2010. végén 357 ezer aktív játékossal rendelkezett. Az egyik olyan oldalt érte az egyik legkitartóbb támadás, amely az EVE Online híreivel és tapasztalataival foglalkozik. Az oldal 35 napig volt DDoS botok célpontja. A WoW (World of Warcraft) és a Lineage is „kapott" némi nem kívánatos kiberbűnözői figyelmet, annak ellenére, hogy ezeket a játékokat kalóz szerverek üzemeltették.

A harmadik és negyedik helyet az elektronikus tőzsdék és a bankok weboldalai foglalják el. A kiberbűnözők abból a célból támadják a kereskedelmi platformokat, hogy csalárd ügyleteik után fedezzék nyomaikat, inkább mintsem kicsikarják a pénzt. Egy ilyen támadás során jellemzően mind a pénzügyi szervezetet, mind ezek ügyfeleit anyagi kár éri. Így ezen cégek számára a szolgáltatásaik a DDoS támadásokkal szembeni ellenállása egy olyan faktor, amelynek közvetlen hatása van a jó hírnévre.

Érdekes, hogy a DDoS támadások jelentős része a tömegkommunikációs oldalakat (7%), valamint a blogokat és fórumokat (8%) érte, amelyek lényegében egyfajta szociális tömegkommunikációs médiának tekinthetőek (lsd. LiveJournal-t ért támadás fentebb). Mindig van olyan, aki nem ért egyet a szólásszabadság keretein belül kifejtett véleménnyel és ez megmutatkozik abban, hogy napjainkban a DDoS támadásokat az egyes média csatornák elnémítására is felhasználják.

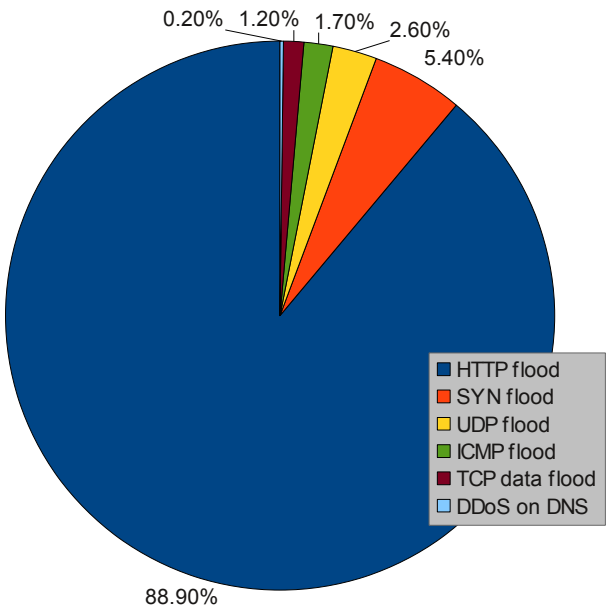
Az összes megtámadott weboldal csupán 1%-át teszik ki a kormányzati oldalak, bár ez a statisztika nem tartalmazza az Anonymous csoport által végrehajtott támadásokat, amelyekhez az „önkéntes" alapon működő botnet hálózatot, a LOIC-ot[4] használták. Több országban is megfigyelhető, hogy a DDoS támadásokat egyre gyakrabban használják arra is, hogy tiltakozzanak a kormányzati szervek ellen, és a szakemberek arra számítanak, hogy a jövőben több hasonló támadás lesz a politikai folyamatok kritikus szakaszaiban.

3 Massively Multiplayer Online Role-Playing Game
4 „Low Orbit Ion Cannon"

A DDoS támadások típusai

2011. második negyedévében a Kaspersky Lab botnet monitoring rendszere által elfogott, több mint 20 ezer web-borne (web-eredetű) parancs kezdeményezett támadásokat különböző weboldalak ellen.

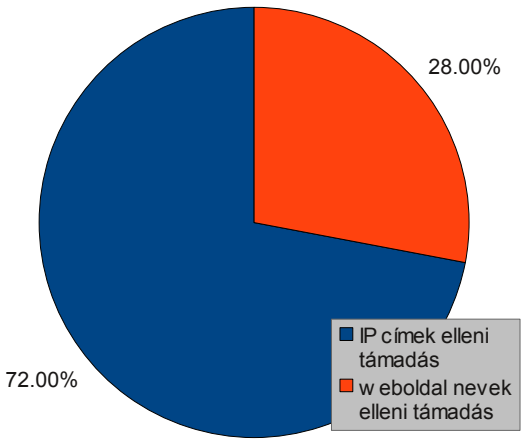
DDoS támadások típusai



A HTTP Flood a legnépszerűbb (88,9%) módszer a weboldalak támadására, igen rövid idő alatt, igen nagy számban küldenek HTTP kéréseket a támadott weboldal felé. A legtöbb esetben úgy néznek ki, mint a megszokott felhasználói kérések, így ezeket nehéz kiszűrni az oldal felé irányuló normál forgalomból. Éppen ezért a DDoS támadás ezen típusa meglehetősen népszerű az internetes bűnözők körében.

A SYN Flood támadás a második legnépszerűbb támadási típus (5,4%). Az ilyen támadások alatt, a botnetek több adat csomagot küldenek a webszerver irányába, annak érdekében, hogy TCP kapcsolatot létesítsenek. A szervek visszaigazolására vár, amit a támadó nem küld el, így a kapcsolatok inkább félig nyitottak, mintsem teljesen felépítettek. Mivel a szerver csak bizonyos mennyiségű kapcsolatot képes kezelni és a botnetek sok kérést képesek generálni rövid idő alatt, így a szerver hamarosan alkalmatlanná válik több kérés kezelésére. Így az oldal elérhetetlenné válik a „normál felhasználók” számára.

DDosS támadások által megbénított célpontok



A DNS szerverek ellen (0,2%) irányuló DDoS támadások voltak a legkevésbé „népszerűek”. Az ilyen jellegű támadások eredményeképpen a DNS szerverek nem képesek átalakítani a weboldalak neveit IP címekké, így a célszerver által kiszolgált oldal elérhetetlenné válik a látogató számára. Ezen típusú támadás különösen nagy kárt tud okozni, ugyanis egyetlen támadás képes elérhetetlenné tenni több száz vagy akár több ezer weboldalt.

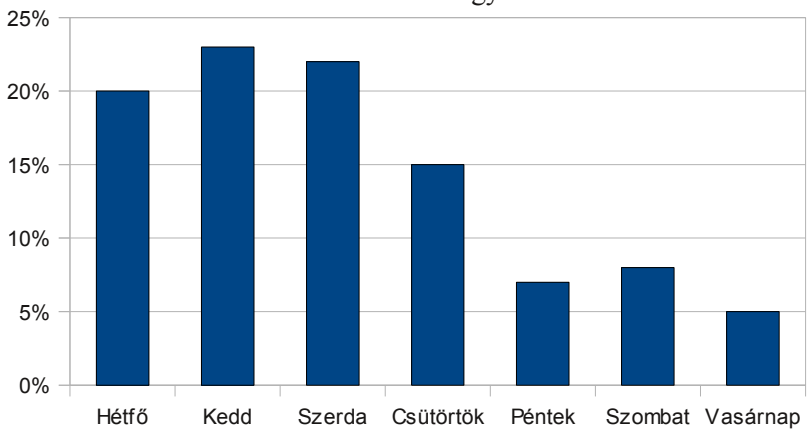
Egy web-erőforrás ellen irányuló DDoS támadás alatt, a bot-ok parancsokat kapnak kérések elküldésére - a célba vett weboldalhoz képest átlagosan két weboldalnyi kérés. Ha összehasonlítjuk az oldal nevek és azok IP címeik ellen végrehajtott támadások számát, akkor azt látjuk, hogy leggyakrabban az IP címeket támadják meg az esetek 72%-ában.

A DDoS botnetek aktivitása az idő függvényében

Az összes rendelkezésre álló adat elemzése után megállapíthatjuk, hogy a kiberbűnözők a hét mely napjain lehetnek képesek a legnagyobb hatékonysággal kivitelezni támadásaikat

Látható, hogy a felhasználók az internetet legaktívabban a hét-köznapokon használják. Ezeken a napokon van a legnagyobb igény a webes erőforrásokra, és feltehetőleg a DDoS támadások is ilyenkor okozhatják a lehető legnagyobb károkat. A másik fontos tényező, hogy a hét melyik napján csatlakozik a legtöbb számítógép, tehát ilyenkor a legaktívabbak a botok is. Ennek eredményeképpen, az internetes bűnözők tevékenységeinek csúcsidőszaka hétfőtől csütörtökig tart - ezeken a napokon zajlik le a DDoS támadások 80%-a.

5. DDoS támadások eloszlása a hét napjain
2011. második negyedév



Következtetés

A DDoS technikát régóta használják bűncselekményekre és napjainkban emelkedik azoknak az eseteknek a száma, amelyekben mind a kormányzati, mind a nagyvállalati szektor tevékenysége ellen, tiltakozásul használják a DDoS támadásokat. Az efféle támadások széleskörű nyilvánosságot kapnak a tömegkommunikációban és általában a rendészeti szerveket is nyomozásra késztetik. Így várható, hogy a különböző országok kormányzati testületeihez tartozó oldalak növekvő számban lesznek DDoS alapú támadások célpontjai, hogy a tiltakozások nagyobb nyilvánosságot kapjanak.

Ez nem jelenti azt, hogy a DDoS támadásokat többé már nem fogják erőszakra és zsarolásra használni. Az ilyen incidensek ritkán válnak ismertté, mert az áldozatok féltik a hírnevüket. Az internetes bűnözők növekvő számban használják a DDoS támadásokat elterelő taktikaként, hogy még kifinomultabb támadásokat indíthassanak, például az online banki rendszerek ellen. Ezekre az összetett támadásokra jellemző, hogy elsősorban a pénzügyi intézeteknek, és azok ügyfeleinek okozhatnak jelentős károkat.

A legtöbb weboldalnak számítania kell a DDoS támadások következményeire, ezért sokkal erősebb védelemre van szükségük. Ez különösen igaz a nyári szabadságolási szezon vége felé, amikor is újra több számítógép csatlakozik az internetre, beleértve a botmaster-ek által vezérelt zombi gépeket is, amik a DDoS támadásokat még erőteljesebbé, ennél fogva még károsabbá teszik.

Forrás: http://www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011

A routing tábla birtoklása – Új OSPF támadások Blackhat USA 2011

A cikk az izraeli Technion Műszaki Egyetem Számítástechnikai Tudományok szakán tevékenykedő Alex Kirshon, Dima Gonikman és Dr. Gabi Nakibly által készített „Owning the Routing Table – New OSPF Attacks" című tanulmány alapján készült, melyet Gabi Nakibly 2011. augusztusában a las vegas-i Black Hat konferencián prezentált.

Az Open Shortest Path First (OSPF) a legnépszerűbb belső routing protokoll az Interneten. A célja az, hogy a router-ek egy AS[5]-ben létrehozzák a routing táblájukat, dinamikusan illeszkedve az autonóm rendszer topológiai változásaihoz. A legtöbb AS az Interneten OSPF-et használ. A protokollt az IETF[6] OSPF munkacsoportja fejlesztette ki és standardizálta. A tanulmányozott protokoll a 2. verzió (RFC2328), melyet az IPv4 hálózatokhoz terveztek, mindamellett ez az egyedüli, jelenleg is használatos verzió. A protokoll 3. verzióját standardizálták az IPv6 hálózatokhoz, mely megtartotta a 2. verzió alapvető mechanizmusait.

Az OSPF kapcsolat-állapot routing protokoll, amely azt jelenti, hogy minden egyes router a szomszédos router-ekkel és hálózatokkal való kapcsolatait hirdeti. A router-ek dinamikusan fedezik fel a szomszédaikat a Hello protokoll alkalmazásával, ahol minden egyes router szórja az üzeneteit a helyi hálózaton. A szomszédok felfedezése után a router hirdeti feléjük a kapcsolatait. Ezen hirdetmények neve a kapcsolat-állapot hirdetmény. A hirdetményekben szereplő információnak fontos része a kapcsolatok költsége. A költséget általában a hálózati adminisztrátor állítja be manuálisan. Az autonóm rendszert LSA[7]-kal árasztják el. Amikor egy router az egyik szomszédjától LSA-t fogad, tovább küldi azt a többi szomszédjának. Ilyen módon minden router összeállítja az adatbázisát az autonóm rendszer LSA-iból. Ez az adatbázis azonos minden router esetén. Az adatbázis használatával a routerek teljes képet kapnak az AS topológiájáról. Ez lehetővé teszi, hogy a Dijkstra algoritmussal kiszámítsák a legkevésbé költséges útvonalat az adott router és akármelyik másik router között a hálózaton. Ezekből az útvonalakból – a csomagok továbbításának szempontjából – minden egyes cél esetén kinyerhető a következő router. Ezek a bejegyzések alkotják a routing táblát.

A dokumentumban olyan új támadások kerülnek bemutatásra, melyek az OSPF funkcióit aknázzák ki. A támadási forma megelőzi a korát és új fényt vet az OSPF gyengeségeire. Az összes támadás az RFC2328-ban lefektetett protokoll specifikáció sérülékenységeit aknázza ki. A szerzők kihangsúlyozzák, hogy a támadások nem implementációs sérülékenységeket használnak ki; következtetésképpen mindegyik OSPF router érintett ezekben a támadási formákban. A gyakorlatban a támadásokat a szerzők sikeresen tesztelték Cisco router-eken (IOS 15.0(1)M – az IOS legfrissebb stabil verzióján). A támadások lehetővé teszik egy rosszindulatú entitásnak, hogy perzisztensen módosítsa az AS más router-einek routing tábláit. A módosítással a támadó kezébe veheti a routing folyamat irányítását az autonóm rendszerben, így szabadon változtathatja a szállított csomagok útvonalait. A módosított útvonalaknak globális hatásai is vannak az AS-t illetően, mivel az összes IP csomagot érintik, függetlenül attól, hogy szállítási rétegbeli vagy alkalmazási rétegben lévő protokollról van szó. A routing folyamat vezérlése két elsődleges cél elérését teszi lehetővé. Egyrészt szolgáltatás megtagadást. Ezen cél megvalósításakor a támadó degradálja a hálózat csomag-továbbítási képességét.

5 AS (Autonomous System): Autonóm rendszer
6 IETF (Internet Engineering Task Force): Internet Mérnöki Munkacsoport
7 LSA (Link State Advertisement): Kapcsolat-állapot hirdetmény

Ebben az esetben a támadó a következő támadási vektorokkal számolhat:

1. **Kapcsolat túlterhelés** – nagy forgalom irányítása egy korlátozott kapacitású kapcsolatra. A csomagok elárasztják a kapcsolatot és használhatatlanná teszik azt.
2. **Hosszú útvonalak** – a forgalom feleslegesen hosszú útvonalakon történik. Más szemszögből nézve a hosszú útvonalak túlterhelik az AS-t, mivel több hálózati erőforrást emésztenek fel. Ráadásul nő a késleltetés az átirányított forgalom miatt.
3. **Szállítási hiba** – a forgalom továbbítása olyan router felé történik, mely nem képes a célhoz eljuttatni a csomagokat. A hálózat egyes részei hibásan úgy gondolják, hogy a cél nem elérhető és nem továbbítják felé a forgalmat.
4. **Routolási hurkok** – a router-ek táblái nincsenek szinkronizálva, így a forgalom továbbítása olyan hurkok mentén történik, melyek soha sem érik el a célpontot. Gyakorlatilag, hatásában megegyezik a szállítási hibánál említettekkel.
5. **„Churn”** – A forgalom továbbítása nagyon gyorsan változik, melynek eredményeképpen a hálózat instabillá válik és a torlódás vezérlési mechanizmusok teljesítménye jelentősen csökken.

A támadó másik potenciális célja a lehallgatás lehet. Ebben az esetben a támadó láthatja azt a forgalmat, amihez egyébként nem férhetne hozzá. Ez lehetővé teszi a támadó részére azt, hogy a forgalmat letárolja, esetleg módosítsa azt. Továbbá lehetőség nyílik egyéb támadásokra (pl.: man-in-the-middle). A lehallgatás megvalósítása egyszerűen kivitelezhető a forgalom továbbításával egy olyan hálózat felé, amelyet a támadó irányít.

A tanulmányban a szerzők feltételezik, hogy a támadó képes LSA-ket küldeni a routing tartományba és a router-ek érvényes LSA-ként dolgozzák fel azokat. Ez a feltételezés általában helytelen, ha a támadó a routing tartományon kívül helyezkedik el, mivel a legtöbb esetben a routing tartományok filterezik a kívülről érkező OSPF csomagokat. A támadó átveheti az irányítást egy legitim router-en az AS-ben például egy olyan személy segítségével, akinek fizikai hozzáférése van az eszközhöz. Esetleg egy implementációs sérülékenység kihasználásával, mely kód végrehajtást tesz lehetővé az eszközön. Számos ilyen sérülékenységet publikáltak a közelmúltban. Ez lehetővé teszi a támadónak, hogy olyan OSPF csomagokat küldjenek, melyeket más OSPF router-ek feldolgoznak a támadott AS-ben.

A tanulmányban a szerzők feltételezik, hogy a támadó a következő jellemzőkkel bír:

a) **Elhelyezkedés** – ahogy az előbbiekben már tárgyalásra került, a szerzők feltételezik, hogy a támadó az autonóm rendszer határán helyezkedik el és egy legitim router van az irányítása alatt. Egyéb megkötés nincs, tehát nem feltételezik azt, hogy a támadó az AS-en belül van, illetve a router által az OSPF folyamaton belül betöltött szerepére sincs megkötés (pl.: AS border router).

b) **Források** – a támadó az AS egy átlagos router-éhez képest átlagos sávszéllel, feldolgozási erőforrással és memóriával rendelkezik. Gyakorlatilag a támadó nem képes feldolgozni vagy generálni nagyobb forgalmat, mint a többi router az autonóm rendszerben.

c) **Egyedül cselekszik** – a támadónak csak egy talpalatnyi helye van az AS-ben. Nem terjed ki az egész AS-re és nem irányít más router-eket. Továbbá nem dolgozik össze más támadókkal az autonóm rendszerben. Az összes többi router az AS-ben legitim és „ártatlan”.

Néhány korábban prezentált támadási mód ismeretes, melyek az OSPF protokoll tervezési gyengeségeit használják ki. A legtöbb ilyen támadás a következő támadási vektorok egyikébe sorolható:

1. **Hamis saját LSA-k** – ennél a támadási vektornál a támadó LSA-kat küld az általa irányított router nevében. Ezek az LSA-k hamis információt tartalmaznak. A támadó hamisan hirdetheti, hogy bizonyos csonk hálózatokhoz csatlakozott. Ezzel hamisíthatja a valós vagy hamis kapcsolatok költségeit is. Ezek a támadások viszonylag egyszerűek és könnyen kivitelezhetőek. Ugyanakkor korlátozott hatékonysággal bírnak, mivel a támadó az AS topológiájának csak kis részét képes hamisítani – a közvetlen szomszédsági viszonyt.
2. **Hamis Hello** – ebben az esetben a támadó hamis Hello üzeneteket küld a hozzákapcsolódó hálózatokba. Ezekkel az üzenetekkel a router elhitetheti a hálózaton lévő többi router-rel, hogy léteznek kapcsolatok új szomszédokkal vagy azt, hogy megszakadt a kapcsolat a létező szomszédokkal. A támadásoknak mindössze helyi hatásuk lehet, mivel csak a helyi hálózaton elhelyezkedő router-eket érintik.
3. **Hamis fantom LSA** – ennél a támadási formánál a támadó egy fantom router, azaz egy nem létező router nevében küld ki LSA-kat. Így a támadásnak szélesebb körben érezhető a hatása, mivel az AS topológiájának nagyobb részét érinti. Viszont a hamis hirdetményeknek nincs közvetlen hatásuk a routing táblákra. Ez azért van így, mert az OSPF protokoll elvárja, hogy a kapcsolat mindkét oldaláról érkezzenek hirdetmények. Mivel más router nem hirdeti a fantom router kapcsolatát, így a hirdetményeket figyelmen kívül hagyják.
4. **Hamis peer LSA** – a támadás során a támadó egy létező (áldozat) router nevében küld LSA-kat. A technikát alkalmazva a támadó globális hatást érhet el az AS-en, az autonóm rendszer topológiájának nagy mértékű befolyásolásával. Ezzel módosításra kerülhetnek a routing táblák, mivel más router-ek is hirdetik a kapcsolatokat az áldozat router-rel. A leginkább fájdalmas hátulütője a támadásnak az, hogy a hatás nem perzisztens. A többi router az AS-ben hamis hirdetményekkel árasztja el az autonóm rendszert. Amint az áldozat router megkapja a hamis LSA-t, azonnal korrekciós hirdetményt bocsájt ki – ez a visszavágó mechanizmus. Ez visszafordítja a támadás hatását. Ezért a támadónak újabb és újabb hamisított LSA-kat szükséges küldenie. Ilyen módon a támadó könnyebben észrevehető.

A tanulmányban újszerű támadási forma kerül bemutatásra, amely újonnan talált tervezési hibát használ ki. A fenti támadási vektorokkal ellentétben az ismertetésre kerülő támadások perzisztensen módosíthatják a routing táblákat az autonóm rendszer router-eiben amellett, hogy globális hatással bírnak az AS-re, az AS topológiájának porcióit hamisítják, melyek nem feltétlenül csatlakoznak a támadó router-hez.

Kapcsolódó tanulmányok

Mindössze egy maréknyi olyan tanulmány létezik, amelyek az OSPF biztonságát elemzik. F. Wang és munkatársai a „Secure routing protocols: theory and practice” című technikai riportban egy olyan támadást ismertetnek, ahol egy AS belső router-e border router-ként hirdeti az LSA-kat. Ez megoldható, mivel nem létezik olyan mechanizmus az OSPF protokollban, melynek segítségével autentikálni lehetne a másik router által vállalt szerepet. A támadás ereje abban rejlik, hogy az AS külső LSA-k elárasztják az autonóm rendszert (kivéve a csonkokat) szemben más típusú LSA-kal, ahol is a hirdetés egy területre korlátozódik. A támadás révén a támadó külső célokkal való kapcsolatokat hirdethet (pl.: Google, Facebook stb.). Ennek eredményeképpen a forgalom egy része, vagy egésze a támadó felé irányítható. Így a támadó a forgalmat elnyelheti, lehallgathatja, vagy csak egy hosszabb útvonalon továbbítja. A támadás hátránya az, hogy nem befolyásolja az AS-en belüli célokat, mivel egy router mindig AS belső router-eket preferál.

S. Wu és munkatársai a „Design and implementation of scalable intrusion detection system for the OSPF routing protocol” című tanulmányban olyan támadásokat mutatnak be, ahol az AS egy másik router-e nevében küldenek ki hamisított LSA-t. A támadás minden variánsa visszavágó mechanizmust vált ki az áldozat router-ből. Így a hatás nem lesz perzisztens, ezért a támadónak újból végre kell hajtania a támadást. Egyrészről a támadó instabillá teheti a routing folyamatot az AS-ben, de jelentősen megnő a leleplezésének valószínűsége.

E. Jones és munkatársai az „OSPF Security Vulnerability Analisys” című tanulmányban felmérték az OSPF különböző támadási vektorait, továbbá pár újszerű támadást is ismertettek. Az egyik közülük kijátsza a visszavágó mechanizmust periodikusan küldött LSA hirdetményekkel (1 csomag per 5 másodperc). Ez kikapcsolja a visszavágó mechanizmust, mivel az OSPF standard nem teszi lehetővé egy router számára, hogy ugyanazon LSA példányból kettőt küldjön adott időintervallum alatt. Ezt az intervallumot a MinLSInterval határozza meg, aminek az alapértelmezett értéke 5 másodperc. Mivel a standard meghatározza azt is, hogy a visszavágó mechanizmus csak azután indulhat el, hogy a router feldolgozta és elárasztotta a hamis LSA-t, így ez azt jelenti, hogy az 5 másodpercenként küldött hamis LSA-k esetén az áldozat router visszavágó mechanizmusa harcképtelenné válik. A támadás hatása így perzisztens viszonylagosan magas áron: a támadónak nagy arányban kell hamisított LSA-kkal elárasztania a hálózatot.

Ugyanebben a tanulmányban egy másik támadási forma is bemutatásra kerül, ahol a támadó hamisított Hello üzeneteket küld, és így megváltoztatja a kijelölt router-t a támadott hálózatban, vagy újraállítja a többi router szomszédossági viszonyát a kijelölt router-rel. Mindkét esetben a LAN-on lévő router-ek szomszédossági viszonyát újra kell állítani. Ez egy olyan folyamat, mely több tíz másodpercet vesz igénybe. Ez alatt az idő alatt, a router által hirdetett LAN egy hálózati csonkként fogható fel, amin keresztül nem áramlanak csomagok. Ennek folyományaként más router-ek az AS-ben ismételten újrakalkulálhatják a routing tábláikat.

A tanulmány más típusú támadásai szolgáltatás megtagadást eredményező támadások. Ebben az esetben a támadó elárasztja az áldozat router-t, amely felhasználja a rendelkezésre álló erőforrásait. Ez jelentősen megterheli a router-t és nem lesz képes a funkcióit rendeltetésszerűen ellátni. A támadás során a támadó nagy számú Hello üzenetet bocsát ki, melynek célja az áldozat router. Mindegyik csomag más, hamisított forrás IP címet tartalmaz. Minden egyes ilyen csomag egy új bejegyzést generál a szomszédossági listában. Teletöltve a listát, a támadó megbizonyosodhat arról, hogy az áldozat nem képes feldolgozni az új szomszédok Hello csomagjait a helyi hálózaton. Egy másik támadás során a támadó hibás LSA hirdetményekkel árasztja el az áldozat router-t. Minden egyes hirdetményt tárolni szükséges az LSA adatbázisban, amíg el nem évül (általában 1 órán át). Az adatbázis kapacitásának felemésztésével az áldozat új LSA-k feldolgozására már nem lesz képes. Ezáltal nem fogja tudni követni az AS topológiájában bekövetkező változásokat.

Egy másik, újszerű támadás során a támadó egy AS border router-t személyesít meg, és AS-külső LSA-kat küld, melyek egy népszerű külső hálózathoz tartoznak. A hirdetmények (az LSA Forward mezőjével) azt jelzik, hogy egy népszerű hálózat egy csonka hálózaton keresztül érhető el. Mivel az AS-külső LSA-k nem árasztják el a csonka hálózatokat, ez route-olási hurkot eredményez: a router-ek a csonka hálózaton kívül a csomagjaikat a csonka hálózatba irányítják, míg a belső router-ek a csonka hálózaton kívülre továbbítják azokat.

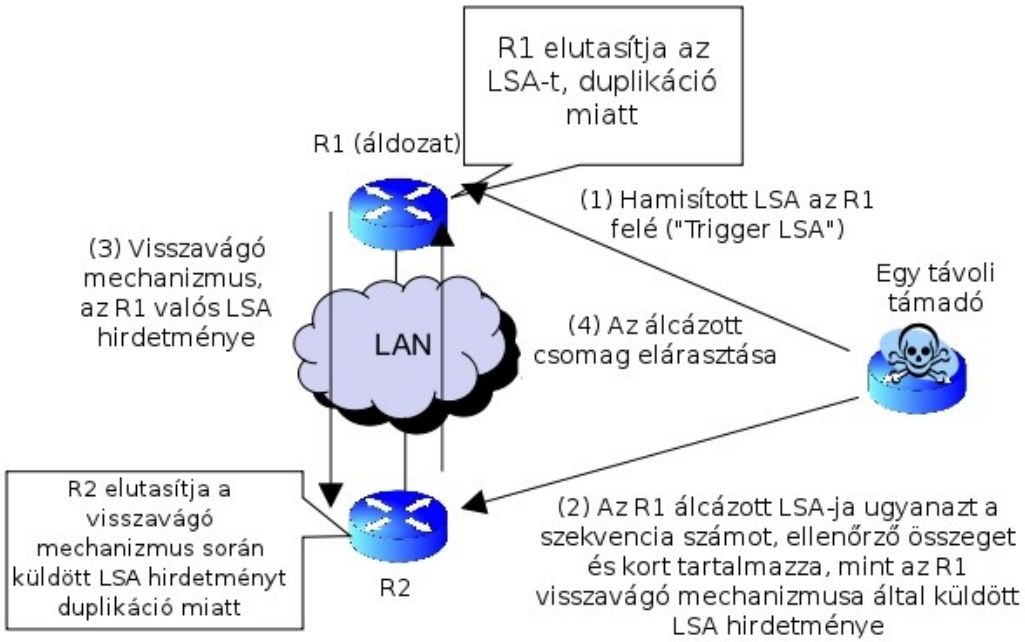
Új támadások

Álcázott LSA

Hivatkozva az RFC2328 13.1. szekciójára, két LSA példány abban az esetben azonos, ha:

1. azonosak a szekvencia számaik (sequence number),
2. azonosak az ellenőrző összegeik (checksum value), és
3. nagyjából azonos korúak (15 percnél nem nagyobb az eltérésük).

Mindez akkor is igaz, ha az LSA tartalma különböző! Minden más router az AS-ben a hamis LSA-kat duplikátumként kezeli, így nem helyezik el azokat az LSA DB[8]-ben. A támadó, hogy áthidalja ezt a problémát, álruhába öltözteti az LSA-t és úgy tüntenti fel azt, mint az áldozat következő érvényes LSA hirdetménye. Amint a támadó elküldi az álcázott LSA-t, kiváltja az áldozatból azt, hogy kibocsájtsa a következő érvényes LSA példányt. Az elsütő szerkezet igen egyszerű, kihasználja a visszavágó mechanizmust. Ugyanis a támadó a hamisított LSA kiküldésével kikényszeríti, hogy az áldozat elküldje – a visszavágó mechanizmus révén – a következő érvényes LSA példányt. A következő ábra illusztrálja a támadást:



1. ábra: Álcázott LSA

(1) A támadó hamisított R1 LSA-t küld R1-nek. Ez biztosan kiváltja R1-ből a visszavágó mechanizmust. Legyen ennek a csomagnak „Trigger” a neve.
(2) Ugyanebben a pillanatban a támadó álcázott R1 LSA-t küld R2-nek. Az álcázott LSA egy különös csomag, melynek megegyezik a szekvencia száma, az ellenőrző összege és a kora (+/- 15 perc) a későbbi R1 által kibocsátott LSA hirdetménnyel. Későbbiekben bemutatásra kerül, hogy hogyan lehetséges megjósolni ennek a három mezőnek a tartalmát.
(3) R1 elküldi a javító LSA-t. Ezt R2 fogadja. Mivel a három mező megegyezik, ezért R2 úgy kezeli, mintha már a fogadott LSA másolatát kapta volna meg. Így nem frissíti vele az adatbázisát és nem fogja ismét elárasztani a hálózatot a csomaggal.
(4) R2 elárasztja az álcázott LSA-t. Ezt fogadja R1, de mivel a három mező megegyezik az általa küldött hirdetményével, ezért a csomagot duplikátumként kezeli és nem vált ki újabb visszavágó mechanizmust.

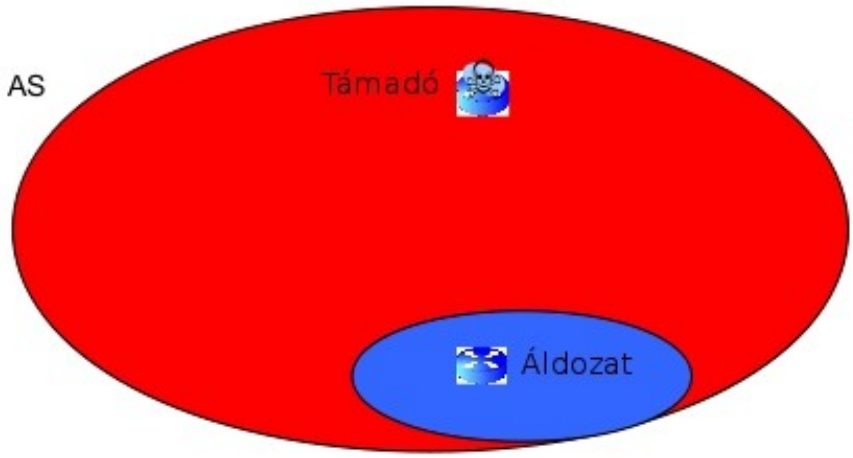
A bemutatott szekvencia után R1 és R2 eltérő LSA adatbázissal rendelkeznek és ez az állapot perzisztens. A router-ek legközelebb akkor szinkronizálnak, amikor R1 hirdetni fogja a következő LSA-t (alapértelmezés szerint 30 perc múlva).

Az álcázott hirdetmény három mezőjének megjóslása a következő módon történhet. A visszavágó mechanizmus során kiküldendő LSA hirdetmények mezői determinisztikusak és előre

8 Database (DB): Adatbázis

meghatározottak. Ezen mezők tartalmazzák a szekvencia számot, a kort és az ellenőrző összeget is. A kor és a szekvencia érték beállítása egyszerű az álcázott csomagban. A kornak '0'-nak kell lennie, míg az időbeli eltérésnek az álcázott csomag és a visszavágó mechanizmus során kiküldött LSA csomag között kevesebb mint 15 percnek kell lennie. A szekvencia számnak eggyel nagyobbnak kell lennie, mint a „trigger" csomagénak. Az ellenőrző összeg generálása kicsit trükkösebb. Az álcázott csomaghoz hozzáadhatunk egy olyan színlelt (dummy) kapcsolat bejegyzést, melynek mezőinek értékei olyan módon választottak, hogy az álcázott LSA ellenőrző összege megegyezik a visszavágó mechanizmus hirdetményével. Mivel az LSA ellenőrző összeg a színlelt (dummy) kapcsolat bejegyzéshez tartozó összes LSA mezők lineáris kombinációja, így könnyedén kalkulálható. Ilyen értékek nagy valószínűséggel léteznek, mivel az ellenőrző összeg mindössze 16 bites, míg 88 bit van a színlelt kapcsolat bejegyzésben, amiket önkényesen állapíthatunk meg (#TOS, metric, Link ID, Link Data). A színlelt kapcsolat bejegyzés maga nem érdekes a számunkra. Mivel a kapcsolat nem kétirányú (más router-ek nem hirdetik a kapcsolat ellentétes irányát), a router-ek nem veszik figyelembe a routing tábla kalkulálásakor.

A fenti támadás sikeres kivitelezéséhez szükséges az, hogy a támadó ismerje az áldozat router kapcsolatához tartozó MD5 kulcsot. A támadás másik alkalmazási lehetősége az, hogy folyamatosan hirdetik a „trigger"-t és az álcázott LSA-t a támadott helyi hálózaton, ahelyett, hogy unicast csomagokat küldenének az áldozat router-nek és szomszédjainak. Így a két csomag elárasztja az AS-t és a router-ek elhelyezik az álcázott LSA-kat az adatbázisaikban. Amint a „trigger" megérkezik az áldozat router-hez, rögtön válaszol rá a visszavágó mechanizmusa révén. A visszavágó LSA-k elárasztják az áldozat szomszédait. Amennyiben már az adatbázisaikba helyezték az álcázott LSA-kat, akkor a hirdetményeket duplikátumként visszautasítják. Mindössze az elsőként beérkező LSA-t tárolják az adatbázisban, a többi elutasításra kerül. Mivel az álcázott LSA jóval hamarabb kerül kiküldésre, mint a visszavágó mechanizmus által küldöttek, ezért nagy eséllyel irányíthatja az AS nagy szeletét. Az alábbiakban látható egy tipikus AS térkép, miután a támadás egy variánsa végrehajtásra került. A piros terület jelöli, hogy a benne lévő router-ek befogadták az álcázott LSA-t, míg a kék rész jelöli azokat a router-eket, amiket hamarabb ért el a visszavágó mechanizmus által kiküldött LSA.



2. ábra: AS térkép a támadás után

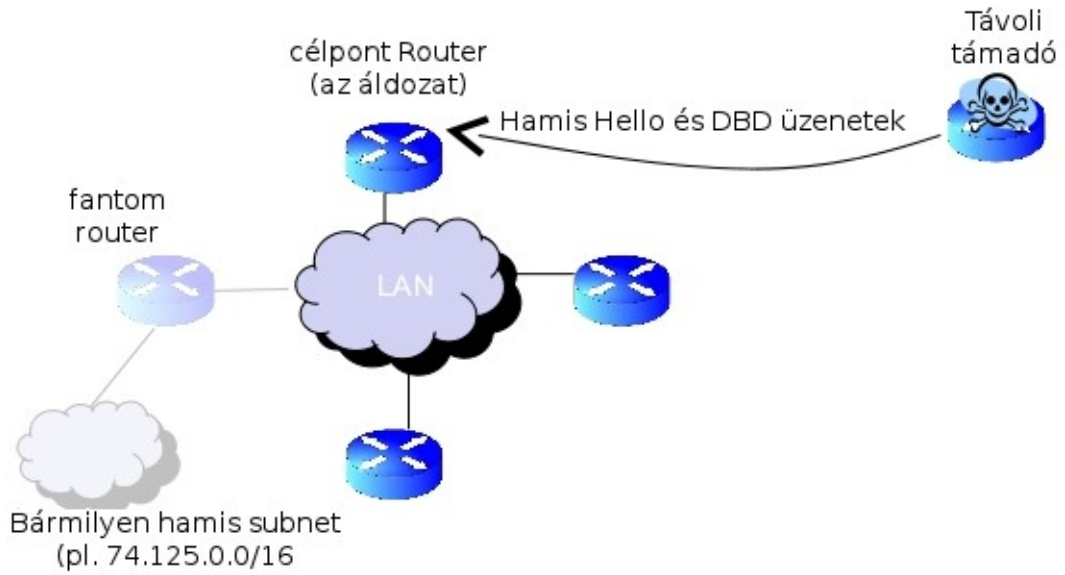
Ahogyan látható, a támadás igen hatékony eszköz ahhoz, hogy a támadó perzisztensen hamisítsa azon router-ek LSA hirdetményeit, melyeket nem kontrollál. A támadó elérheti azt az állapotot, amikor az összes/legtöbb router a routing tartományban az ő irányítása alá kerül. A támadó megismételheti a támadást más áldozat router-eket véve célba, hogy a teljes topológiát az irányítása alá vegye.

Hamis távoli szomszédosság

A támadás által kihasznált sérülékenységet az RFC2328 10.8. szekciója írja le. Ez a szekció bemutatja az adatbázist leíró csomagok küldésének folyamatát a szomszédosság beállításakor. A szekció áttekintése felfedi, hogy a master router sikeresen véghezviheti a szomszédossági beállítást a párja (slave router) üzeneteinek látta nélkül. Ez azt jelenti, hogy a támadó távolról beállíthat egy szomszédosságot az áldozat router-rel, amennyiben az áldozat router „slave" (szolga) szerepkörben van. Mivel az áldozat szomszédjának olyan IP címmel kell rendelkeznie, mely az áldozat kapcsolatának alhálózati azonosítójához tartozik, ezért a támadó egy fantom (nem létező) router-ként jelenik meg az áldozat kapcsolatában. Az áldozat pedig beállít egy szomszédossági kapcsolatot a nem létező router-rel.

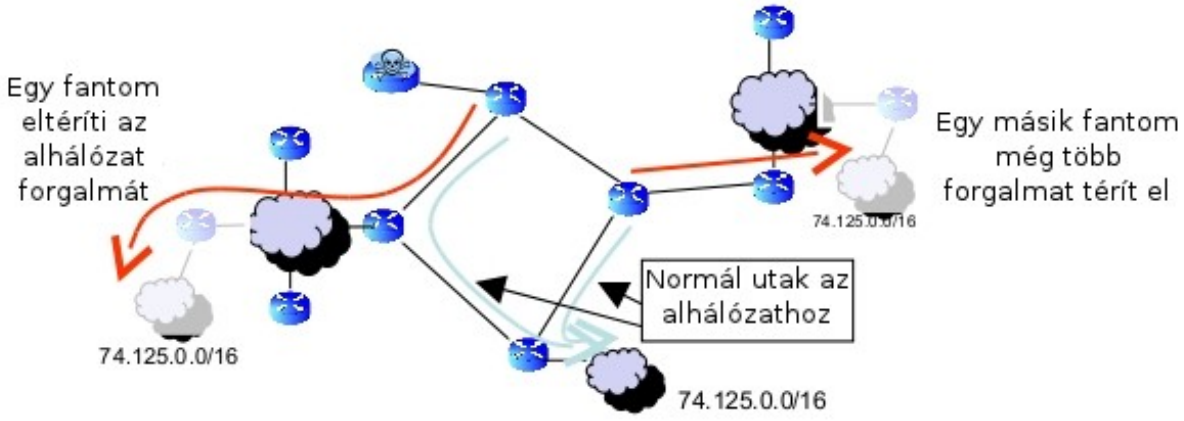
A támadás végrehajtása után az áldozat router szomszédosnak látja magát a fantom router-rel és hirdeti a kapcsolatát a fantom router-rel! Ez lenne a támadás lényege. Amennyiben a támadó hirdetné a hamisított LSA-t a fantom router nevében, mely kapcsolódik az áldozat router-éhez, a hirdetett kapcsolat a fantom router és az áldozat router-e között kétirányú lenne. Ez azt jelenti, hogy minden más router a routing tartományban figyelembe venné a fantom router nevében hirdetett LSA-kat és számolna velük a routing táblájuk kalkulálásakor. A támadó így tetszőleges LSA-t hirdethet a fantom router nevében. Ezek az LSA-k hatással lesznek az AS router-einek routing táblái kalkulálásakor. A támadás sikeres kivitelezéséhez a támadónak a következőket kell ismernie:

1. A távoli LAN MD5 kulcsát. A legtöbb esetben megegyezik az összes LAN osztott kulcsával az autonóm rendszerben.
2. A távoli LAN konfigurációs paramétereit, például: HelloInterval, RouterDeadInterval, stb. A legtöbb esetben ezek azonosak az összes LAN-nál az AS-ben.



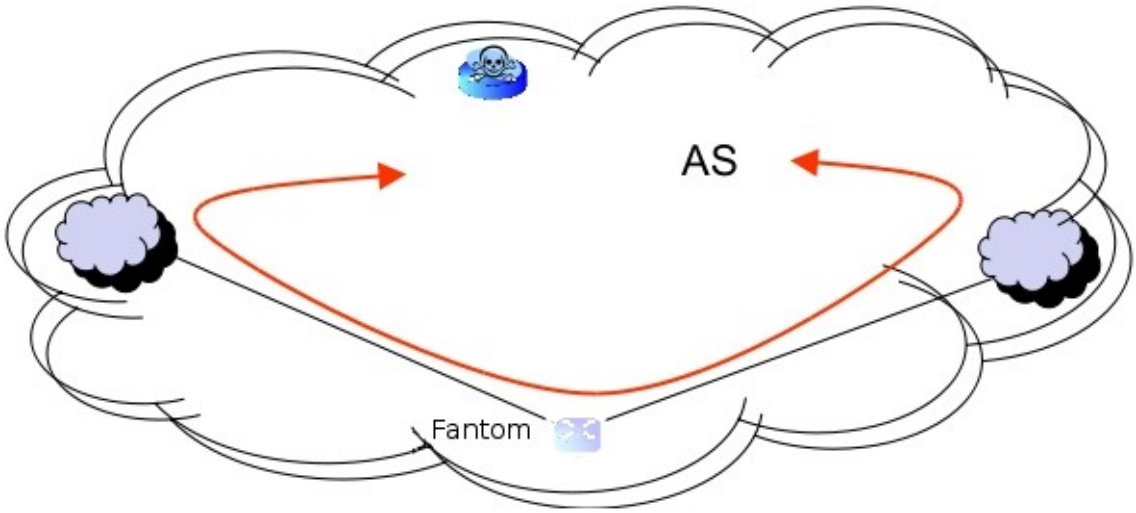
3. ábra: „Távoli szomszédosság" támadás

A támadással elnyelhető egy alhálózat forgalma. Mivel a támadó az AS-ben akárhol elhelyezheti a fantom router-t, gyakorlatilag a hálózat bármely részéről származó forgalmat elnyelheti, melynek célja ez az alhálózat.



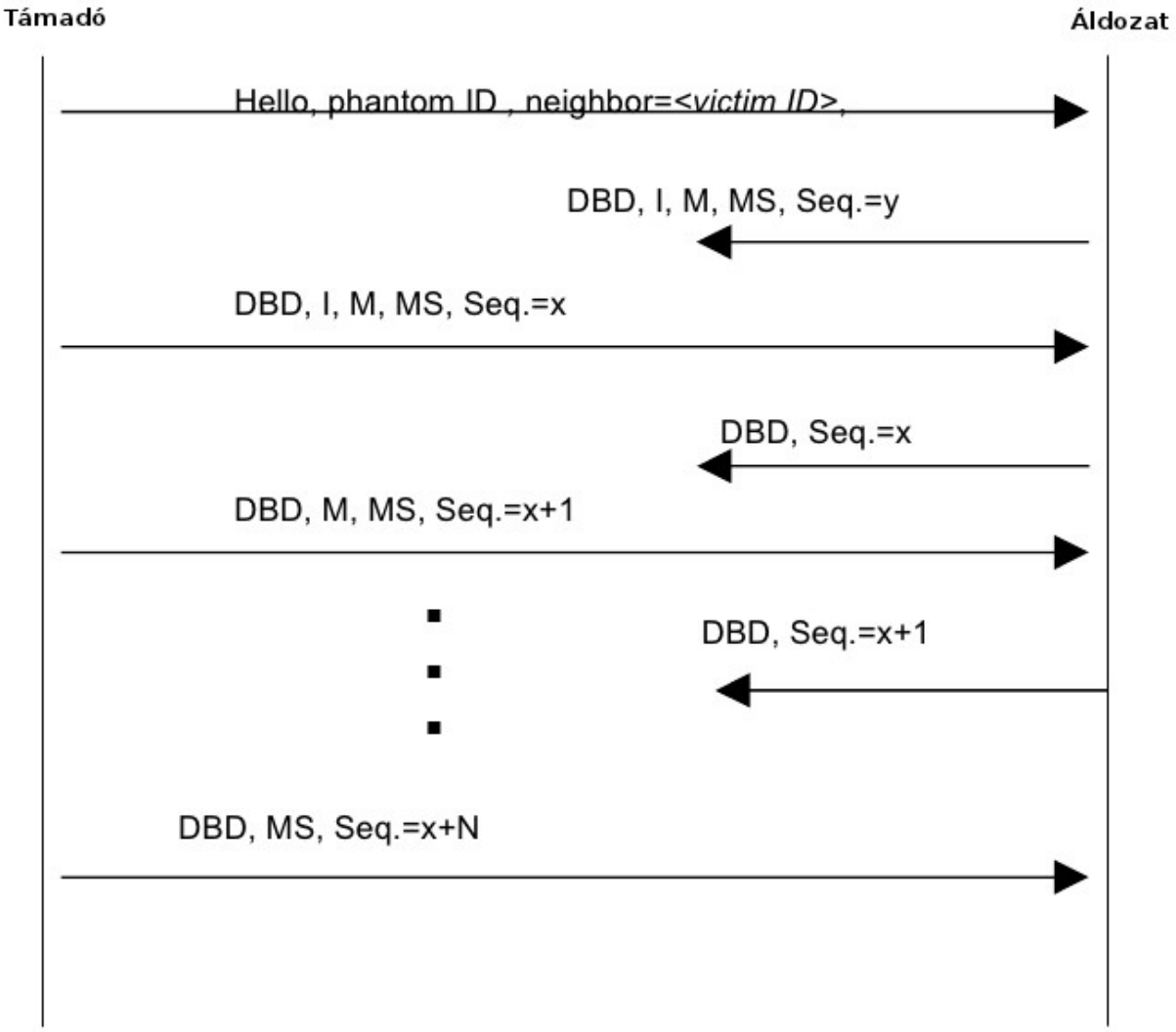
4. ábra: Egy alhálózatot célzó forgalom elnyelése

A támadás arra is használható, hogy elhelyezzünk egy fantom router-t egy stratégiai helyen, amellyel lerövidíthető a csomagok útja az AS-ben. Például két fantom router-rel kapcsolat létesíthető két távoli hálózat között az autonóm rendszerben, ahogyan ezt a következő ábra illusztrálja. Ez könnyen kivitelezhető két áldozat router támadásával a két hálózaton. A két áldozat router-nek kijelölt router-nek kell lenniük a saját szomszédaik részéről.



5. ábra: A fantom router lerövidíti az AS forgalmának jelentős részét

A szomszédosság beállításának folyamata a következő. A támadó által küldött csomagok hamis forrás IP-vel rendelkeznek, melyek megegyezzenek a fantom router IP címével. A címnek illeszkednie kell az áldozat helyi alhálózati címéhez.



6. ábra: A hamis szomszédossági támadás szekvenciája

A támadás Hello csomagok küldésével indul az áldozat router felé. Mivel a Hello tartalmazza szomszédját, az áldozat azonosítót (victim ID), az áldozat két-utas állapotba lép. Az áldozat feltételezhetően a kijelölt router (DR), mivel elkezdi beállítani a szomszédosságát a fantom router-rel, majd ExStart állapotba lép. Majd az áldozat adatbázis leíró (DBD – DB description) csomagot küld saját szekvenciájával (y). A csomagot – mint az áldozat által küldött többi csomagot – a támadó nem fogadja, mivel a fantom router hamis IP címére van címezve az áldozat alhálózatán.

A támadó elküldi első DBD csomagját. A csomag időzítése nem igazán fontos, az áldozat újraadja az első DBD csomagját számos alkalommal, pár másodpercenként (alapértelmezés szerint 5 másodpercenként). A támadó (gyakorlatilag a fantom) első DBD csomagja beállítja az Initialize (I), More (M) és a Master (MS) biteket és beállítja egy tetszőleges értékre (x) a szekvencia számot. Mivel a csomag felépítése különleges, méghozzá olyan módon, hogy a fantom azonosítója nagyobb mint az áldozaté, ezért a fantom router felé az áldozat átengedi a master szerepkört. Ez azt jelenti, hogy az áldozat elfogadja a fantom (x) szekvencia számát és csak azután küldi el a következő DBD csomagot, miután megkapta a fantom DBD küldeményét.

A támadó ezután ismételten DBD-ket küld, növekvő szekvencia értékekkel. A fantom DBD-i nem tartalmaznak LSA-kat, mintha a fantom LSA adatbázisa üres lenne. A támadó folyamatosan küldi ezeket a DBD-ket, hogy lehetővé tegye az áldozat számára, hogy elküldje az LSA adatbázisának

megfelelő LSA-ket. A támadó nem tudhatja, hogy valójában mennyi DBD üzenetet kell az áldozatnak küldenie, hogy megküldje a teljes adatbázisát, ugyanakkor könnyedén behatárolhatja azt (általában 10 DBD üzenet elég). A példában ez a határ N. Nem érdekes, ha N értékkel túllövünk a célon; az áldozat üres DBD-ket küld, ha már nincs kiküldésre váró LSA-ja.

Miután a támadó (fantom) elküldte az utolsó DBD-t (feltételezhető, hogy ekkorra az áldozat is elküldte a saját DBD-it), az áldozat átugorja a betöltési állapotot (Loading State), mivel a fantomnak nincsenek újabb LSA-i, majd az áldozat belép a Teli állapotba (Full State). Ezen a ponton az áldozat teljes mértékben úgy látja, hogy szomszédos a fantommal és ennek megfelelően frissíti a hálózata LSA-ját.

A támadás számos ellentmondással bír:

1. A szomszédosság fenntartása folyamatos Hello üzenetek küldésével történik, minden egyes RouterDeadInterval intervallumban. Alapértelmezés szerint ez az érték 40 másodperc.
2. A szomszédossági beállítást követően az áldozat LSA-kkal árasztja el a fantomot és elvárja, hogy nyugtákat (ACK) kapjon tőle. Az OSPF specifikációnak megfelelően – amennyiben a router nem válaszol nyugtával – az áldozat újra és újraküldi az LSA-kat a végtelenségig. Mindazonáltal a Cisco router feladja ezeket a kísérleteket 125 másodperc után és felbontja a szomszédosságot.

Az utolsó ellentmondás a Cisco router-ek esetében az, hogy a támadást 125 másodpercenként újra kivitelezni szükséges. Ugyanakkor, ha az áldozat és a támadó router ugyanazon a területen helyezkedik el, akkor a támadó ismerheti az áldozat által elárasztott LSA-kat, így hamis nyugtákat küldhet (120 másodperces időkeretben). Ez az elképzelés a gyakorlatban nem volt még tesztelve.

Konklúziók

A bemutatott támadások az OSPF specifikáció (RFC 2328) analízisére épültek. A támadások sikeresek voltak a Cisco IOS 15.0(1)M (7200-series routerek esetén). Ez azt jelenti, hogy a támadások során bemutatott sérülékenységek elvártak és megtalálhatók a Cisco IOS-ben. A támadás során alkalmazott szkriptek igény szerint elérhetők.

A szerzők úgy hiszik, hogy a sérülékenységek és a bemutatott támadások úttörőek. Mostanáig az volt a köztudatban, hogy még akkor sem lehet perzisztensen hamisítani azon router-ek LSA-it, amiket a támadó nem kontrollál, ha a támadó bennfentes. A tanulmány rávilágít erre a tévhitre. A támadások bemutatása során beláthattuk, hogy már egyetlen router segítségével az egész routing tartomány irányítható.

Referenciák

Black Hat USA 2011 (archives)

Owning the Routing Table – New OSPF Attacks

J. Moy, „OSPF Version2”, IETF RFC 2328, 1998. április

F. Wang et. al., „Secure routing protocols: theory and practice”, Technical Report, North Carolina State University, 1997. május

E. Jones et. al. „OSPF Security Vulnerability analisys”, IETF draft-ietf-rpsec-ospf-vuln-02, 2006. június

S. Wu et. al., „JiNao: Design and implementation of scalable intrusion detection system for the OSPF routing protocol”, Journal of Computer Network and ISDN systems, 1999.

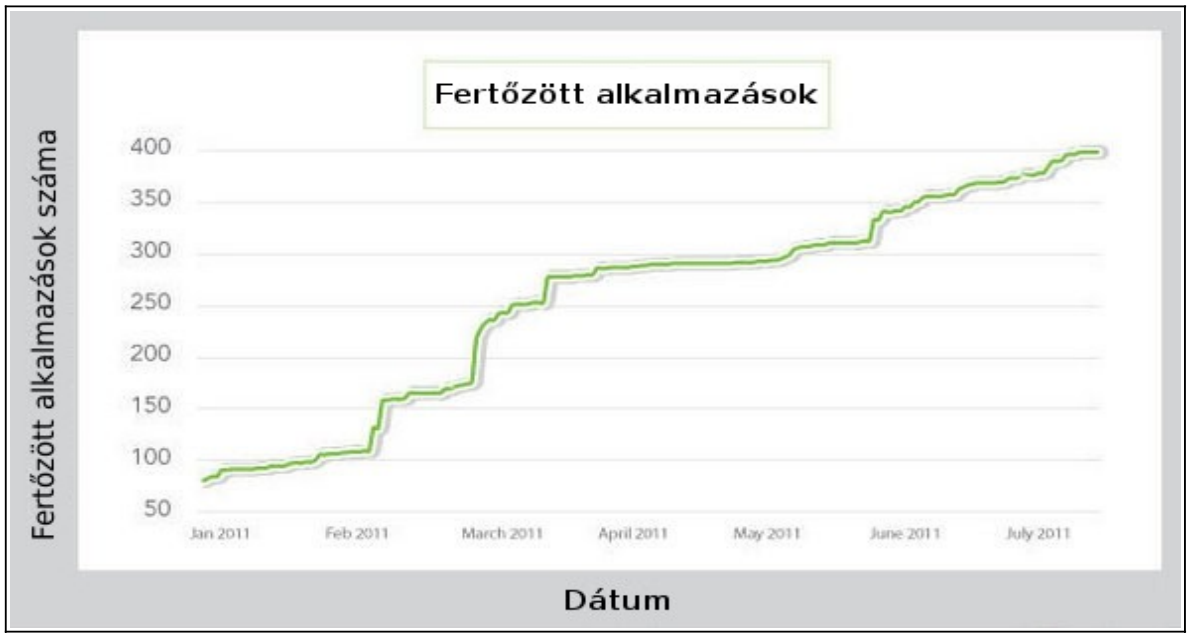
Káros szoftverek az mobil készülékek világában

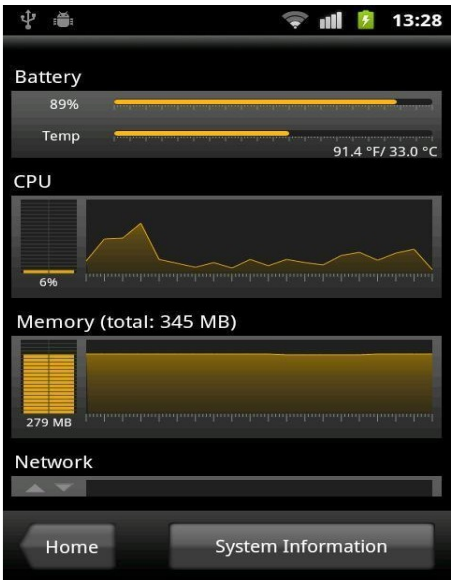
Trendek és tendenciák

Az elmúlt 3 évben az okostelefonok piacán történt robbanásszerű fejlődés egyértelműen kihatással van az IT biztonság világára is. A mobil eszközök látványos fejlődésével a tulajdonosok, ha teljesítményben nem is, de funkcionalitás tekintetében majdnem egy asztali számítógéppel megegyező tudású készüléket tarthatnak zsebeikben. A felhasználók készülékeik segítségével folyamatos összeköttetésben vannak a világhálóval, e-mail üzeneteket olvasnak és küldenek, személyes információkat osztanak meg a közösségi oldalakon, de akár banki átutalásokat is intézhetnek.

Ez a változás azonban nem csak az egyéni felhasználókat, de a vállalatokat is kiemelten érinti. A cégek felfedezték az okostelefonokban rejlő lehetőségeket és igyekeznek azokat a lehető legjobban kihasználni. Például, úgy, hogy saját munkahelyi alkalmazásokat fejlesztenek, hogy így tegyék hatékonyabbá a távoli munkavégzést. Ezzel együtt egyre gyakrabban adnak lehetőséget a dolgozóknak arra, hogy saját készülékeiket használják a munkahelyükön is (BYOD - bring your own device policy szellemében), így a felhasználók egyre gyakrabban férnek hozzá a céges hálózatokhoz és így akár bizalmas adatokhoz is mobil készülékeikről.

Ez a tendencia természetesen a csalók és káros szoftver készítők figyelmét sem kerülte el. A mobil eszközöket célzó káros szoftverek elterjedését a biztonsági cégek már fél évtizede megjósolták és a 2011-es év igazolta is ezeket a jóslatokat. A felmérések szerint a kifejezetten mobiltelefonokat célzó káros szoftverek száma fél év alatt a négyszeresére nőt. Bár az idén megjelent egyedi káros szoftver családok száma még így is valamivel 1000 alatt van, a személyi számítógépeket célzó több tízmillióhoz képest, de a növekedés mértéke mindenképpen figyelemfelkeltő.

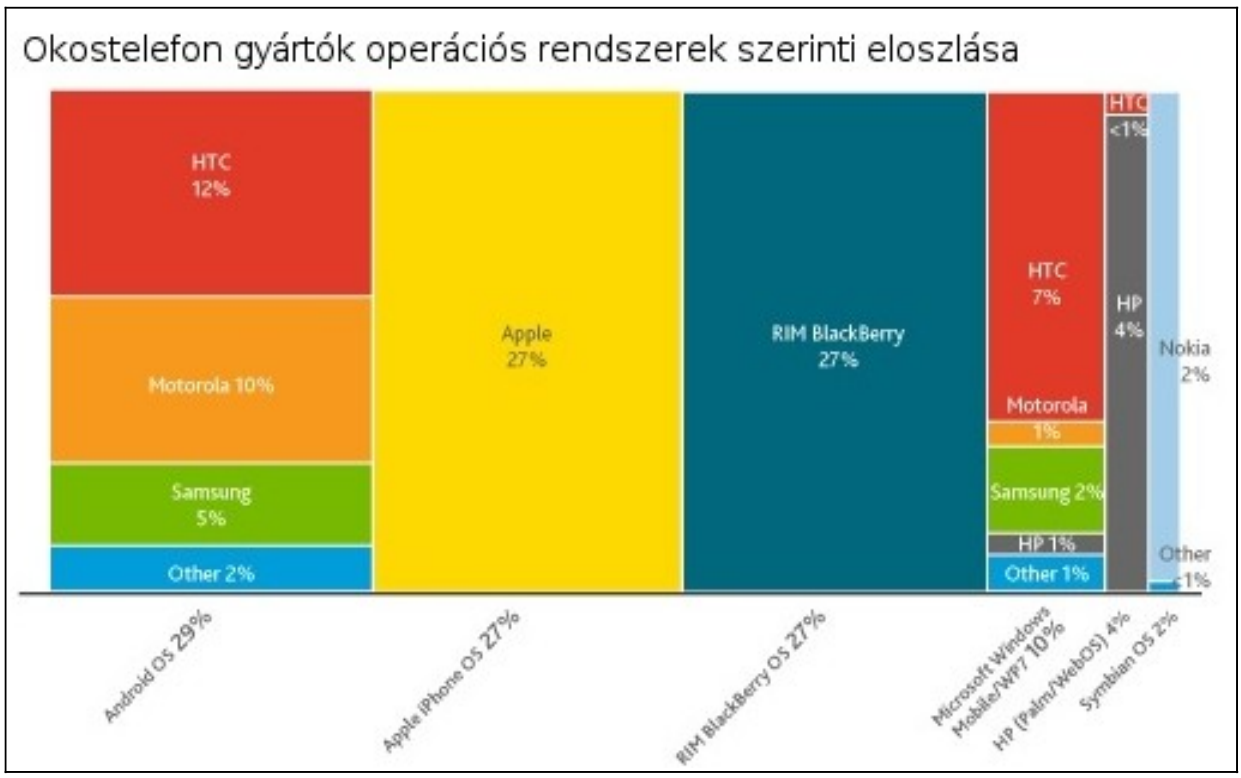


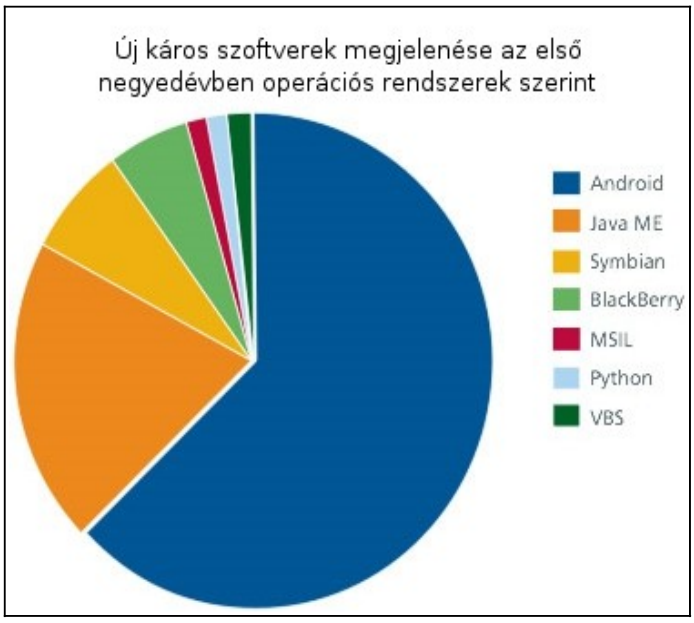


A lassú processzor, az indokolatlanul hamar lemerülő készülék, a gyanúsan kevés memória akár káros szoftver fertőzés jele is lehet, bár a rosszul megírt programok is okozhatnak hasonló hibákat. A káros szoftver fertőzések felfedezésében a különböző erőforrás monitorozó alkalmazások is a felhasználók segítségére lehetnek.

Célpontok

Akár csak az asztali számítógépek világában, az okostelefonok esetében is igaz az, hogy a bűnözők igyekeznek a káros szoftverekkel a lehető legtöbb felhasználót elérni. Éppen ezért a különböző mobil operációs rendszerek népszerűsége összefüggésben van az adott rendszereket támadó vírusok, trójai programok számával. A Nielsen piackutató cég felmérései alapján 2011. elejére a Google Android operációs rendszere jelentős piaci befolyást ért el, és az amerikai piacon nem csak utolérte két legnagyobb riválisát, a Research in Motion BlackBerry-t és az Apple iPhone-t, de meg is előzte azokat.





Ezt figyelembe véve nem meglepő, hogy az Android népszerűségének növekedésével párhuzamosan, jelentősen nőtt a Google mobil operációs rendszerét támadó káros szoftverek száma is, eddig sohasem látott mértékben - egyetlen negyedév alatt 76%-kal - így három hónap alatt az Android lett a legtöbbet támadott mobil operációs rendszer.

A mobil káros szoftverek területén érzékelhető növekvő tendencia egyébként nem csak az Android felhasználókat érinti, hanem ez jellemző általánosan az egész káros szoftver „piacra" is. A biztonsági cégek 2011 első két negyedévében 12 millió egyedi káros szoftver mintával találkoztak, amely 22%-kal több, mint 2010. ugyanezen időszakában. Ez eddig soha nem tapasztalt növekedést jelent a káros szoftverek történetében. Egyes biztonsági szakértők szerint elképzelhető, hogy az év végére akár 75 millióra is növekedhet az ismert egyedi káros szoftver minták adatbázisa.

Célkeresztben az Android

Márciusban a Google ötvennél is több alkalmazást hívott vissza az Android Marketplace-ről miután egy biztonsági kutató felfedezte, hogy egy trójai program látszólag legális programnak álcázva fertőzi a felhasználókat. A DroidDream névre keresztelt trójai - nevét arról kapta, hogy a program este 11 óra és reggel 8 óra között aktív, amikor az átlagos felhasználók alszanak - további káros szoftvereket tölt le a megfertőzött készülékre a felhasználó tudta és beleegyezése nélkül, ami így a bűnözők irányítása alá kerül. A DroidDream a felmérések szerint több, mint negyed millió Android készüléket fertőzött meg.

Vannak olyan káros szoftverek is, amelyek a készülék tulajdonosok mozgása után kémkednek és bizonyos időközönként elküldik a készülék helyzetét egy harmadik fél számára. Az Android.Tapsnake látszólag a klasszikus Snake játék teljesen működő Androidos változata, de háttérben a felhasználó tudta nélkül a program 15 percenként elküldi a fertőzött készülék GPS koordinátáit, egy a készítők által üzemeltetett szervernek.

Az Android.Pjapps - Steamy Window néven - szintén egy létező legitim alkalmazásnak álcázza magát, hogy így vegye rá a felhasználókat, hogy letöltsék azt telefonjukra. Azonban, ha a felhasználó figyelmesen megnézi az alkalmazás telepítésekor, hogy az milyen hozzáférésekhez kér engedélyt feltűnhet, hogy valami nincs rendben. Vajon miért akar egy, a megjelenítést manipuláló alkalmazás személyes információkhoz vagy az SMS funkciókhoz hozzáférni.

Az üzenet küldési funkcióhoz való hozzáférés egyébként jellemző a mobil káros szoftverek nagy részére, egyrészt, mert ez is egy módja annak, hogy a program a készítőivel kommunikálni tudjon, másrészt az emelt díjas SMS szolgáltatások igénybevételével a csalók pénzügyi haszonra is szert tehetnek. Emellett megszokott még, hogy a kártékony alkalmazás a telefonon tárolt adatokat, képeket, üzeneteket, jelszavakat igyekszik a készítők felé eljuttatni, de egyre gyakoribbak a mobilos zombihálózatok, avagy botnetek kialakítására szolgáló káros alkalmazások is.

Tudatosítás

Bár a felhasználók túlnyomó része még nem találkozott káros szoftverrel készülékén, azért, hogy ez így is maradjon, nem csak a biztonsági cégekre, de a felhasználókra is nagy felelősség hárul. Az egyértelműen látszik, hogy a bűnözők és káros szoftver készítők lépést tartanak a technológiák és a technika fejlődésével és ez a jövőben sem lesz másképp. Fontos, hogy a felhasználók körültekintően járjanak el a különböző alkalmazások letöltése és telepítése esetén és, hogy tisztában legyenek a védekezés és megelőzés különböző módjaival és lehetőségeivel.

Források:

http://www.net-security.org/malware_news.php?id=1883

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

http://www.darkreading.com/galleries/security/vulnerabilities/231900951/slide-show-signs-that-malware-could-be-on-your-mobile-device.html?pgno=2

Kitekintés a kiber-bűnözéssel kapcsolatos nemzetközi jogi, nemzetközi büntetőjogi környezetre

Cyber Crime Convention – Budapest, a múlt és a jelen

2001. november 23-án az Európai Unió miniszterei Budapesten aláírták a nemzetközi számítógépes bűnözés elleni egyezményt. A dokumentum megoldást kínált a nemzetközi kiber-bűnüldözés jogi problémáira, az együttműködések továbbfejlesztésére, és lehetővé tette a számítógépes bűnözéssel gyanúsítottak kiadatását, a számítástechnikai rendszerbe betörők kriminalizálását, továbbá egy erős fegyvert adott a pedofil képek terjesztése és az internetes pedofília elleni nemzetközi harchoz.

2011. áprilisában, mintegy előrehozott születésnapi eseményként, a számítógépes bűnözés elleni küzdelemről és az ezzel kapcsolatos együttműködés javításáról tárgyaltak az uniós tagállamok, valamint az Egyesült Államok képviselői a budapesti „Cyber Crime" miniszteri konferencián. Különösen azért vált ez fontossá, mivel a statisztikák szerint az Európai Unió kedvelt célpontja a számítástechnikai bűnözésnek, hiszen fejlett internetes infrastruktúrával rendelkezik, amely folyamatosan fejlődik. Az utóbbi években már a szervezett bűnözői körök is olyan szoftverek fejlesztésére fordították profitjuk egy részét, amelyek megkönnyítik a hagyományos bűncselekmények végrehajtását. A magyarországi Symantec publikussá tett felmérései szerint az elmúlt évben csak Magyarországon 9 milliárd forintnyi kárt okoztak ezek a bűncselekmények. Fontos megemlíteni a budapesti konvenció elfogadottsága kapcsán, hogy már 30 ország ratifikálta azt.[9]

Előkészületben van továbbá egy olyan irányelv, amely korszerűsítené a korábbi, 2005-ös kerethatározatot és bűncselekménynek minősítése terén az eszközhasználatot is kriminalizálná, így a jelszavakkal, számítógépes programokkal, hozzáférési kódokkal való visszaélést is, és kiterjedne a virtuális személyazonossággal való visszaélésre is, továbbá bűncselekménynek minősítené a számítógépes adatok ellopását is.

Az Europol

Cél: a hatékonyabb együttműködés

Az Europol, az Európai Rendőrségi Hivatal 1992-ben jött létre európai bűnügyi hírszerző funkcióval. Központja a hollandiai Hágában van, és személyzete a nemzeti bűnüldöző szervek (rendőrségek, vámhivatalok, bevándorlási hivatalok stb.) képviselőit fogja össze. Az Europol Igazgatótanácsában minden EU tagországból egy-egy képviselő kapott helyet.[10]

Az Europol célja, hogy segítse az uniós tagországok lehető legszorosabb és leghatékonyabb együttműködését a szervezett bűnözés elleni harcban, különös tekintettel az alábbi területekre:

kábítószer-csempészet, bevándorlói hálózatok, gépjárműcsempészet, embercsempészet és gyermekpornográfia, pénz- vagy egyéb fizetőeszköz hamisítása, radioaktív illetve nukleáris anyagok csempészete, terrorizmus.

Az Europol tagállamoknak nyújtott támogatása a következőket foglalja magába: az információcsere előmozdítása az uniós tagállamok között, műveleti elemzés, illetve támogatás biztosítása a tagállamok műveleteihez, szakértelem és technikai támogatás biztosítása az Európai Unión belüli

9 Forrás: http://www.eu2011.hu/hu/hir/kiberbunozes-gyors-reagalasra-van-szukseg
10 Forrás: http://europa.eu/agencies/pol_agencies/europol/index_hu.htm

nyomozásokhoz és műveletekhez, a tagállamok felügyelete és jogi felelőssége mellett;

a tagállamoktól vagy egyéb forrásból származó információk és adatok alapján stratégiai jelentések (pl. veszélyértékelések) és bűnügyi elemzések készítése.

Az Europol további feladata a szükséges adatok bevitelét, hozzáférést és elemzését lehetővé tévő számítógépes rendszer létrehozása és karbantartása. A tagállamonként két-két adatvédelmi szakértőt számláló közös ellenőrző hatóság felügyeli az Europol adatállományában lévő valamennyi személyes adat jogszerű felhasználását.

Az Europol a Bel- és Igazságügyek Tanácsának, azaz a tagállamok bel- és igazságügy-minisztereinek tartozik elszámolással.

Az Europol a kiber-bűnözés, a szerzői jogok megsértése és a készpénzt helyettesítő fizetőeszközökkel való visszaélések visszaszorítása és felderítése érdekében nyilvántartásokat üzemeltet.

Nemzetközi bűnügyi jogsegély intézménye az internetes bűncselekmények területén

A bűnügyi jogsegélyről és formáiról a 1996. évi XXXVIII. Törvény rendelkezik részletesen. Alapvetően akkor beszélhetünk a bűnügyi jogsegély intézményéről, ennek szükségességéről, mikor a magyar rendőrség olyan ügyben folytat nyomozást, melynek egyes elemei külföldön valósultak meg, és a felderítés vagy a bizonyítékok biztosításához szükségessé válik az adott ország rendőri szervének segítsége, eljárása.

A bűnügyi jogsegély alkalmazásának általános feltételei:

Jogsegély iránti megkeresés akkor teljesíthető vagy terjeszthető elő, ha: a cselekmény mind a magyar jog, mind a külföldi állam joga szerint büntetendő, a jogsegély nem politikai bűncselekményre, vagy az azzal szorosan összefüggő egyéb bűncselekményre vonatkozik, illetve nem katonai bűncselekményre vonatkozik, továbbá ha nemzetközi szerződés eltérően nem rendelkezik.

A Magyarországra irányuló jogsegély kérelem akkor nem teljesíthető a hatóságok által, illetve akkor nem terjeszthető elő, ha: csorbítja a Magyar Köztársaság felségjogait, veszélyezteti biztonságát, sérti közrendjét. Ezek az abszolút kizáró okok. Ettől függetlenül, a jogsegély iránti megkeresés teljesítését az igazságügyért felelős miniszter megtagadhatja, ill. a legfőbb ügyész megfelelő garanciákhoz kötheti, a garanciavállalás elutasítása esetén pedig megtagadhatja a teljesítést, ha feltételezhető, hogy a külföldön folyó eljárás, a várható büntetés vagy annak végrehajtása nincs összhangban a magyar Alkotmánnyal, továbbá a nemzetközi jognak az emberi jogok védelmére vonatkozó rendelkezéseivel és alapelveivel.

A bűnügyi jogsegély működése:

A bűnügyi jogsegély formái:

- a kiadatás,
- a büntetőeljárás átadása, átvétele,
- feljelentés külföldi államnál,
- a végrehajtás átvétele, átadása,
- és az eljárási jogsegély

A büntetőeljárás átadása

A mindennapi gyakorlatban a legtöbbször ez az a módja a nemzetközi bűnügyi jogsegélynek, ami alkalmazásra kerül. Amennyiben a nyomozás, büntetőeljárás folyamán olyan gyanú vagy tény merül fel, hogy egy másik ország hatósága is illetékes lehet a nyomozásnál, mérlegelni kell, hogy a nyomozásban való segítséget kér a büntetőeljárást folytató hatóság, vagy átadja az eljárást. Átadáskor a Magyarországon folyó büntetőeljárásnak a külföldi állam igazságszolgáltatása részére való átadásról van szó, melynél a célszerűség a fő szempont.

A célszerűség akkor áll fenn, ha az elkövető Magyarországon van, így az eljárás itt lefolytatható, de indokolt, hogy az állampolgársága vagy az állandó lakóhelye szerinti eljárásban vonják felelősségre, vagy pedig ha nincs Magyarországon és a kiadatásának nincs helye vagy pedig azt megtagadták.

A büntetőeljárás átvétele

A büntetőeljárás átadásához hasonlóan, ilyen esetben a külföldön folyó eljárásnak magyarországi átvételéről van szó.

A külföldi állam igazságügyi hatósága előtt folyó büntetőeljárás akkor vehető át, ha a terhelt magyar állampolgár, vagy Magyarországra bevándorolt külföldi állampolgár. Erről a kérdésről is a legfőbb ügyész elsősorban célszerűségi szempontok alapján dönt.

A Nemzetközi Büntetőjog, a nemzetközi felelősségre vonás szabályai

A nemzetközi büntetőjog fogalma a nemzetközi bűncselekmények meghatározását, az ezzel kapcsolatos felelősségre vonás szabályait öleli fel.[11]

A nemzetközi szintű büntetőjogi felelősség megállapítására jogosult állandó bíróság Hágában jött létre először, (1998. július 17-én fogadták el Rómában a Nemzetközi Büntetőbíróság Statútumát az ENSZ tagállamai) a népirtás, a háborús bűntettek, az emberiség elleni bűncselekmények és az agresszió bűncselekményének elbírálására. Magyarország 2003. november 30-i hatállyal erősítette meg a Statútumhoz való csatlakozását.

A nemzetközi bűnügyi együttműködés szabályai az ún. transznacionális büntetőjog részét képezik, amelynek keretében az egyes államok maguk határozzák meg büntető joghatóságukat, de teret engednek más államok büntető igazságszolgáltatásának is, ennek keretében születtek meg a korábban már ismertetett bűnügyi jogsegély feltételei, megoldásai.

Jogforrási szempontból az egyes államok egymás között megkötött kétoldalú (bilaterális) megállapodásait, illetve viszonossági gyakorlata mellett a multilaterális (többoldalú) szabályozású egyezmények játszanak szerepet a bűnügyi együttműködés bonyolításában.

11 Forrás: http://cograf.hu/tudastar/a-nemzetkozi-buntetojog-fogalma-a-nemzetkozi-bunugyi-egyuttmukodes-forrasai

A VirusBuster Kft. összefoglalója 2011 harmadik negyedévének IT biztonsági trendjeiről

Milyen fontos, netán trendjelző események játszódtak le a nyár végén, az ősz elején az informatikai biztonság területén? Milyen új fenyegetésekkel kell számolnunk, s hogyan igyekeznek védekezni ellenük állami és szervezeti szinten, illetve az otthonokban?

Beszámolónkban nemcsak ezekre a kérdésekre igyekszünk válaszolni, hanem – a VirusBuster Kft. víruslaboratóriumának észlelései alapján – áttekintést nyújtunk a 2011. július-szeptember időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól is.

Az anyag elkészítéséhez felhasználtuk a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ adatait, illetve a szerteágazó nemzetközi kapcsolataink révén begyűjtött információkat is. Bízunk benne, hogy összefoglalónkban mind a szervezeti, mind az egyéni felhasználók találnak számukra hasznos információt.

Államok rémálmai

Izgalmas előadást tartott szeptember elején Londonban *Michael Chertoff,* az Egyesült Államok korábbi belbiztonsági minisztere. Kifejtette: a világháló előretörése „kétségtelenül növekvő kockázatot jelent". „Minél fejlettebb a technológia, annál inkább számíthatunk arra, hogy rendkívül veszedelmes behatolók látogatnak kiberterünkbe" – jelentette ki.

Az amerikai belbiztonsági minisztérium jelenlegi vezetői láthatóan osztják Chertoff aggodalmát. Júliusban arra figyelmeztettek: annyi részlet került napvilágra az eredetileg feltehetőleg iráni nukleáris létesítmények megrongálására kifejlesztett Stuxnet féregről, hogy hackerek viszonylag könnyen elkészíthetik a kártevő valamilyen hasonmását. Márpedig akinek ilyen eszköz van a birtokában, az erőművek, vízszolgáltatási létesítmények és más, a kritikus infrastruktúra részét képező objektumok ellen is bevetheti azt. Nemzetállamok, szervezett bűnöző csoportok, de akár Amerikában élő egyének is „célba vehetik az Egyesült Államok információs infrastruktúrájának elemeit, s így létfontosságú rendszereket állíthatnak le vagy tehetnek tönkre" – fogalmaztak a minisztérium tisztségviselői.

Volt olyan szakértő is, aki nemrég azzal riogatott: ha valaki egy börtön rendszerébe csempészne valamilyen Stuxnet-szerű férget, azzal kikapcsolhatná a riasztókat, sőt ajtókat, kapukat nyithatna ki. Könnyű átlátni, hogy ennek közbiztonsági, de politikai síkon milyen következményei lehetnek.

Nemcsak a nagyhatalmak vezetőit és szakértőit foglalkoztatják ilyen gondolatok. Hasonló problémákat feszegettek szeptember végén a budapesti Arena Plazában is, az immár hetedszer – és nagy sikerrel – megrendezett Informatikai Biztonság Napja (ITBN) egyes előadásain. Így nagy érdeklődés kísérte dr. *Angyal Zoltánnak,* a Puskás Tivadar Közalapítvány hálózatbiztonsági igazgatójának, a CERT-Hungary Központ vezetőjének prezentációját. Szervezetük munkájáról szólva a szakember a kritikus információs infrastruktúra védelmét és a nemzetközi kapcsolatok építését, illetve ápolását nevezte a két legfontosabb feladatnak. Megtudhattuk azt is, hogy tavaly az év szinte minden napjára jutott hazánkban egy incidens – a CERT-nek 2010-ben összesen 306 esettel kellett megküzdenie.

Egy nagyhatalomnak persze nagyságrendekkel több támadással kell számolnia. Vegyük például Kínát, amelyet a világsajtóban az elmúlt hónapokban nem egyszer vádoltak kiberakciók szervezésével. Ám az ottani CERT 2010-et áttekintő jelentése szerint az ázsiai ország kormánya maga is a hackerek kereszttüzében állt. Az augusztusban közzétett dokumentumban az áll: az incidensek száma megközelítette a félmilliót. A támadásokat többnyire trójaiakra építették, s az országon kívülről indították – 14,7 százalékukat az Egyesült Államokból, 8 százalékukat pedig Indiából.

Persze egy kiberháborúban pont az okozhatja a legtöbb fejtörést a stratégáknak: ki is valójában a támadó? A mai napig csak találgatni lehet, milyen szervezet állt amögött a – szakmai körökben Shady RAT néven elhíresült – kémtámadás-sorozat mögött, amely 2006 közepétől 28 hónapon át folyt. Elemzők szerint a kártevőkre épített akciók jegyei arra utalnak, hogy egy nemzetállam kívánt információhoz jutni – mégpedig igen sok helyről. A támadások nem kevesebb, mint 14 országra terjedtek ki. Az áldozatok listája rendkívül változatos: ott találjuk az amerikai szövetségi kormányt, a kanadai, a vietnámi és a tajvani kormányt, az ENSZ-t. Támadás ért 13 katonai szállítót, három építőipari, négy informatikai, valamint több műholdas távközlési céget, sőt, öt sportszervezetet is.

Azt sem tudni bizonyossággal, ki a felelős azért a gigatámadásért, amelyet Dél-Korea szenvedett el júliusban. Az, hogy kínai IP címekről indították az akciót, önmagában nem bizonyít semmit. De mi is történt? Nos, az országban rendkívül népszerű Nate portált, valamint a Cyworld közösségi hálózatot törték fel ismeretlen tettesek. A Cyworldnek 35 millió felhasználója van, s potenciálisan valamennyiük neve, telefonszáma, e-mail címe a hackerek kezére kerülhetett. Más szóval a támadók a 49 milliós Dél-Korea gyakorlatilag teljes internetező táborát egy csapásra „kiütötték”.

Ilyen adatok hallatán nem meglepő, ha egy tanulmányban azt olvassuk: a számítógépes bűnözés már nagyobb tényező a világ gazdaságában, mint a kábítószer-kereskedelem. A marihuána-, a heroin- és a kokain-piacot összességében 388 milliárd dollárra becsülik. Ugyanakkor a kibertámadások világszerte 114 milliárd dollár közvetlen kárt okoztak, amihez ha hozzávesszük a nyomozásra és helyreállításra fordított idő 274 milliárdra becsült értékét, összesen 391 milliárd dollárt kapunk.

Becslések szerint minden másodpercben 14-en – napi több mint egymillióan – esnek valamilyen informatikai incidens áldozatául. Az emberek túlnyomó többsége mégsem látja a kockázatot. Jóllehet egy kutatásban a megkérdezettek 74 százaléka tudott a kiberbűnözésről, 41 százalékuknak nem volt naprakészen tartott védelmi szoftvere, s 61 százalékuk egyszerű, állandó jelszavakkal dolgozott.

A közelmúlt eseményei arra is rávilágítottak, hogy az IT nemcsak a kártevők vagy kibertámadások révén érinti mindannyiunk biztonságát. Emlékezetes, hogy a tavaszi arab forradalmakat jórészt a Facebookon szervezték. Nos, a nyár végi angliai zavargások szítóinak is megvolt a maguk informatikai háttere: a Blackberry okostelefon, illetve a rajta működő (zártkörű) üzenetküldő szolgáltatás, a Messenger.

Pár éve még üzletemberi státusszimbólum volt a RIM cég kézikészüléke. Napjainkra ez a helyzet ugyancsak megváltozott: egy közelmúltban végzett felmérés szerint a brit tinédzserek 37 százalékának a Blackberry az első számú kommunikációs eszköze. Így aztán nem csoda, hogy a rendbontás által különösen sújtott Tottenham parlamenti képviselője egyenesen azt kérte a RIM-től: éjszakára állítsa le a Blackberry Messengert. Erre ugyan nem került sor, ám a cég együttérzését fejezte ki az áldozatok iránt és együttműködést ígért a hatóságoknak. Egy ilyen ígéret nagyon is jól jön a rendőröknek, hiszen a RIM átadhatja nekik – dekódolva – az üzenetforgalmat.

Dekódolni azért kell, mert a Blackberry szolgáltatásnak része az erős titkosítás. Ami az üzletembereknek jól jött, az azonban a világ egyes tájain gondok forrása. Az indiai távközlési minisztérium például már régóta követel a RIM-től hozzáférést az ottani Blackberry forgalomhoz, nemzetbiztonsági érdekekre hivatkozva. Tény, hogy a kontinensnyi országban 500-600 ezerre teszik a RIM készülékeinek számát, s mindannyian emlékezhetünk az ott elkövetett véres terrorcselekményekre. A gyártó több megoldást javasolt, de Indiát egyelőre egyik sem elégítette ki. A hatóságok várhatóan azt követelik majd, hogy a cég állítson fel Indiában szervert, amelyet aztán szükség esetén lehallgathatnak.

Az ötlet nem eredeti: Szaúd-Arábiában ugyanilyen érvek alapján pontosan erre kötelezték a RIM-et. Az Egyesült Arab Emirátusokban viszont egyenesen betiltották a szolgáltatást. A sorba szeptemberben beállt Dél-Afrika, amely ugyancsak hozzá kíván férni az üzenetforgalomhoz.

Bűn...

Az előzőekből is kiderült: a kibertámadások nem állnak meg egy pillanatra sem. Az akciók többségét az anyagi haszonszerzés motiválja, de nem kevés az üzleti és hatalmi érdekből, ideológiai alapon vagy személyes indulatból elkövetett támadás sem. Minél híresebb, nagyobb az áldozat, annál nagyobb port kavar az eset.

Hogy személyekkel – sztárokkal – kezdjük, júliusban *David Beckham* nemcsak azzal került a lapok címoldalára, hogy megszületett az első lánya. Az is bejárta a világsajtót, hogy a világhírű labdarúgó website-ját feltörték, s a látogatót egy ebeledel-reklámposzter elfogyasztásán fáradozó kutya képe fogadta. Nem járt jobban *Lady GaGa* sem, akinek a webhelyéről viszont csodálók ezreinek nevét és e-mail címét szippantották ki a támadók, akik bizonyítékul zsákmányuk egy részét ki is tették a site-ra.

Gazdasági és politikai szempontból persze lényegesen nagyobb súlya van a vállalatok, szervezetek, kormányszervek ellen elkövetett támadásoknak. Míg az előző negyedévnek ilyen tekintetben a Sony volt a főszereplője, most egy másik japán társaságra irányult ez a nem éppen felemelő reflektorfény. A szigetország legjelentősebb katonai szállítójáról, a Mitsubishi Heavy Industriesről van szó, amelynek tíz telephelyére hatoltak be – többek között egy kobei tengeralattjáró-gyárba és egy nagojai üzembe, ahol rakéta-alkatrészek készülnek. Az egyelőre ismeretlen tettesek nyolcféle kártevővel összesen 45 szervert és 38 PC-t fertőztek meg.

Hogy ne ugorjunk túl nagyot, folytassuk a Toshibával! Ennek a cégnek az egyik amerikai szerverét törték fel, ahonnan 7500 ügyfél elérhetőségeit és jelszavát szerezték meg. Szerencsére hitelkártya-adatokhoz nem fértek hozzá.

Egy kicsit tovább lépve Ázsiában, nem hagyhatjuk ki a Hong Kong-i tőzsde esetét. A kontinens harmadik legnagyobb börzéjén egy augusztusi napon kibertámadás miatt fel kellett függeszteni több cég papírjainak a kereskedését.

A Pfizernek a Facebook-oldala esett a magát The Script Kiddies néven jegyző hackercsoport áldozatául. Ugyanez a banda korábban betört a Fox News Twitter-fiókjába, s onnan *Barack Obama* elnök meggyilkolásáról terjesztett rémhíreket.

Spammel szórták meg hackerek a Travelodge nagy-britanniai ügyfeleit. Az utazási szolgáltató biztosította az érintetteket: pénzügyi adatokhoz nem férhettek hozzá a támadók.

Ugyancsak neveket, e-mail címeket zsákmányoltak azok, akik a Nokia egyik közösségi site-jára hatoltak be. Igaz, nem akárkik kontakt-adatait szerezték meg: az információk ugyanis az okostelefon-alkalmazásfejlesztőkre vonatkoztak.

Nem maradt ki az elmúlt negyedév áldozatainak köréből a nyílt szoftver világa sem. A hivatalos Linux kernel szervezet (Linux Kernel Organization) bejelentette: támadók augusztusban több, az operációs rendszer karbantartását, illetve letöltését lehetővé tevő szervert is megfertőztek. A kártevő gyökérszintű hozzáférést szerzett, módosította a rendszer-szoftvert, naplózta a felhasználók tranzakcióit és jelszavát.

...és a bűnhődés

Bár az előző szakaszban többször emlegettünk ismeretlen tetteseket, azért a bűnüldöző szervek munkájának megvan az eredménye. Nagy sikernek könyvelhették el például az amerikai hatóságok, hogy kézre kerítették *Sanford Wallace*-t, aki öt hónap leforgása alatt körülbelül félmillió Facebook-fiókot tört fel, s szerezte meg belőlük a kontakt-adatokat, amelyekre aztán 27 millió kéretlen reklámot küldött ki. A visszaeső spammert három éve a MySpace-en elkövetett hasonló akcióért 230 millió dollár kártérítésre ítélték, két éve pedig a Facebooknak ítélt meg tőle a bíróság 711 millió dollárt. Mindebből aligha fizetett ki egy centet is...

Ugyancsak visszaeső került rendőrkézre Japánban. A 28 éves *Masato Nakatsuji* ráadásul még próbaidejét töltötte azért, mert kártevőt indított útnak a szigetországban népszerű Winny fájlmegosztón. Akkor – 2008-ban – megfelelőbb törvény hiányában szerzői jog megsértése címén ítélték két évi szabadságvesztésre, aminek a végrehajtását három évre felfüggesztették. Azóta – idén júniusban – viszont megszületett a számítógépes vírusok írását büntető paragrafus. Így a férfit most már ennek alapján ítélheti el a bíróság, mégpedig kísértetiesen ugyanazért, mint három esztendeje: a Winnyre rászabadított kártevője ezúttal egy polip képére cserélte le az áldozatok állományait.

Eközben a brit rendőrök három adathalász elfogásának örülhettek. Májusban mindhárman beismerő vallomást tettek, most mégsem maguktól járultak a hatóságokhoz. A vád szerint a trió 900 bankszámlát és 10 ezer hitelkártyát tört fel, s összesen 570 ezer fontot zsákmányolt. Cserébe most összesen 13 évet tölthetnek rács mögött.

Említettük korábban a nyár végi angliai zavargások ügyét. Igaz, nem Blackberryvel, hanem az immár klasszikusnak számító Facebookon buzdított rendbontásra a 20 éves *Jordan Blackshaw* és a 22 éves *Perry Sutcliffe-Keenan*. A bíróság nem bánt kesztyűs kézzel a fiatalemberekkel: négy-négy évre ítélte őket. „Ha visszagondolunk a pár nappal ezelőtti eseményekre, arra, hogyan használták a technológiát izgatásra, bűncselekményeket elkövető csoportok szervezésére, akkor könnyen megérthetjük a ma kiosztott négyéves ítéleteket” – hangoztatta *Phil Thompson* főfelügyelő-helyettes.

Tanulságos egy mexikói tárgyalás is. Nem kevesebbel, mint terrorizmussal és szabotázzsal vádol az ügyész egy 47 éves matematikatanárt és egy 57 éves újságírót. A duó azt írta augusztus végén a Twitteren: kábítószer-maffiózok fegyverrel támadtak egy helyi általános iskolára. Mindebből egy szó sem volt igaz, de a rémült szülők az iskola felé száguldva összesen 26 közlekedési balesetet okoztak. Ugyanolyan pánikot keltettek tehát, mint 1938-ban Amerikában *Wells* a *Világok harca* című regényének túl jól sikerült rádióváltozata – érvelt az ügyész. Akkor az emberek azt hitték, csakugyan marslakók érkeztek a földre.

Bűn és bűnhődés egyaránt megjelenik, csapás és ellencsapás váltja egymást abban a rabló-pandúr történetben, amelynek egyik főszereplője a magát nemes egyszerűséggel Anonymousnak nevező hackercsoport, a másik pedig a fél világ rendőrsége. Az Anonymous a Szcientológiai Egyház elleni – 2008-ban végrehajtott – támadásával kezdte „pályafutását”, igazából azonban tavaly került az érdeklődés homlokterébe, amikor egymás után vette célba azokat a pénzügyi szolgáltatókat, amelyek nem engedtek adományt küldeni az amerikai diplomáciai táviratokat kiszivárogtató WikiLeaksnek.

Persze a társaság tevékenysége igencsak szerteágazó. Hosszú hadjáratot folytattak a fájlmegosztókat kritizáló szórakoztatóipari cégek – leginkább a Sony – ellen. Céltáblájukon volt/vannak az elnyomó rezsimek – korábban Tunézia és Egyiptom, illetve jelenleg is Szíria – pontosabban az ottani webes infrastruktúra elemei. Ellenségnek tekintik a tagjaikat letartóztató államok (például Spanyolország vagy Törökország) kormányát és rendőrségét. Nem kímélik az állami biztonsági szállítókat és más nagy cégeket sem.

Csak a harmadik negyedév krónikájából idézve, megtámadták a Monsanto mezőgazdasági óriást, 8 gigabájtnyi dokumentumot emeltek el az olasz kritikus IT infrastruktúráért felelős kormányszerv, a CNAIPIC rendszeréből, betörtek egy amerikai kormányzati szállító, a Mantech hálózatába, megszerezték 45 ezer ecuadori rendőrtiszt adatait (az ottani kormány fenyegetéseit megbosszulandó), s ha ennyi nem lenne elég, lejáró tartalmat csempésztek a szíriai hadügyminisztérium site-jára.

Mit csinált eközben az ellenfél? Július elején közös olasz-svájci akcióval 15 Anonymous-tagsággal vádolt hackert vettek őrizetbe. Két héttel később az Egyesült Államokban tartóztattak le 16 gyanúsítottat, akik vélhetőleg részt vettek a PayPal elleni tavaly decemberi támadásban. Ugyanakkor brit földön egy tizenévest, Hollandiában pedig négy személyt helyeztek vád alá.

Válaszul a letartóztatásokra, augusztus első napjaiban az Anonymous 10 gigabájtnyi amerikai rendőrségi adatot tett közzé. A csomagba 11 állam 76 rendőrségi site-jából kerültek személyi információk, azonosítók. Nem hiányoztak besúgók és hitelkártyák adatai sem.

Augusztus végén aztán a brit rendőrök három letartóztatást foganatosítottak, legutóbb, szeptember végén pedig Amerikában emeltek vádat egy trió ellen. Ez utóbbi Anonymous-sejt akár 15 év börtönt is kaphat.

A történet folytatására bizonyára nem kell sokáig várni...

Spamesnek áll a világ?

Szokás szerint ebben a negyedévben is minden szenzációszámba menő hírt meglovagoltak a spammerek. *Amy Winehouse* halála után áradtak azok az üzenetek, amelyek az énekesnő kábítószerezését megörökítő videóval kecsegtettek. Gátlástalan bűnözők videofelvételt ígértek a norvégiai vérengzésről is. Nem kerülte el ez a fajta megemlékezés szeptember 11-ét sem, melynek kapcsán többek között „Bin Laden életben van", „Nyomozási eredmények", „Ledőlő tornyok" tárgyú kéretlen levelek szennyezték a világhálót.

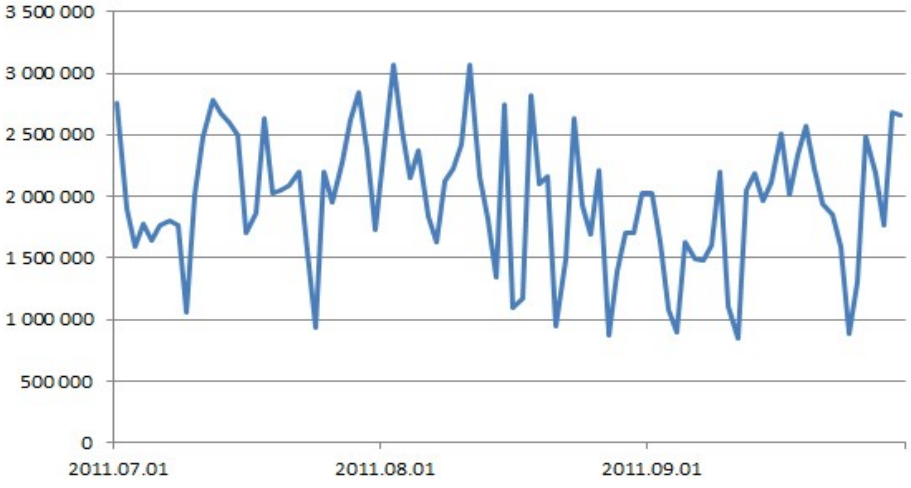
Jóllehet az előbb épp olyasmiről beszéltünk, amit a bűnözők évek óta űznek, a Cisco szakértői júliusban kiadott tanulmányukban rámutatnak: a tömeges „egyen-spammelés" helyett a levél-lovagok mindinkább kisebb volumenű, ámde célzott akciókkal igyekeznek bevételhez jutni. Mint a jelentés szerzői, a személyre szabott támadások üzleti kihatása 2010-ben megháromszorozódott. Ilyen akció áldozata lett egyebek mellett az RSA, a Google vagy a Sony.

Szorul a hurok a tömeges levélszórás körül azért is, mert nagyjából egy év leforgása alatt négy botnetet („zombi" gépekből szervezett, bűnözők által felügyelt robothálózatot) sikerült lekapcsolni. Előbb a Waledac, majd a Rustock botnetet iktatta ki – hatósági közreműködéssel – a Microsoft, aztán az amerikai bűnüldöző szervek csaptak le a Coreflood elnevezésű hálózatra, szeptember végén pedig a Kelihos botnetet tették harcképtelenné. Ez utóbbi ismét a Microsoft érdeme, s egyebek között 21 domain letiltásával járt. Érdekesség, hogy egyikük, a cz.cc egy Csehországban működő ingyenes domainregisztrációs szolgáltatást takart.

A redmondi óriás ráadásul 250 ezer dolláros jutalmat ajánlott föl annak, aki a Rustock üzemeltetőinek nyomára vezeti a rendőrséget. Fénykorában ez a hírhedt botnet jó egymillió gépet tartott rabszolgasorban, s minden idők legnagyobb spamforrása volt.

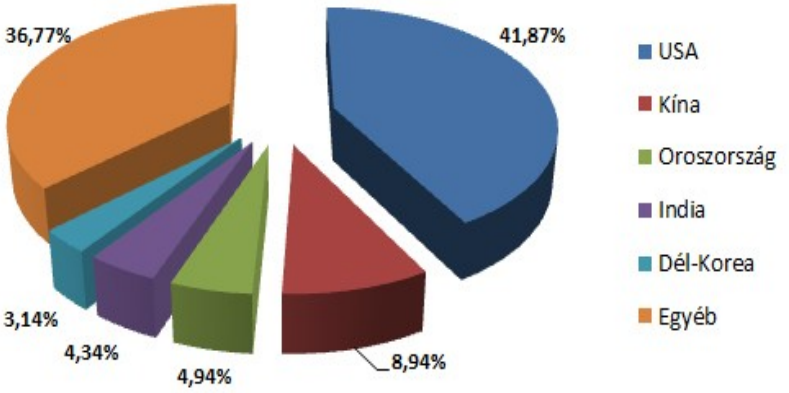
Jó képet kaphatunk a spamhelyzetről a Commtouch adatai alapján.

Az alábbi grafikon a július-szeptember időszak spamkitöréseit mutatja.[12]



12 *Commtouch Software Online Labs*)

A tortadiagramon a legtöbb levélszemetet kiküldő országokat, illetve spamforgalombeli részesedésüket láthatjuk.[13]



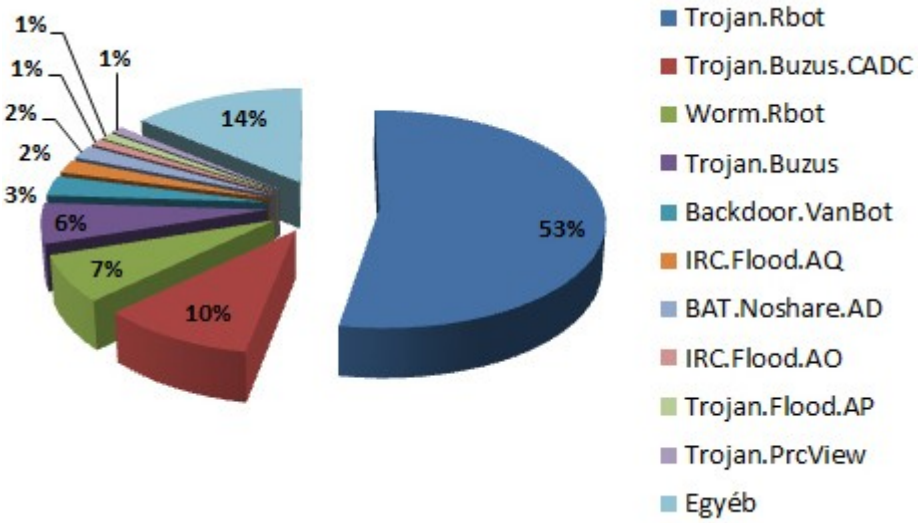
Kiemelkedő kártevők

Természetesen a kártevők áradata a mögöttünk álló negyedévben sem apadt. Ha azonban fontos trendeket szeretnénk kitapintani, akkor nem is annyira a „hagyományos" számítógépek, hanem inkább kistestvéreik, a korszerű okostelefonok, táblagépek felé kell fordulnunk, amelyek rohamos térhódítása kapcsán mind több szakértő fejezi ki aggodalmát a mobilhálózatok biztonsága miatt. „Tovább súlyosbítja a problémát a mobil architektúrák konvergenciája és felhasználói táboruk növekedése. Az interneten 1,5 milliárdnyian vannak világszerte, a mobilosok számát viszont már 5 milliárdra teszik. A bűnözők a profitot keresik. Ha egyszer a mobiltelefonok jelentik a legnagyobb számítástechnikai platformot, akkor nyilván rendszeresen célkeresztbe kerülnek" – jellemezte a helyzetet *Patrick Traynor,* a Georgiai Műszaki Egyetem (Georgia Tech) tanára.

Van szakértő, aki azt jósolja: az Android operációs rendszeren támadó kártevők száma a következő fél évben hatvanszorosára nő. Ma 200 körüli fajt ismerünk – ha az előrejelzés beválik, akkor jövő márciusban már 12 ezer miatt fájhat a fejünk. Zártsága miatt az Apple iOS platformja kevésbé van veszélyben, de elemzők az iPhone, iPod és iPad felhasználókat óvják attól, hogy hamis biztonságérzetbe ringassák magukat.

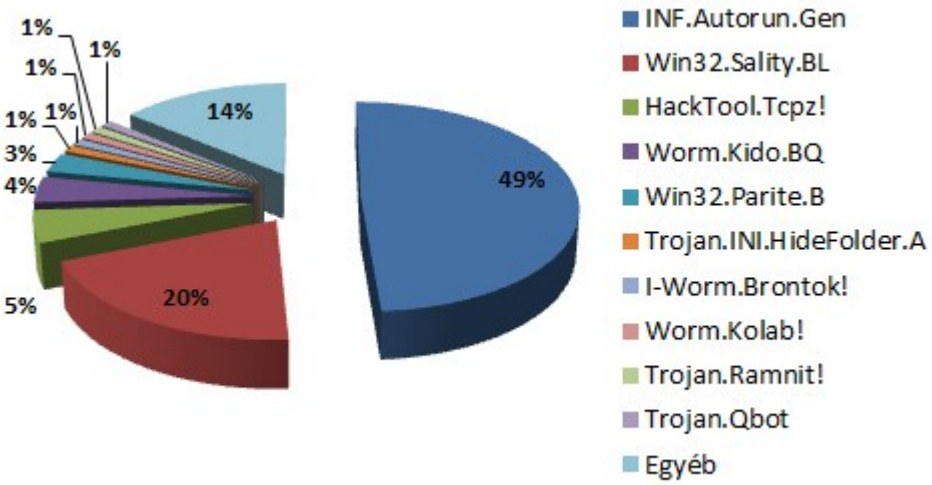
De térjünk vissza a számítógépek világába! Következzenek a VirusBuster havi kártevő-toplistái 2011 legutóbbi negyedévéről. Az alábbi tortadiagramok azt mutatják, hogy az egyes hónapokban melyek voltak a leggyakoribb károkozók a magyar neten.

Július

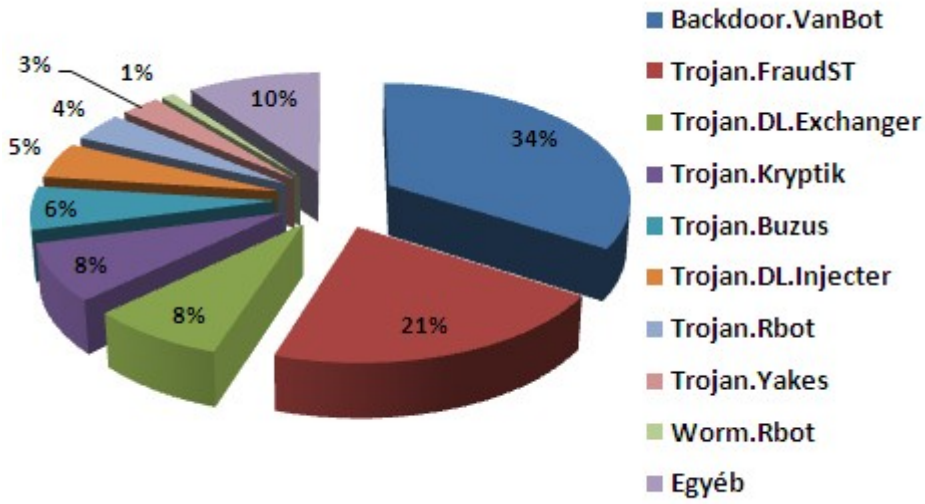


13 *Commtouch Software Online Labs*

Augusztus



Szeptember



Az sem érdektelen, hogy a weben barangolva hol kell leginkább fertőzéstől vagy adathalászattól tartanunk. Napjaink elterjedtebb kártevőit alkotóik weboldalakon keresztül (is) folyamatosan frissítik. A kártevők felismerésének biztosítása érdekében más víruslaborokhoz hasonlóan a VirusBuster is folyamatosan nyomon követi ezeket a webhelyeket. A gyakori frissítések miatt természetesen csak generikus felismerési módszerekkel kezeljük őket, az utánkövető feldolgozás nem szolgálná a felhasználók érdekeit.

Következő táblázatunk július-szeptember legaktívabb kártevőszóró domainjeit foglalja össze.

	Domain	Fájlok száma
1.	origin-ics.hotbar.com	1225
2.	origin-ics.fivemillionfriends.com	760
3.	origin-ics.clickpotato.tv	513
4.	afggxcyayus.com	66
5.	85.17.200.9	64
6.	182.18.185.81	62
7.	dl.dropbox.com	51
8.	d1.youxi.31dj.com	42
9.	origin-ics.brightbreeze.com	36
10.	jabqnhijyus.com	29

Folt hátán folt

A Secunia biztonságtechnikai cég közelmúltban közzétett adatai szerint az elmúlt 12 hónapban a sérülékenységeken belül 24-ről 30 százalékra nőtt a kritikus – rendszerhozzáférést lehetővé tevő – rések aránya. Érthető tehát, hogy a cégek fizetni is hajlandók azoknak a kutatóknak, akik közvetlenül őket értesítik egy-egy felfedezett sebezhetőségről.

A Mozilla és a Google után július végén a Facebook is bejelentette: jutalmat ad a sérülékenységek bejelentőinek. A legkisebb díj 500 dollár, de egy különösen fontos hiba ennek a tízszeresét is hozhatja a kutató konyhájára.

Augusztusban aztán a webes arcképcsarnok nyilvánosságra hozta jutalomprogramja első három hetének mérlegét. Eszerint 16 ország szakembereinek összesen 40 ezer dollárt fizettek ki. Közöttük volt olyan, aki egymaga hat rést jelentett be, s ezért 7 ezer dollár ütötte a markát. Hasonló programjának elindítása óta a Google eddig 300 ezer dollárral jutalmazta a site-jain talált biztonsági problémák felfedezőit.

Ugyancsak augusztusban, de másfajta elismerést hirdetett meg a Microsoft. A 200 ezer dolláros Blue Hat (=kék kalap) díjat az kapja, aki a legjobb „új, futási idejű technológiát dolgozza ki a memóriasérülékenységek kiaknázásának kivédésére”. Az „ezüstérem” 50 ezer dollárt ér, míg a harmadik helyezett 10 ezer dollár értékű MSDN Universal előfizetést kap.

Foltoznivaló tehát volt 2011 harmadik negyedévében is bőven. Az alábbiakban csak az időszakban kibocsátott legfontosabb biztonsági frissítésekről adunk áttekintést, időrendben.

Július

- Havi foltozó keddjén négy javítócsomagot bocsátott ki a Microsoft. Közülük egy kritikus, három pedig fontos besorolást kapott. A foltok a Windowshoz és az Office-hoz készültek, s összesen 22 hibát orvosoltak.
- Az iOS, az iWork és a Safari különböző verzióit frissítette az Apple.
- Menetrendszerű negyedéves biztonsági frissítési napján számos termékéhez bocsátott ki foltot az Oracle. Az adatbázis-kezelőn kívül javítást kapott a Fusion Middleware, az Enterprise Manager Suite, az E-Business Suite, az Oracle Supply Chain, a Peoplesoft Enterprise család és az Oracle Sun Product Suite.

Augusztus

- Rendszeres havi frissítési ciklusa keretében a Microsoft 13 javítócsomaggal jelentkezett. Kritikus minősítést kettő, fontosat kilenc, mérsékelten fontosat ismét két frissítés kapott. Az

összesen 22 folt a Windows, az Internet Explorer, az Office, a .NET keretrendszer, valamint a fejlesztői eszközkészlet (Developer Tools) réseire került.
- Biztonsági frissítést kapott több Adobe termék, így a Shockwave Player, a Flash Media Server, a Flash Player, a Photoshop CS5 és a RoboHelp. Az utóbbi szoftver javítását fontosnak, az első ötét kritikusnak minősítette a gyártó.
- Foltot bocsátott ki a QuickTime-hoz az Apple.
- Több biztonsági problémát javítottak az Apache webszerveren.

Szeptember
- A negyedév utolsó foltozó keddjén öt – egytől egyig fontos besorolású – biztonsági frissítés látott napvilágot a Microsoftnál. Az érintett termékek: Windows, Office, valamint a cég szerverszoftvere.
- Menetrendszerű negyedéves frissítést bocsátott ki PDF-szoftvereihez – a Readerhez és az Acrobathoz – az Adobe. A cég ezen kívül foltozta a Flash Playert is.
- Biztonsági frissítést kaptak az Apple Mac OS X operációs rendszerének egyes változatai, így a legfrissebb kiadás, a Lion is.
- Szakítva negyedéves ciklusával, rendkívüli frissítést bocsátott ki egy szolgáltatásmegtagadási támadást lehetővé tevő rés eltakarására Apache webszerveréhez az Oracle.
- Megújította Chrome böngészőjét a Google. A frissített változat védelmet nyújt a BEAST, vagyis egy – egyelőre szerencsére csak demonstráció formájában létező – SSL protokoll elleni támadási módszer ellen. A javítás azért fontos, mert site-ok milliói az SSL-re építették az adatok titkosítását.

A VirusBuster Kft.-ről

Aki a VirusBustert (www.virusbuster.hu) választja üzleti partneréül, több mint húsz év szakmai tapasztalatára támaszkodhat. A nemzetközi hírnevű, ám kizárólag magyar tulajdonú, külföldi tőkebevonás nélkül működő cég a számítógépes vírus-, spamvédelmi és egyéb biztonságtechnikai megoldások úttörői közé tartozik. Az évek során a VirusBuster partneri viszonyt épített ki az ágazat számos vállalatával. Víruskereső technológiáját több vezető cég, köztük a Microsoft is beépíti termékeibe. A VirusBuster szoftverei számos nemzetközi díjat, illetve tanúsítványt nyertek, s ma már harmincnál több országban kaphatók.

Magyarországon is több nagy szervezet alapozta informatikai védelmét VirusBuster megoldásokra – köztük a Debreceni Egyetem, az Eötvös Loránd Tudományegyetem, az Invitel, a Magyar Fejlesztési Bank vagy a Magyar Televízió.

Átgondolt szoftver- és szolgáltatásfejlesztést követően 2010-ben a VirusBuster újabb piaci szegmens felé nyitott. Azt a minőséget, amely a nagyvállalatoknál bevált, s amelyet gyártófüggetlen tesztelők is sokszorosan tanúsítottak, elérhetővé tette a cég azoknak az egyéni felhasználóknak a számára is, akik nem az olcsó tömegterméket, hanem a prémium színvonalat, a valódi biztonságot keresik.

A VirusBuster világszerte elismert szakemberei rendszeres előadói hazai és nemzetközi konferenciáknak. Bozsó Julianna, a cég ügyvezető igazgatója az Informatikai Vállalkozások Szövetségétől (az IVSZ-től) 2008-ban elnyerte az „Év Informatikai Cégvezetője” díjat. A kft. 2003-ban „Év innovatív üzleti megoldása”, 2004-ben pedig „IT Reménység” díjban részesült. Két ízben is megkapta a cég az IVSZ-től a „Minősített Szoftver Exportőr” címet és 2005-ben megszerezte az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási tanúsítványt. A vállalat webáruháza 2009-ben kiérdemelte a „Fair Business” minősítést, s ugyanebben az évben a VirusBuster Üzleti Etikai Díjat kapott.

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937