PTA CERT HUNGARY

Puskás Tivadar Közalapítvány

PTA CERT-Hungary Központ

2008. éves jelentés

www.cert-hungary.hu

Puskás Tivadar Közalapítvány



Tartalomjegyzék

Bevezető....3
Szoftver sérülékenységek....4
Internet biztonsági incidensek....7
Górcső alatt a 2008-as év....8
SPAM – Kéretlen levelek....9
SPAM Trendek....10
Botnet evolúció I. - SPAM....11
Káros szoftverek....13
Botnet evolúció II. – káros szoftverek....15
Phishing és csalások....15
Botnet evolúció III. – csalások és phishing....17
Sérülékenységek az Internet PKI-ban, melyet az MD5 használata okoz....18
Hazai tevékenységek, 2008....24
Hazai hálózatbiztonsági és kritikus információs infrastruktúra védelmi együttműködések....24
Pályázati tevékenység....26
Nemzetközi tevékenységek, 2008....27
Egyéb nemzetközi tevékenységek....28
Elérhetőségeink....29

Bevezető

A **Puskás Tivadar Közalapítvány**on belül működő **CERT-Hungary Központ** ezúton kívánja szakmai közönségének rendelkezésére bocsátani a 2008. évi jelentését, amely magában foglalja a 2008. évre vonatkozó időszaki riportokat is.

A CERT-Hungary Központ, mint a kormány hálózatbiztonsági központja, feladatának tekinti az informatikai szakértők széles körének tájékoztatását hálózatbiztonsági témában.

A Központ által kibocsátott 2008. évi összesített jelentés, egyfajta almanachként beszámol mindazokról a jelentősebb hálózatbiztonsági konferenciákról, nemzetközi rendezvényekről, amelyek a Központ munkájának és fejlődésének szerves részét képezték a 2008. évben, továbbá cikkekkel és esettanulmányokkal reprezentálja az év rendszerbiztonsági és kritikus informatikai infrastruktúrákat érintő fejleményeit.

Az alábbi jelentés felsorakoztatja és osztályozza a 2008. év szoftversérülékenységi információit, internet biztonsági incidenseit, valamint a nemzetközi szinten is eredményes és jelentős pályázatokat és fejleményeket.

Valamennyi, az alábbi jelentésben szereplő információ, biztonsági érték és kutatási eredmény a CERT-Hungary Központ, illetve nemzetközi és hazai kapcsolatai által biztosított aktuális és hiteles adatokon alapszik.

Célunk ezzel a jelentéssel egy olyan tájékoztató kiadvány megjelentetése, amely támogatja az informatikai és internet biztonságban érintett szervezetek munkáját és segítséget nyújthat védelmi stratégiai felkészülésükben.

A PTA CERT-Hungary Központ nevében:

Dr. Angyal Zoltán

Puskás Tivadar Közalapítvány

CERT-Hungary Központ

hálózatbiztonsági igazgató

Dr. Suba Ferenc

Puskás Tivadar Közalapítvány

CERT-Hungary Központ

testületi elnök

Dr. Kőhalmi Zsolt

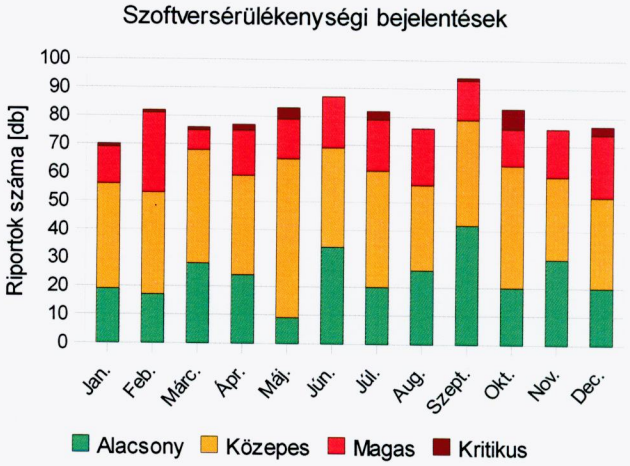
Puskás Tivadar Közalapítvány

ügyvezető igazgató

Szoftver sérülékenységek

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

A **PTA CERT-Hungary Központ** a 2008. év során **963 db szoftver sérülékenységi információt** publikált, amelyekből 289 db alacsony, 451 db közepes, 200 db magas és 23 db kritikus kockázati besorolású.



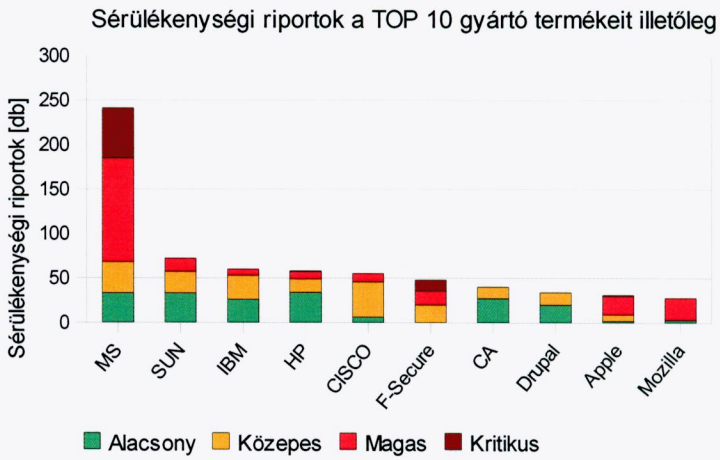
Az év során riportolt sérülékenységi információk havi eloszlása, az egyes hónapok összesített értékei kismértékben ingadozóak, de összességében mérvadó eltérést nem mutatnak. Legnagyobb számban közepes kockázati besorolású sérülékenységi bejelentések kerültek regisztrálásra, amelyek az összes riport 46%-át teszik ki.

Nem mehetünk el szó nélkül a kisebb számban (2%) publikált, de kritikus kockázati besorolással bíró sérülékenységek mellett sem, hiszen potenciálisan a legnagyobb veszélyt ezek jelentik, melyek kapcsán a PTA CERT-Hungary Központ 2008. évben 23 ízben adott ki tájékoztatót támogatott szervezetei részére, továbbá adott ki publikációt weboldalán:

- Microsoft Excel fájl kezelési sérülékenység - 2008. 01. 16.
- IBM DB2 UDB sérülékenységei - 2008. 02. 04.
- WinRAR többszörös sérülékenységei - 2008. 03. 19.
- Apple QuickTime többszörös sérülékenységei - 2008. 04. 04.
- Adobe Flash Player sérülékenységek - 2008. 04. 10.
- PHP-t futtató, HP-UX Apache rendszerek többszörös sérülékenységei - 2008. 05. 06.
- OpenSSL kiszámítható véletlenszám generátor - 2008. 05. 13.
- Microsoft termékek többszörös sérülékenysége - 2008. 05. 14.
- Adobe Flash Player kód futtatási sérülékenység - 2008. 05. 28.
- Microsoft Office Snapshot Viewer ActiveX sérülékenysége - 2008. 07. 08.
- Microsoft Word érvénytelen hosszúságú smart tag feldolgozási sebezhetősége - 2008. 07. 09.
- Oracle termékek többszörös sérülékenységei - 2008. 07. 16.
- Microsoft Windows és Office sérülékenységek - 2008. 09. 10.
- Microsoft Excel többszörös sérülékenységek - 2008. 10. 15.
- Microsoft Internet Explorer többszörös sérülékenységek - 2008. 10. 15.

- Microsoft Host Integration Server sérülékenysége - 2008. 10. 15.
- Microsoft Windows 2000 Active Directory sérülékenység - 2008. 10. 15.
- Microsoft Windows MSMQ sérülékenység - 2008. 10. 15.
- F-Secure RPM Server file feldolgozási sérülékenység - 2008. 10. 21.
- F-Secure RPM Gateway file feldolgozási sérülékenység - 2008. 10. 21.
- Internet Explorer memória hivatkozási sérülékenység - 2008. 12. 16.
- Microsoft Windows WordPad Text Converter sérülékenység - 2008. 12. 10.
- Internet Explorer memória hivatkozási hiba - 2008. 12. 10.

Az egyes gyártók tekintetében a Microsoft (MS) termékei kapcsán kerültek publikálásra a legnagyobb számban sérülékenységi riportok, összesen 241 db a 2008-as év során.



Az sem elhanyagolható, hogy a riportolt Microsoft termékek sérülékenységeinek közel 75%-a magas, illetve kritikus kockázati besorolású.

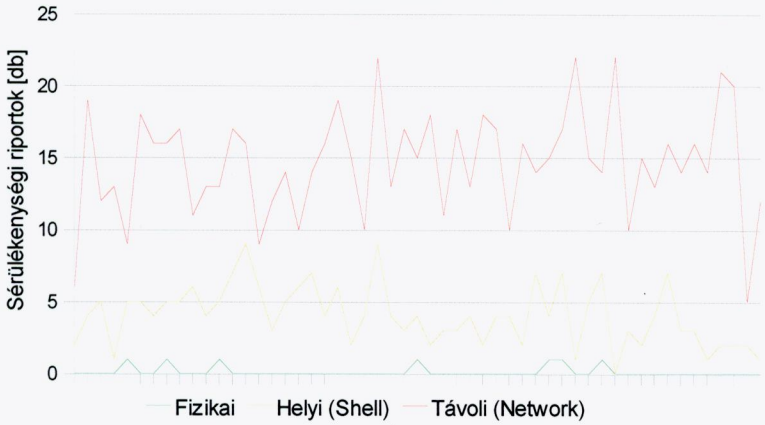
Itt meg kell jegyeznünk azt is, hogy a különböző gyártók egyes termékei kapcsán megjelenő sérülékenységi riportok esetenként meglehetősen nagy előfordulási aránya azt is jelezheti, hogy az adott gyártó jóval szélesebb termékpalettával van jelen a piacon.

Ennek okán statisztikailag is nagyobb az esélye annak, hogy több sérülékenységet fedeznek fel adott gyártó termékeiben, mint más gyártók termékeit illetőleg, melyek például a piaci szegmens jóval kisebb hányadát tudhatják magukénak.

Mindezek által, legyen a használt szoftver vagy szoftver komponens akár CISCO, IBM vagy HP – de sorolhatnánk tovább is - fontos, hogy az esetleges sérülékenységek kihasználásával okozható károkat megelőzzük, illetve megpróbáljuk azok hatását mérsékelni.

Ezért célszerű az egyes szoftvereket, szoftver komponenseket mindig a kiadott frissítésekkel aktualizálni.

Sérülékenységek eloszlása a sikeres kihasználáshoz szükséges hozzáférés tekintetében, heti bontásban 2008



Ezt azért is javasolt megtenni, mert a sérülékenységeket kihasználva támadást intézni adott rendszer ellen legkönnyebben távoli kapcsolat használatával lehet.

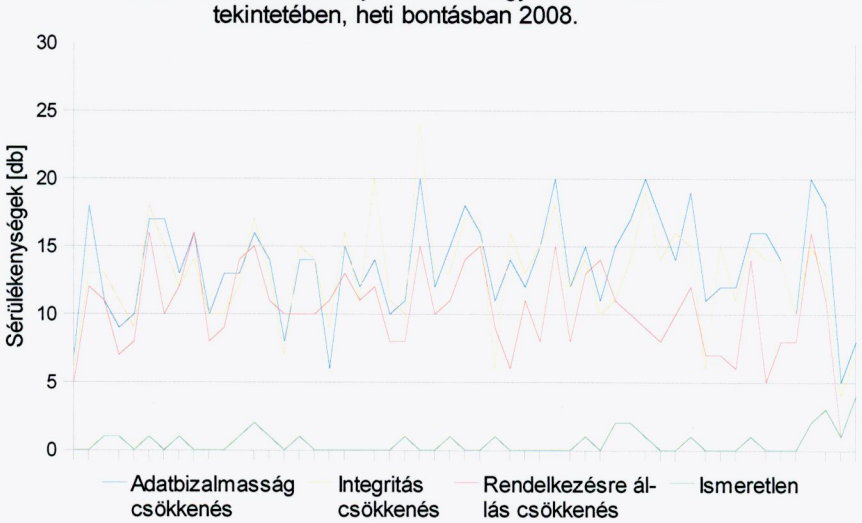
A grafikonon is jól látszik, hogy a távoli kapcsolaton keresztül kihasználható sérülékenységek vannak jelen a legnagyobb számban, mely feltehetőleg a jövőben sem fog megváltozni.

Egy nagyobb visszaesés volt tapasztalható december hónap végén - az 52. héten - a távolról kihasználható sérülékenységek terén, de ennek oka a héten regisztrált sérülékenységi bejelentések alacsony száma.

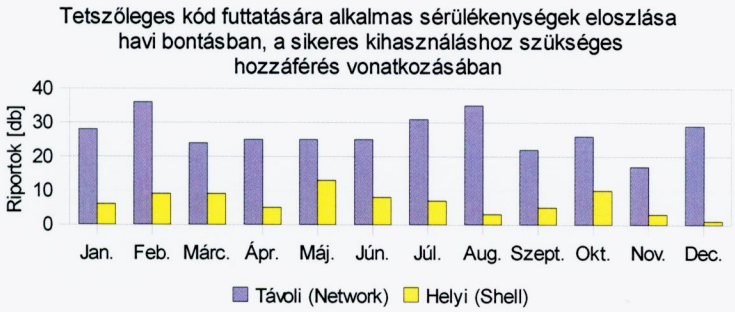
Egy sikeresen lefolytatható támadás esélyét tovább növelik a kihasználáshoz szükséges - az interneten publikusan elérhető - előre elkészített kódok, kódrészletek (exploit-ok).

Az így beszerezhető kódok használatával, egyre kevesebb szakmai tudással rendelkező "ifjú titánok", egyre több és nagyobb horderejű támadások lefolytatására lehetnek képesek.

Sérülékenységek eloszlása, azok sikeres kihasználásával előidézhető, a sérülékeny rendszerre gyakorolt hatásuk tekintetében, heti bontásban 2008.



A sérülékenységek eloszlását a rendszerre gyakorolt hatásukkal együtt ábrázoló grafikonon megfigyelhető, hogy a görbék meglehetősen együtt mozognak. Ezt azt jelenti, hogy egy sérülékenység kihasználásával sikeresen lefolytatott támadás által, az adott rendszer több szempontból is kompromittálható.

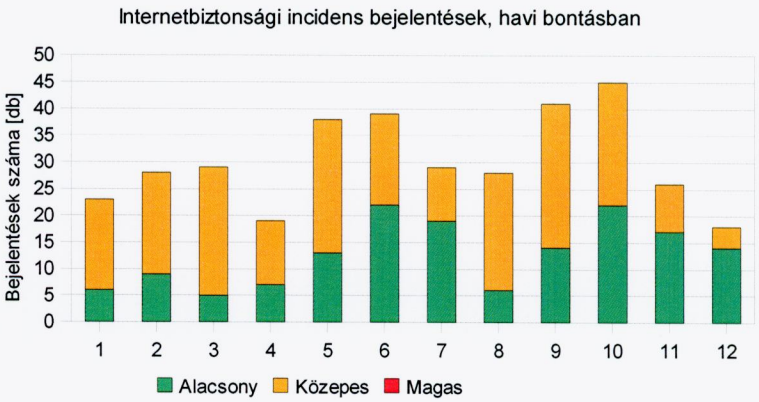


A tetszőleges kód futtatására alkalmas sérülékenységek kihasználása által képesek az egyes támadók a legnagyobb károk okozására. Az ilyen jellegű sérülékenységek száma 2008. évben 402, amely mintegy 41%-a az évben regisztrált sérülékenységeknek.

Internet biztonsági incidensek

Internet biztonsági 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 Központ a 2008. év során összesen **363 db incidens bejelentést** regisztrált és kezelt, ebből 154 db alacsony és 209 db közepes kockázati besorolású. A kimutatás nem tartalmazza a Shadowserver Foundation szervezettől beérkező botnet hálózatok bejelentéseit, mivel azok napi rendszerességgel érkeznek.



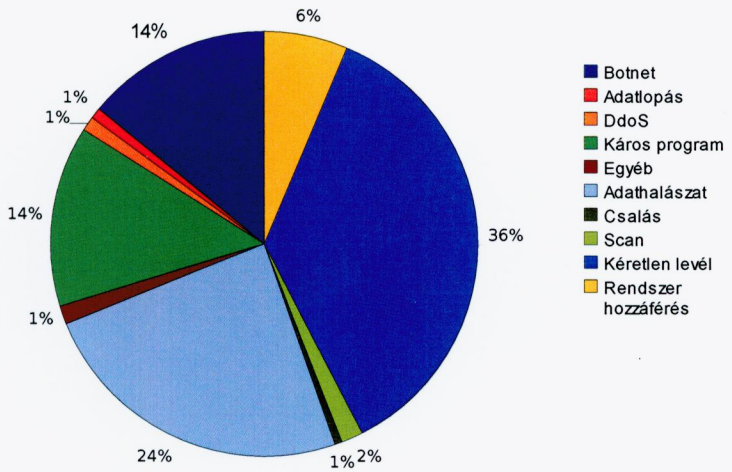
Az **PTA CERT-Hungary Központ** a hatékony incidenskezelés érdekében **24 órás ügyeletet működtet** az év minden napján. Az ügyelet feladata az egyes incidensek kapcsán adandó válaszintézkedések megtétele. Összesen ebben az évben a bejelentett 363 db incidens kapcsán az ügyelet több mint 4200 szálon folytatott vizsgálatot, illetve végzett koordinációs feladatokat.

Ezek közel egyharmada, két egymást követő - október és december hónapokban beérkezett - nagyszámú feltört ftp hozzáférések adatait riportoló, incidens bejelentés kapcsán történt.

A két incidens kapcsán összesen több mint **30.000 felhasználói fiók** tulajdonosa került kiértesítésre, közel **1300 szolgáltató** közreműködésével.

Legnagyobb számban 2008-ban - leszámítva a Shadowserver Foundation-től beérkező botnet hálózatok bejelentéseit - spam tevékenység, adathalász oldalak és botnet hálózatok kapcsán érkeztek bejelentések.

Incidens bejelentések típus szerinti eloszlása



A bejelentések 90%-a (319 db) hazai forrású káros tevékenységgel vagy tartalommal volt összefüggésben, és túlnyomó részt külföldi partnerszervezetektől származott.

A további fennmaradó 10% (44 db bejelentés) külföldi szolgáltatók hálózatain üzemelő eszközökkel vagy azokon tárolt káros, illetve jogsértő tartalommal volt kapcsolatos.

Górcső alatt a 2008-as év

- avagy kiemelkedő veszélyforrások a 2008-as évben -

A MessageLabs Ltd. idén kiadott 2008. éves értékelése szerint - a teljes e-mail forgalomhoz viszonyított - spam szint 2008 februárjában csúcsosodott ki és elérte a 82,7%-ot. Az egész évet tekintve a spam szint 81,2%-os volt, mely a 2007 évben tapasztalt 84,4%-hoz képest csökkenést jelent. A kéretlen levelek közel 90%-át botnetek terjesztették, közöttük a hírhedt Storm botnet. Szeptemberi és novemberi közösségi akciók révén két internet szolgáltatót zártak be az Amerikai Egyesült Államokban a legnagyobb botnethálózatot – pl. Mega-D és a Srizbi hálózatok – kiszolgáló command és control csatorna hosztingjának vádjával. A Srizbi kivételével, az érintett botnetek alternatív "hosztingra" leltek. A rivális botnetek, mint a Cutwail és Rustock, kitöltötték a Srizbi "hiányával jelentkező űrt", melynek eredményeképpen a spam szint megközelítette a bezárások előtti állapotot.

A spammerek 2008-ban a CAPTCHA (Completely Automated Public Turing test to Tell Computers and Humans Apart - teljesen automatizált, nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére) technikák legyőzése révén lehetőség kínálkozott arra, hogy a kéretlen levelek terjesztése jóhírű web-alapú e-mail, valamint alkalmazás-szolgáltatások segítségével történjen. A spamek 6,5%-a ezen webmail fiókoktól származtatható januárban, míg szeptemberben 25%-ra ugrott meg a fenti forrásokból származó kéretlen levelek száma, az év fennmaradó részében pedig az átlag 12%-ra tehető.

A közösségi oldalakat és azok sérülékenységeit támadó komplex, web-alapú kártékony szoftverek száma 2008-ban megnövekedett és széles körben elterjedtek. A kártékony alkalmazások felhasználói beavatkozás nélkül is képesek voltak installálni magukat a számítógépekre. A káros szoftvereket tartalmazó website-ok száma átlagosan 1068 volt januárban, amely novemberben 5424-re emelkedett, elérve az év maximumát. Átlagosan napi 2290-re nőtt a blokkolt új oldalak

száma, amelynek fő oka az SQL befecskendezéses technikákat alkalmazó támadások megnövekedett száma - 2007-ben 1253 ilyen támadást regisztráltak.

Ahogy 2008-ban a web alapú támadások egyre "népszerűbbé" váltak, úgy az e-mail alapú támadások száma - a 2007. évi adatokhoz képest - 0,15%-kal csökkent. A 2008-ban eddig kevésbé alkalmazott célzott támadások száma is erőteljesen megnövekedett. Napi szinten átlagosan 53-ra nőtt az elfogott, célzott trójai támadások száma, míg áprilisban már a 78-at is elérte, ami egyben az éves maximumot jelentette. Viszonyításképpen ez a szám 2005-ben 1-2 eset/hét, 2006-ban 1-2 eset/nap, illetve 2007 elején 10 eset/nap volt.

A 2008-as év vége felé haladva, a gazdasági válság számos pénzügyi vonatkozású támadást generált, mivel a támadók világszerte igyekeztek a változásokkal járó bizonytalanságot és pánikot a saját előnyükre fordítani. Mindennapossá vált a speciális botnetek támadásaként kivitelezett phishing tevékenység, amely a vizsgált év folyamán számos átalakuláson ment keresztül.

SPAM – Kéretlen levelek

A 2008-as évet tekintve, az összes levél 81,2% spam volt, amely a 2007-es 84,6%-os átlaghoz képest minimális javulást jelent.

A 2007-es évet a csatolmányokat tartalmazó kéretlen levelek gyors fejlődése jellemezte, ugyanakkor a 2008-as évben a különféle csatolmányok alkalmazása – az előzmények ellenére – nem folytatódott. A kéretlen levelek terjesztésének mérföldkövét a CAPTCHA technikák kijátszása jelentette, melyet a prominens szolgáltatók használtak szolgáltatásaik védelme érdekében. A spamek gyors és hatékonyabb terjedésének okaként felróható, hogy a jó hírű, web alapú e-mail szolgáltatások esetében is ritka a spamek szűrése, különösen akkor, amikor a leveleket adott szolgáltatón, illetve szolgáltatáson belül küldik egymásnak. A spam-szűrés eseti jellege a bizalmi hierarchiának köszönhető, amely az adott szolgáltatások levelezőszerverei között kölcsönösen fennáll, ezért megfelelőnek értékelik a másik féltől érkező üzeneteket.



Az email forgalom átlagos spam hányada.

A gazdasági válsággal járó bizonytalanságot a cyber-bűnözők igyekeztek saját előnyükre fordítani, ennek eredményeként megnövekedtek a pénzügyi vonatkozású kéretlen e-mail üzenetek, melyek akár phishing támadások részét is képezhették. A célpontok között főként bankok és hitelintézetek szerepeltek, de ezzel párhuzamosan megemelkedett a lottó csalások, a hitel- és munka ajánlatok, illetve más pénzügyi félrevezetések száma is.

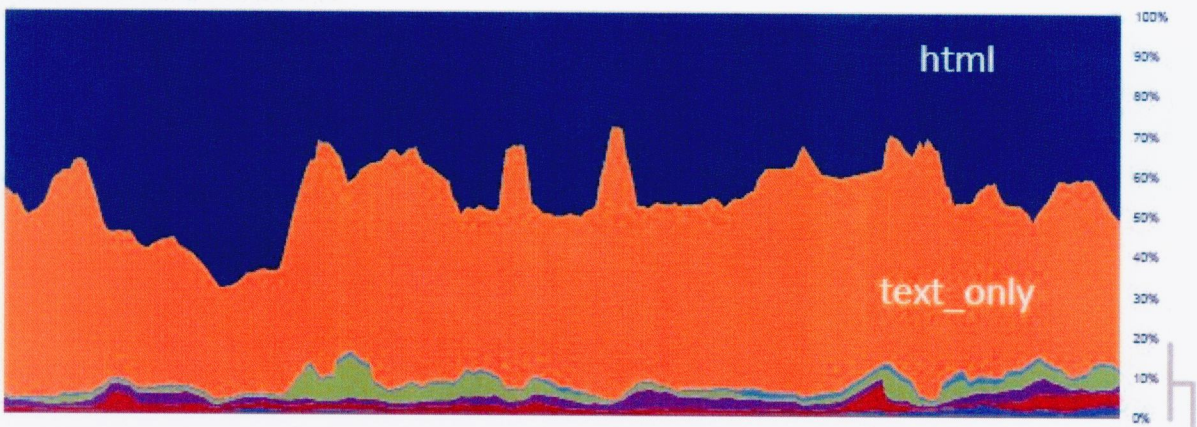
SPAM Trendek

- A rövidebb spam üzenetek, hírösszefoglalók inspirálták a spamelőket -

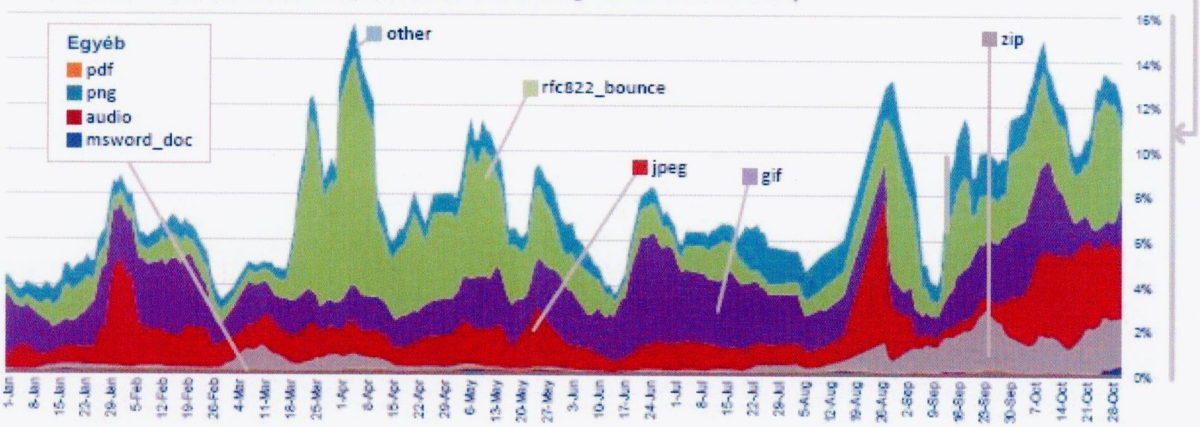
A 2007-es év nyarán a képeket tartalmazó kéretlen levelek mennyisége elérte a 20%-ot is, ugyanakkor 2008-as év folyamán ez 2 % alá csökkent. A spam üzenetek többségét a csak szöveges, illetve HTML tartalmú levelek alkották. Az üzenetek rövidebbé váltak, többnyire egy-két mondatból és egy weboldalra mutató linkből álltak, amely nagyban megnehezítette az anti-spam technikák által használt szövegkörnyezeti analízist.

2008 második felében és a novemberi botnet hálózatok felszámolása előtt, a spam üzenetek hossza mérséklődött és tartalma a tiszta szöveg vagy HTML kód használata felé tolódott el.

Spam tartalmi típusok szerint



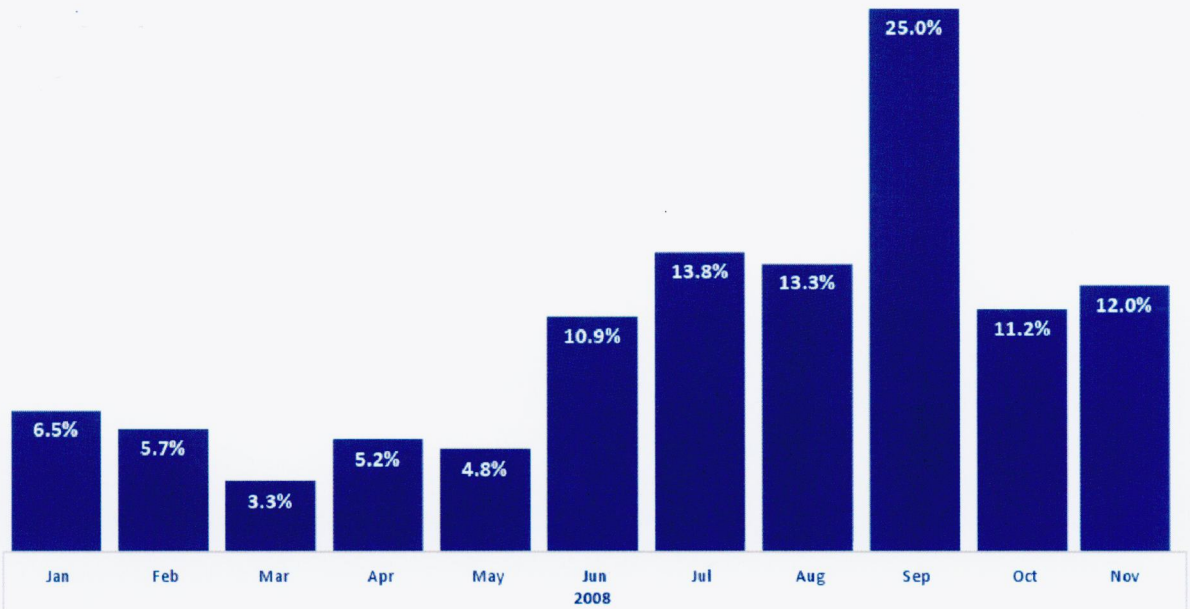
Spam tartalmi típusok szerint (html és csak szöveges üzenetek nélkül)



Agresszív növekedését láthattuk 2008-ban a cyber bűnözők, ismertebb és jó hírnévvel rendelkező, web-alapú e-mail szolgáltatatók elleni támadásainak. Az előző években a domain nevekről küldött üzenetek általában hamisítottak voltak, ezzel szemben 2008-ban a spammerek felismerték a szolgáltatók hiteles és nagyszámú online fiókjainak használatában rejlő lehetőségeket. A CAPTCHA töréssel megnyílt az út az ingyenes e-mail postafiókok létrehozásához, melyeket széles körben felhasználhatók spam terjesztésre.

Januárban az ingyenes és széles körben ismert web alapú e-mail szolgáltatók szolgáltatásait kihasználva, az összes spam forgalom 6,5%-a bonyolódott le. Szeptemberben 25%-os értékkel érte el az éves maximumot.

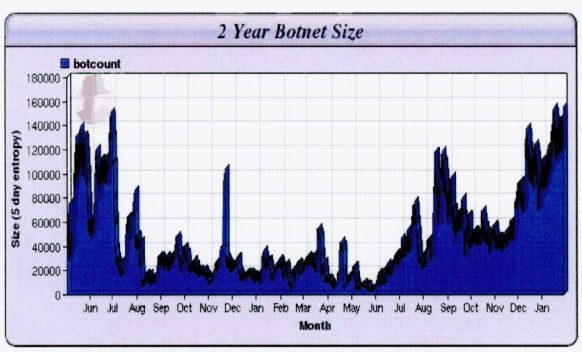
Webmail fiókokból származó spamek



Az ábra az összes kéretlen levél és azon spamek arányát mutatja, amelyeket publikus webmail fiókokról küldtek

Botnet evolúció I. - SPAM

A PTA CERT-Hungary Központ együttműködik a Shadowserver Foundation szervezettel, amelynek célja, hogy felderítse és felszámolja az interneten található botnet hálózatokat, azok klienseit, valamint az irányításukhoz szükséges C&C szervereket. A PTA CERT-Hungary Központ, mint nemzeti kapcsolati pont, 2008 második negyedévétől napi szinten jelentést kap a magyarországi hálózatokon található botnet kliensekről és C&C szerverekről.



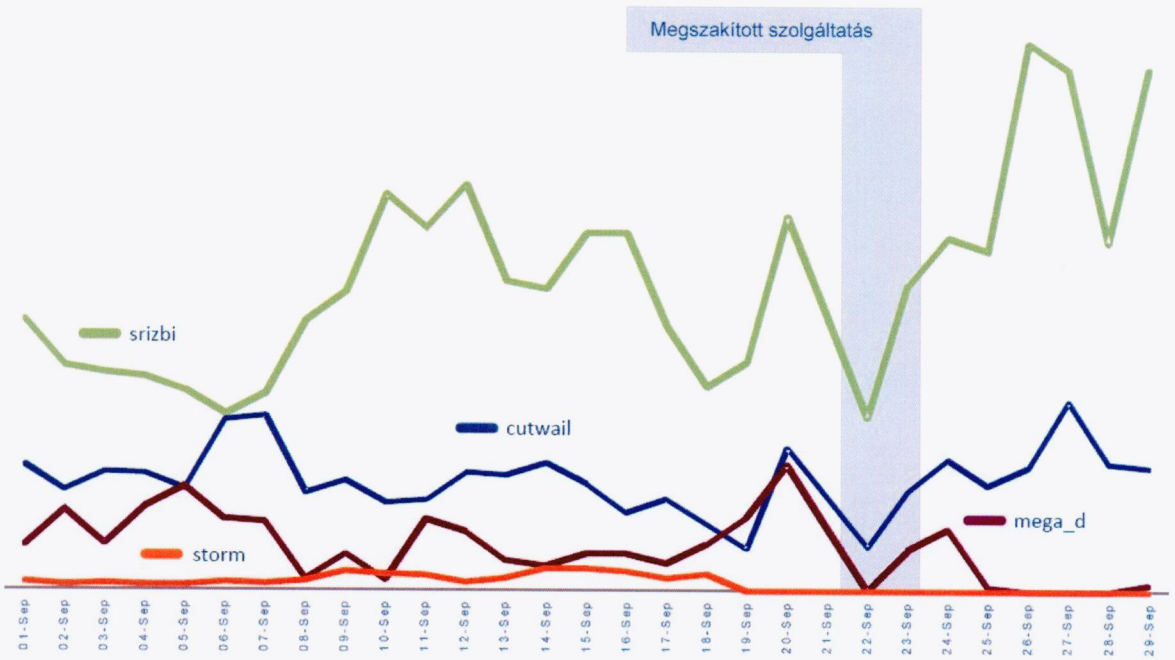
A mellékelt ábra a Shadowserver Foundation által nyomonkövetett aktuális zombi-gépek, botok számát mutatja - 5 napos eloszlásban - két év távlatában.

A hirtelen változások okai minden esetben a C&C szerverek be-, illetve lekapcsolása, bár számos más elmélet is létezik, amelyek magyarázni próbálják a görbe változásait, azonban ezek megalapozottsága kétséges.

A 2007-es évben a spamek, a kártékony szoftverek és a phishing csalások terjesztésének domináns erejévé a botnetek váltak. 2008-ban a botnetek voltak a spam üzenetek 90 százalékáért felelősek.

2008 első negyedévében az összes kéretlen levél 20 %-át a Storm botnet által kibocsátott spam üzenetek tették ki. Április folyamán a Malicious Software Removal Tool (Microsoft) frissítése megtörtént, amelynek eredményeként a Storm hálózatok spamküldő kapacitása jelentősen csökkent. Ettől kezdve egy riválisan botnet, a Srizbi vette át a vezető szerepet a spamek terjesztésében.

Az év késői szakaszában a Mega-D hálózat szinte teljesen eltűnt, amikor az online csalóknak és cyber bűnözőknek biztonságos otthont nyújtó kaliforniai Intercage internet szolgáltató működését szeptember 20-án leállították. A későbbiekben egy másik szolgáltató vette át a Intercage szerepét, de a fellépő problémák miatt a szolgáltatást szeptember 25-én megszüntették.



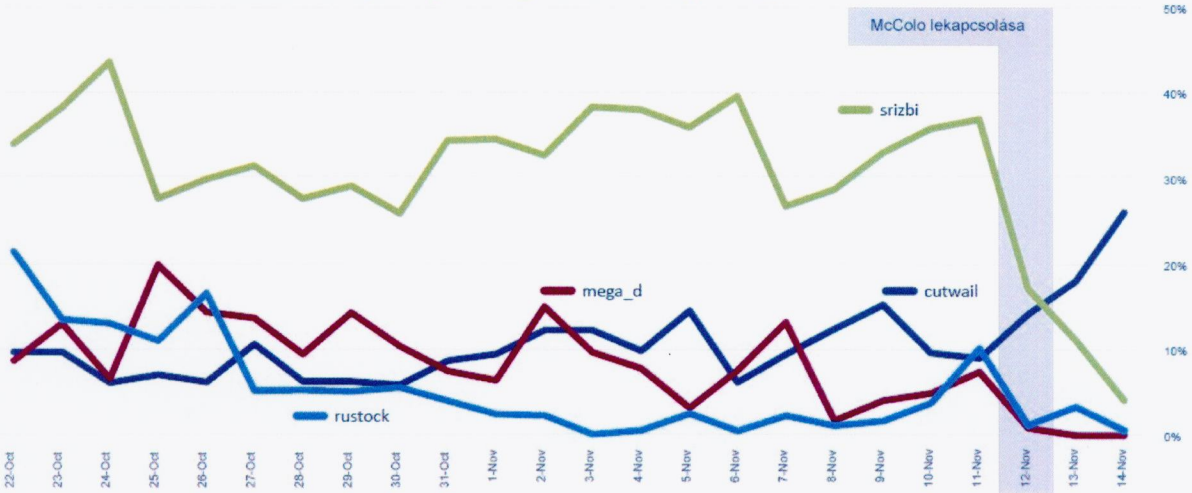
Főbb botnetek tevékenysége az Intercage leválasztásának ideje alatt

Az Intercage leválasztásával, ideiglenesen csökkent a spam levelek száma.

Novemberben ismét egy kaliforniai internet szolgáltatót fosztottak meg internet kapcsolatától, amikor a hálózatukból származó, jogellenes tevékenységekkel kapcsolatos bizonyítékokra derült fény.

Feltevések szerint a McColo Corporation számos, a világ legnagyobb cyber-bűnözői csoportjainak biztosította szolgáltatásait. A szolgáltató lekapcsolásával egyidejűleg a Srizbi, a Rustock és a Mega-D botnet hálózatokból eredő kéretlen levelek száma radikálisan csökkent.

Botnet hálózatok szerepe a spam terjesztésében *(egy honeypot mintája alapján)*



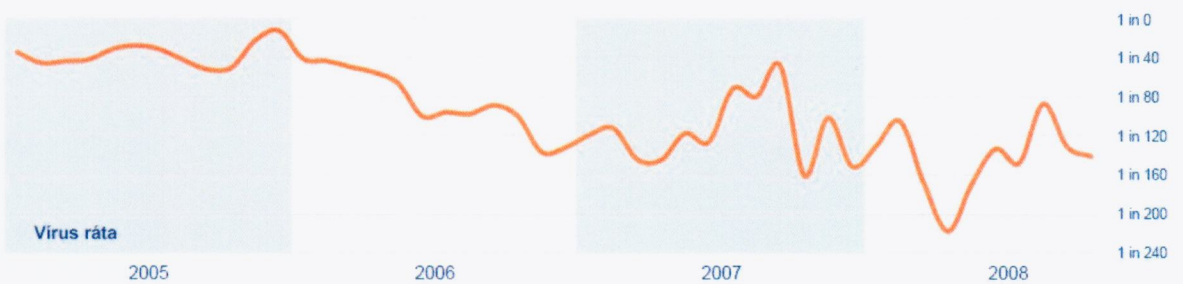
A McColo lekapcsolása idején észlelt, főbb botnet hálózatok tevékenysége

A McColo Corporation lekapcsolását követően - 12 órán belül - a terjesztett kéretlen levelek száma az eredeti érték nyolcadára süllyedt, jelezve azt, hogy a feketegazdaság kiemelkedő szereplőinek kiszűrése jelentősen hat a globális spam szintre.

A 2008-ban történt bezárások hatására, az eseményben nem érintett, rivális botnetek jelentősen nagyobb aktivitást mutattak a lekapcsolások idején. Hetekkel később, a bezárások által érintett botnet hálózatok üzemeltetőinek egy része újabb szolgáltatót talált és folytathatta működését.

Káros szoftverek

Az e-mail formában terjesztett kártékony szoftverekre vonatkozó 2008-as trend szerint, a kezdeti csökkenés után – követve a Storm botnet 2008. áprilisi visszaesését – a káros szoftverek szintje ismét növekedésnek indult. Az elfogott levelek 0.70%-a volt kártékony tartalmú, míg 2007-ben 0.85% volt ez az érték. A számok utalnak arra, hogy a kártékony alkalmazások terjedése sokkal nagyobb hatékonyságú, weboldalakon keresztüli terjesztéssel és a hordozható adattárolókról való telepítéssel, mintsem e-mail-ek útján.



A káros szoftvert tartalmazó levelek hányada az e-mail forgalomban

2008-ban a botnetek, vagy más néven a robot hálózatok, jelentős fejlődésen estek át az előző évhez képest. A trójai programok installálására számos új metódus jelent meg, lehetővé téve telepítésüket hordozható adattárolókról, közösségi oldalakról és üzenetküldő alkalmazásokon keresztül. Mindez a kártékony alkalmazások áradatát indította el.

2008 első felében a sérülékenységeket és a webes alkalmazások gyenge biztonságát egyre szélesebb körben használták ki a bűnözők, web alapú kártékony szoftverek fejlesztésére. Az új eszköztárak képesek voltak kikeresni és célba venni a gyenge biztonsági szinttel rendelkező web oldalakat. Jó példája ezen támadási típusoknak, a kiterjesztett SQL befecskendezéses támadás, amely képes a dinamikus, adatvezérelt oldalak megfertőzésére, ezáltal kártékony JavaScript-ek megjelenítésére a weboldalak látogatói számára.

Source	24 hour	10 day	30 day	60 day	90 day	180 day	12 month	2 year	Total
email	796/2.200	12.956/44.865	28.290/90.355	34.640/123.514	53.149/187.647	118.708/301.484	298.054/534.732	1.017.647/1.266.848	1.079.663/1.333.036
honeyclient	6.786/6.886	83.477/84.295	293.310/296.031	400.669/407.091	507.711/517.828	888.691/919.386	1.881.865/1.949.790	1.881.865/1.949.790	1.881.865/1.949.790
honeypot	1.535/1.600	25.269/44.962	70.014/120.897	115.277/216.246	168.927/296.588	385.592/633.930	778.657/1.081.660	1.954.674/2.272.319	1.955.135/2.297.986
irc	20/20	618/621	1.768/1.789	2.424/2.471	2.829/2.901	3.553/3.666	4.226/4.588	11.483/12.115	12.284/22.452
sandbox	1/9	79.742/80.683	403.572/405.681	2.612.700/2.662.035	6.153.626/6.301.495	10.519.006/10.971.805	18.583.135/20.551.116	33.012.410/36.323.642	33.012.410/36.323.642
submission	72/114	283/383	691/1.183	56.142/108.786	56.890/110.385	58.545/116.079	60.668/120.165	297.887/488.740	298.060/488.951
~total~	9.210/10.829	202.345/255.809	797.645/915.936	3.221.852/3.520.143	6.943.132/7.416.844	11.974.095/12.946.350	21.606.605/24.242.051	38.175.966/42.313.454	38.239.417/42.415.857

Az alábbi táblázat a Shadowserver Foundation által érzékelt kártékony kódok (bináris file-ok) számát mutatja. Minden egyes oszlopban két érték szerepel. Az első érték az egyedi kártékony file-ok számát, míg a második az összes felismert kártékony file számát mutatja, adott forrásból és időkereten belül.

A káros tartalom miatt tiltott új oldalak száma 2290-re nőtt 2008-ban. Viszonyításképpen, ez 82,8% növekedést jelent a 2007-es adatokhoz képest.



Az ábra a web alapú kártékony szoftverek növekedését mutatja 2008-ban.

A 2008 júniusában érte el a 2007 áprilisa óta számított legmagasabb szintet a kártékony tartalom miatt blokkolt weboldalak száma (2076 db). 2008 második felében jelentősen megnőtt a sérülékeny web szervereket ért SQL befecskendezéses támadások száma, ezáltal a kártékony kódot tartalmazó weboldalak száma is jelentősen emelkedett. 2008 októberében a naponta kártékony tartalom miatt blokkolt weboldalak száma is tovább nőt és elérte az 5424-et, amely az adott időszak csúcsértékét jelentette.

A web-alapú kártékony szoftverek 2008-ban szélesebb körben terjedtek, mint a spyware és adware alkalmazások. Ez azzal magyarázható, hogy a cyber bűnözők felismerték, a web-felhasználók tájékozatlanságában rejlő lehetőségeket.

Botnet evolúció II. – káros szoftverek

Mióta 2007 januárjában megszületett a Storm botnet, valamiféle titokzatosság lebegte körül biztonságtechnikai körökben. Számos riport szólt arról, hogy a Storm botnet hálózat zsugorodik, vagy éppen más botnetek veszik át az irányítást, míg mások éppen arra mutattak rá, hogy egyszerűen egy csendes perióduson megy keresztül mielőtt versenyre kelne az újabb botnetekkel.

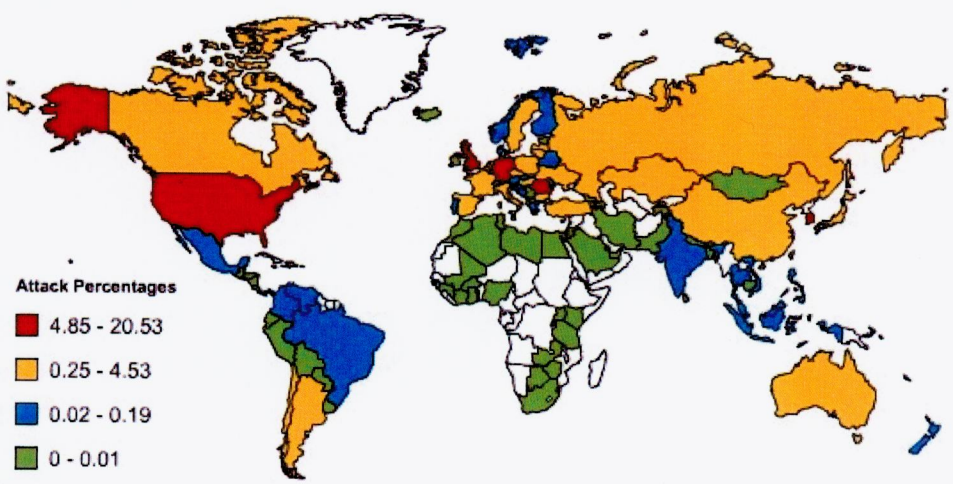
Számos szempont figyelembevételével, a Storm hálózatot kisebb szegmensekre szeletelték, darabjait különböző spam-melőknek adták bérbe, ugyanakkor az egyes - különálló - részek egy botnethálózat részét képezték. A bot-hálózat nagy részét spam tevékenységen kívül kártékony szoftverek terjesztésére, továbbá phishing támadásokra használtak.

2008 májusában több mint 81000 káros alkalmazás másolatot fogott el a MessageLabs, amelyek azonos jellemvonásokkal rendelkeztek a korábbiakban észlelt Storm vírussal.

A Unix alapú operációs rendszereken elérhető "Nginx" elnevezésű, kisméretű, nyílt forráskódú web szervert portolták Windows-ra, és ezt használta a Storm botnet a web-es tartalom kiszolgálására. Bár az Nginx web szervert számos weboldal használja, mégsem olyan elterjedt, mint más nyílt forráskódú alkalmazások, ugyanakkor kisméretű és jól felkészített alkalmazás, amely tulajdonságok igencsak vonzóak bármely botnet hálózat számára.

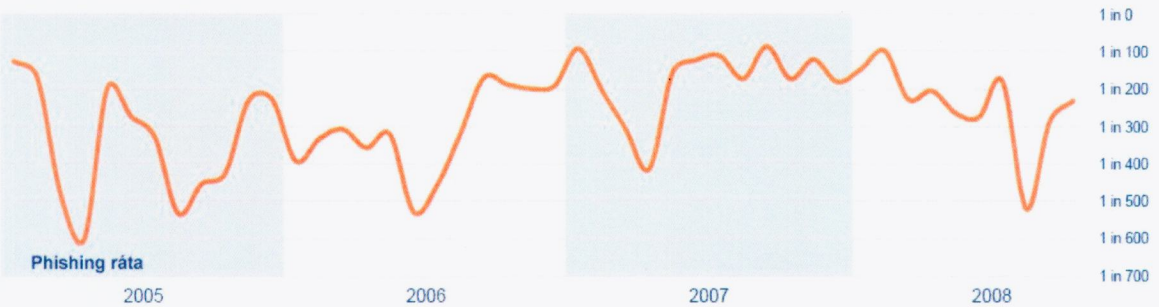
Phishing és csalások

A PTA CERT-Hungary Központ 2007 júliusa óta tagja az 'Anti-Phishing Working Group'-nak (Nemzetközi Adathalászat Elleni Munkacsoport), amelyhez bankok, IT beszállítók, non-profit szervezetek, hálózatbiztonsági cégek, egyéb szervezetek (pl. CERT-ek), valamint a kormányzati és/vagy bűnüldöző szervek is kapcsolódtak a világ számos pontjáról. Az Anti-Phishing Working Group célja, hogy értékelje az adathalász támadásokkal, hamisított e-mailekkel végrehajtott csalások és személyiség lopások mértékét, továbbá vizsgálja azok technológiáját, lehetséges károkozását, és együttműködve megoldásokat találjon a támadások visszaszorítására.



Az iménti ábra az Anti-phishing Working Group által regisztrált – 2008. évre vonatkozó – incidensek eloszlását mutatja be világviszonylatban. A képen a többi ország mellett nehezen kivehető, de az adatok alapján Magyarország mindössze 0,25 - 4,53%-ot képvisel éves szinten az összes elkövetett bűncselekményből. Ez az érték a negyedéves elemzésekben 0,3% körül mozgott és az év során számottevően nem változott. Az alacsony arány elsősorban a támadók magyar nyelvtudásának hiányával magyarázható.

A teljes, globális e-mail forgalom 0,41%-át tették ki 2008-ban a phishing tartalmú levelek, amely a 2007-es 0,64%-hoz képest visszaesést jelent.



A phishing tartalmú levelek hányada az e-mail forgalomban

A phishing tevékenység 2008 februárjában csúcsosodott ki, amikor minden 99 levélből 1 phishing tartalmú volt. A növekedést részben a plug-and-play stílusú phishing alkalmazások elérhetőségének növekedése okozta, amelyek használata nem igényelt komolyabb szakmai ismeretet, másrészt a phishing tevékenységet specializált botnethálózatok használatán keresztül valósították meg.

Viszonylagosan új trendnek számít a botnet hálózatok alkalmazása phishing oldalak kiszolgálásában, amelyet először - 2008 januárjában - a Storm botnettel kapcsolatban figyelhettünk meg. Korábban a botneteket mindössze spam és kártékony szoftverek terjesztésére használták.

A phishing támadások intenzitása kis mértékben csökkent 2008 folyamán, de a célpontok spektruma bővült. Annak ellenére, hogy a főbb pénzügyi intézmények továbbra is a bűnözők célpontjai voltak, a kisebb bankok, hitelszövetkezetek is fókuszba kerültek.

A DNS (Domain Name System) protokoll - 2008-ban felfedezett - sarkalatos tervezési gyengesége melegágyat teremtett az alacsony biztonsági szinttel rendelkező DNS domain-ek és sérülékeny weboldalak használatával megvalósított phishing támadások lefolytatására. Megszerezve a populáris és egyben sérülékeny domain nevekkel járó előnyöket, a "tradicionális" – az eredetivel a megtévesztésig egyező vagy arra hasonlító - phishing domain nevek (pl.: enbankom.hu és enbank0m.hu) feledésbe merültek.

2008 második felében meglehetősen elszaporodtak a web alapú, jelszó gyűjtésére készült trójai programok, főként az online játékokkal kapcsolatban, melynek oka feltehetően az, hogy a bűnözők megpróbálták valódi pénzzé váltani a virtuális valóságban összegyűjtött vagyont.

A globális gazdasági válság hatására a phishing támadások száma a pénzügyi tartalmú kéretlen levelek mennyiségével párhuzamosan ismét emelkedésnek indult.

Botnet evolúció III. – csalások és phishing

2008-ban még inkább nyilvánvalóvá vált, hogy a phishing támadások forrásai az e célra specializált botnetek. A fast-flux technikát használó hálózatokban minden egyes phishing domain gyorsan változó IP címet használ. A technika előnye a terhelés elosztás, valamint a phishing oldalak felszámolásának ellehetetlenítése, illetve életciklusuk növelése.

Az ASPROX elnevezésű botnetet - szinte kizárólagosan - csak phishing támadások véghezvitelére tervezték. Amikor az ASPROX először felbukkant egy phishing trójai volt, azonban fejlődése során fertőző képes botnetté alakult és a sérülékeny weboldalakat SQL befecskendezéses technikával támadta. ASP (Active Server Pages) nyelven fejlesztették és automatikusan HTTP GET kéréseket használt a sérülékeny oldalak adatbázisaihoz való kapcsolódásra.

Az ASPROX-ot tulajdonságai képessé tették, hogy az adatbázis kulcstábláiba kártékony JavaScript kódot fecskendezzen és így az oldal későbbi látogatóit megfertőzze. A JavaScript-et rejtett HTML <IFRAME> tag-ek tartalmazták. A kártékony kódok más weboldalakon keresztül, a támadók irányításával végrehajthatók voltak a felhasználók böngészőjében, azok tudta és beleegyezése nélkül.

Sérülékenységek az Internet PKI-ban, melyet az MD5 használata okoz

GOV<>CERT.NL

2008. december 30-án a "Chaos Communucation Congress" kutatócsoportja az évente megrendezésre kerülő berlini biztonsági konferencián gyakorlati demonstrációt tartott a Public Key Infrastructure (PKI) gyenge pontjairól. Bemutattak[1] egy általuk készített hamis tanúsítványt, amelyet minden hagyományos böngésző megbízhatónak talál.

Ebben a dokumentumban egy rövid leírás található a kutatásról, a rövidtávú kockázati tényezőkről és azokról a lépésekről, amelyet minden érdekelt félnek meg kell tennie saját védelme érdekében.

Tények áttekintése

- A kutatók készítettek egy hamis tanúsítványt, amivel a világ bármely weboldala utánozható.
- Ezt a hamis tanúsítványt automatikusan megbízhatóként kezeli a legtöbb hagyományos böngésző.
- A kutatók ezt, az MD5 hash titkosítási funkciójának gyengeségét kihasználva érték el.
- Annak ellenére, hogy az MD5 ezen hibája már évek óta közismert, még mindig használják biztonsági tanúsítványok ellenőrzésére az Interneten.
- Ha Ön az MD5 segítségével bizonyosodik meg a tanúsítványok megbízhatóságáról, amint lehetséges cserélje le.

A kutatás

A kutatás a tanúsítványok használatával van összefüggésben, amikor is egy biztonságos kapcsolat épül fel a böngésző és a weboldal között, amely a 'HTTPS' vagy az 'SSL/TLS' kapcsolatokat érinti. A kapcsolat megbízhatósága felismerhető a böngészőben egy "lakat" megjelenésével vagy néhány esetben a címsor elszíneződésével. A kutatók demonstrálták, hogy amikor egy tanúsítványt egy hitelesítés szolgáltató (Certificate Authority vagy röviden CA) aláír (illetve ha úgy tűnik mintha aláírna), akkor a későbbiekben ez nem jelent semmilyen garanciát arra, hogy a tanúsítvány ellenőrzésre is került.

1 A részletes leírás a kutatásról, az eredményekről és a javaslatokról megtalálható a http://www.win.tue.nl/hashclash/rogue-ca/ oldalon. A prezentáció videó és hanganyaga szintén elérhető.

Más szóval a múltban - a tanúsítvány ellenőrzése után - a biztonságos kapcsolatok használatakor nagy volt annak a valószínűsége[2], hogy a megfelelő oldallal van dolgunk. Gyakorlati támadásokon keresztül bemutatták, hogy ez a biztonság kijátszható.

Még mindig vannak olyan CA-k, amelyek tanúsítványait MD5-tel írják alá. Ez a módszer már egy elavult titkosítási eljárás, és a kutatók sikeresen létrehoztak egy hamis tanúsítványt, melyet látszólag aláírt egy hivatalos Certificate Authority (root CA), így ezt automatikusan megbízhatónak ítéli meg a legtöbb hagyományos böngésző. Még ennél is rosszabb, hogy ez a hamis tanúsítvány akár önmaga is egy Certificate Authority-ként viselkedhet.

Igazolások és biztonságos kapcsolatok

Biztonságos kapcsolat esetén a tanúsítványoknak két alapvető funkciójuk van.

1. Az adatok titkosítása a böngésző és a weboldal között. Így az adatok nem lesznek olvashatóak egy harmadik fél által.
2. Annak ellenőrzése, hogy a kapcsolat tényleg a megfelelő weboldallal jött-e létre.

Ezek a legfontosabbak az olyan szolgáltatásoknál, ahol személyes vagy pénzügyi adatokat közlünk egy másik fél számára, például telebank, Inter-netes ügyintézés vagy online vásárlás esetén.

Ezzel a módszerrel a kutatóknak lehetőségük nyílt arra, hogy létrehozzanak és aláírjanak egy tanúsítványt saját maguknak, illetve bármilyen webszerver részére a világon, amelyet nem lehet megkülönböztetni egy eredetitől és automatikusan megbízhatónak lesz ítélve. Bármilyen weboldalt utánozhatnak anélkül, hogy a látogató felfedezné a hamis tanúsítványt.

Rövidtávú kockázatok

A kutatók állítása szerint valószínűtlen, hogy rövidtávon bárkinek lehetősége lenne hasonló támadásokat indítani az internetes PKI-n.

Eddig a GOVCERT.NL nem dokumentált egyetlen ezt kihasználó támadást sem, leszámítva a már keringő hamis tanúsítványokat. Ahhoz, hogy valaki egy ilyen támadást indítson elengedhetetlen az MD5 gyengeségeinek, valamint az elavult titkosítási eljárás alapos ismerete, amelyet még mindig használ néhány CA a tanúsítványok aláírására. A kutatóknak viszonylag rövid idő alatt sikerült előállítani egy hamis tanúsítványt, úgy hiszik, hogy a szóban forgó CA-knak, melyek még mindig az elavult digitális aláírásokat használják, lesz idejük átállni új, korszerűbb módszerekre.

Mi is a Public Key Infrastructure (PKI)?

A Public Key Infrastructure (PKI) olyan technikai és szervezeti erőforrások gyűjteménye, melyek segítségével Ön megbízhatóan elvégezheti a következőket:

1. A másik fél azonosságának meghatározása
2. Az információ titkosítása
3. Az információk aláírása

Technikai felhasználási példák:

-Titkosítás és aláírás

-A tanúsítványok azonosítják a tulajdonost és a titkosítási kulcsokat

További információk a PKI-ről

http://en.wikipedia.org/wiki/Public_key_infrastructure

(angol nyelvű oldal)

2 Természetesen nincs olyan, hogy 100%-os biztonság. A PKI technikai és szervezési lépéseket tartalmaz, így bizonyos szervezési lépések hiányában előfordulhat, hogy nem megfelelő tanúsítvány keletkezik. Eddy Nigg ezt mutatta be, mikor a mozilla.com domain-hez kért és kapott is tanúsítványt minden probléma nélkül.
Lásd: https://blog.startcom.org/?p=145

Végeredményben a kutatók intézkedéseket tettek arra, hogy megakadályozzák az általuk készített tanúsítványok kártékony felhasználását, bár kijelentették, hogy módszereiket néhány hónapon belül nyilvánosságra hozzák majd[3].

Az egyértelműség kedvéért, a 2005-ben és 2007-ben jelentett támadások kapcsán levonható az a következtetés, hogy felelőtlenség az MD5 további használata.

Védekezés a sérülékenységekkel szemben és azok a lépések, amelyeket Ön is megtehet

A kutatók bebizonyították, hogy az Internetes PKI-nek vannak gyenge pontjai, mert néhány CA még mindig elavult módszereket használ a digitális aláírások előállítására. Következésképpen a PKI nem csak azokra jelent veszélyt, akiknek a CA-val kapcsolatos ügyeik vannak. Következzen egy példa ennek tisztázására: tegyük fel kiderült, hogy nagyon könnyű csalással egy eredeti útlevelet szerezni bizonyos hatóságon keresztül. Az útlevél megszerzése nem csak az adott hatóság problémája. A "hamisítás" miatt megbízhatatlanná válik minden útlevél, és minden az útlevéllel kapcsolatban álló személy fedhetetlensége.

Az előzmények értelmében az egyéni végfelhasználóknak és a tanúsítványok tulajdonosainak lépéseket kell tennie annak érdekében, hogy megvédjék magukat a sérülékenységgel szemben. Ideális esetben a következő történik:

1. Minden olyan CA-t, amely még MD5 aláírást használ, célszerű minél hamarabb átmigrálni egy jobb hash funkcióra[4].
2. Mindenki aki MD5-tel aláírt tanúsítványt használ, amint lehetséges cserélje le azt.(lsd még: "Az MD5 lecserélése...de mire?" - a következő oldalon)
3. Amennyiben az előző két pontban említett követelmények teljesülnek (esetleg hamarabb, mint ahogy szükséges lenne), úgy a böngészőket gyártó cégek visszavonhatnák az MD5 támogatását.

A legfontosabb partnerek ebben a folyamatban a CA-k és a böngészőket gyártó cégek. A CA-k, mint megbízható szervezetek, akiknek jogában áll tanúsítványokat aláírni a PKI közösségen belül, feladatuk alapjaként felelősséggel tartoznak azért, hogy biztonságos titkosítási eljárásokat használjanak. Elengedhetetlen felülvizsgálni a titkosítási eljárás megbízhatóságát, mert elképzelhető, hogy a titkosítási eljárás, amely most még biztonságos, az a későbbiekben számos okból kifolyólag már nem lesz az.

A böngészőket gyártó cégek közvetett módon nagy hatást gyakorolhatnak a CA-kra, mert ők döntik el, mely tanúsítványokat illesztik be alapértelmezetten megbízhatóként az általuk készített böngészőkbe. Amennyiben a böngészők nem támogatják tovább az MD5-öt, úgy ennek azonnali

3 Az, hogy a szoftver sérülékenységeket nyilvánosságra kell-e hozni vagy sem és, hogy hogyan kéne ennek zajlania, arról heves viták vannak a biztonsági közösségen belül. Arról, hogy a kutatók, hogyan bírkóznak meg ezzel, a http://www.phreedom.org/blog/2009/verisign-and-responsible-disclosure/ elérhetőségen olvashat.
4 A Verisign, az egyik root CA gazdája. A cég még mindig az MD5-öt használja, de időközben bejelentették, hogy felhagynak az MD5-tel és a vásárlók ingyenesen lecserélhetik a régi MD5-ös tanúsítványaikat.
Lásd https://blogs.verisign.com/ssl-blog/2008/12/on_md5_vulnerabilities_and_mit.php

következménye lesz a még forgalomban lévő MD5-tel aláírt és az MD5-öt használó tanúsítványokra. A gyártók megoldásától függően a tanúsítványok vagy nem fognak működni vagy hibaüzeneteket adnak.

Mindez nem jelenti azt, hogy nem kell lépéseket tennie:

1. A végfelhasználó, szinte semmit sem tehet, hogy csökkentse fenyegetettségét. Jelenleg még mindig túl sok MD5 aláírást használó tanúsítvány van forgalomban, így ezek elutasítása nem célszerű megoldás. A Firefox[5] böngészőhöz készítettek egy olyan kiegészítőt, amely figyelmezteti a felhasználót, ha az adott aláírások MD5-ön alapulnak, de ez a gyakorlatban hibás visszajelzést eredményezhet. Az előbb említett megoldás csak egy lehetőség a képzettebb otthoni felhasználók számára.
2. Fontos, hogy a szervezeteken belül nyomon kövessük, hogy milyen és melyik típusú aláírásokat használnak, még akkor is, ha megvan a saját belső PKI-nk root tanúsítvánnyal. Ebbe beletartoznak a saját weblapok tanusítványai, valamint a belső oldalaké, a kliens tanúsítványok és minden más egyéb megoldás, amely SSL tanúsítványt igényel, mint például az SSL VPN-ek.
3. Amennyiben még mindig az MD5 alapjait használó tanúsítványt használ, tervezze meg ezek mielőbbi lecserélését, modernebb algoritmusokon alapulóra. A lehetőségekről bővebben a következő bekezdésben olvashat.

Az MD5 lecserélése...de mire?

A kutatók célja az eredmények nyilvánosságra hozatalával az volt, hogy sikeresen bemutassák, milyen régóta felelőtlenségnek számít MD5-öt használni a tanúsítványok aláírására. Éppen ezért felmerülhet a kérdés: Mi van, ha az MD5 többé már nem kielégítő? Az MD5 örököse az SHA-1, de egy rövid ideje már egy újabb verzió is elérhető, név szerint az SHA-2.

Továbbá bemutatták, hogy az SHA-1-nek[6] is vannak gyenge pontjai, és ez előrevetíti, hogy a közeljövőben a különböző támadások hatására az SHA-1 is el fog tűnni. A "The US National Institute of Standards and Technology" (NIST) még ennél is tovább megy. Elengedhetetlen, hogy az amerikai kormányzati szervezetek elhagyják az SHA-1-et és továbblépjenek az SHA-2[7] változataira még 2010 vége előtt.

Jelenleg két lehetőség merülhet fel:

1. Váltás az SHA-1-re. Ez a legkönnyebb megoldás. Az SHA-1-et gyakorlatilag minden szoftver és az összes CA támogatja, éppen ezért az átállás viszonylag olcsó és könnyen kivitelezhető. A hátránya ennek a lehetőségnek az, hogy már az SHA-1-ben is vannak ismert sérülékenységek, bár ez önmagában még nem jelent valós fenyegetést. Az SHA-1-re hamarosan nagy nyomás fog nehezedni és elengedhetetlen lesz az újabb átállás, amely újabb költségeket fog maga után vonni.
2. Váltás az SHA-2-re. Ez a lehetőség kevésbé egyszerű. Az SHA-2 támogatottsága nem magától értetődő dolog az összes CA, valamint a szoftver számára. Mielőtt átállna az

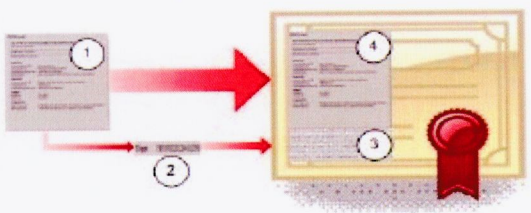
5 A kiegészítő, az SSL Blacklist megtalálható a: http://www.codefromthe70s.org/sslblacklist.aspx elérhetőségen.
6 Az NIST álláspontját az SHA-1-ről a http://csrc.nist.gov/groups/ST/hash/statement.html elérhetőségen találja.
7 Lásd: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

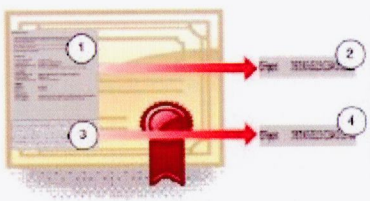
SHA-2-re, utána kell járni, miként lehet frissítenie a szoftverét, mely további költségeket jelenthet. Ezen felül egy ilyen tanúsítvány használata további problémákat is eredményezhet, például előfordulhat, hogy a weboldalt látogató felhasználók böngészője nem támogatja az SHA-2-t. Van azért előnye is, ha az SHA-2-t választjuk, ugyanis várhatóan legalább tíz évig kitart majd mielőtt bármilyen támadás érné.

Háttér információk

- Digitális aláírások, hash-ek és ütközések

A digitális aláírás egy tanúsítványon a 'hash funkció' segítségével történik. Jól ismert példa a hash funkciókra az MD4, MD5 és az SHA különböző verziói. A hash funkció egy rövid karaktersort (a hash) számol egy adathalmazból. Ez az adathalmaz bármi lehet, egy dokumentum, egy e-mail, de akár egy program forráskódja is. A következő ábrán láthatjuk hash szerepét a tanúsítvány aláírásban.





Digitális aláírás elhelyezése és engedélyezése, egy aláírt tanúsítvány a következőképpen készül: (1) A Certificate Authority (CA) megkapja az adatot a jelentkezőtől. (2) A CA egy hash-t számít ebből. (3) A CA saját kulcsával hitelesíti a hash-t. (4) Ez alkotja az aláírt tanúsítványt az eredeti adattal együtt.

A böngésző a következőképpen ellenőrzi a tanúsítványt: a böngésző kiszámítja a hash-t (2) az eredeti adatból (1). Ezután a böngésző dekódolja a hash-t (4), melyet a CA hitelesített (3) Ha mindkét hash (2-4) megegyezik, akkor a tanúsítványt nem módosították, tehát megbízható.

Mivel a hash egy rövid karakter sor, mindig lesz néhány olyan adathalmaz, ami ugyanazt a hash-t generálja.

Egy jó hash funkció a következő tulajdonságokkal rendelkezik:

- Minden változás az eredeti adathalmazon (újraszámolás után) gyökeresen más hash-t kell hogy eredményezzen.
- Megengedhetetlen az, hogy az eredeti adatcsomagot (előkép) visszanyerjük a hash-ből.
- Nagyon nehéz egy második összeállítás (második előkép) készítése az önmagában már létező adathalmazból, ami ugyanazt a hash-t generálná. Ez még nem lehetséges az MD5-tel, de a jelenlegi támadások közel járnak ehhez.
- Nagyon nehéz két olyan egyedülálló összeállítást készíteni, ami ugyanazt a hash-t eredményezné (ütközés), bár ez néha előfordulhat az MD5-tel[8].

8 Az MD5 ütközéseivel kapcsolatos eredményeket a http://www.win.tue.nl/hashclash/ elérhetőségen talál. A szoftver, melynek segítségevel MD5 ütközések készíthetők, szintén itt érhető el.

A titkosítás "fél élete"

Egy jó titkosítás úgy kódolja az adatot, hogy azt csak a megfelelő kód segítségével lehessen visszafejteni. Egy "brute force" támadás egyszerűen csak kipróbál minden lehetséges kulcsot és kiválasztja a megfelelőt ezek közül. Ez nehezen kivitelezhető a gyakorlatban, mert túl sok időt igényel. Hiba lenne azt hinni, hogy bárki képes meghatározhatatlan időre egy jó terméket vagy szolgáltatást készíteni egy "jó" titkosítási algoritmusra alapozva. A valóságban a tények mást mutatnak.

Két tényező határozza meg azt, hogy végül melyik algoritmus nem fog veszíteni az értékéből. Első helyen a számítógépek számítási gyorsasága áll, amely évről évre nő, tehát a 'brute force' támadások hamarosan kivitelezhetőek lesznek a gyakorlatban is. Másodsorban nagyon bonyolult jó kódolási algoritmust készíteni, hiszen a kisebb hibáknak is messzemenő következményei lehetnek az algoritmusban, függetlenül annak bonyolultságától. Éppen ezért nagyon fontos, hogy többen ellenőrizzék ezeket. Ezen folyamat során az eredeti készítő által nem látott hibák majdnem mindig a felszínre kerülnek, de még így is valószínűtlen, hogy az algoritmus hibátlan lesz. A fentiek tudatában bizonyítható, hogy minden gyengeség megrövidíti az algoritmus használhatóságának élettartamát.

Hazai tevékenységek, 2008

Hazai hálózatbiztonsági és kritikus információs infrastruktúra védelmi együttműködések

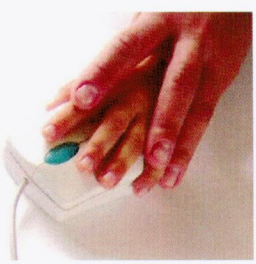
➢ CERT együttműködések

A PTA-CHK 2008 elején újrastruktúrálta szolgáltatásait, amelynek eredményeként alap- és értéknövelt szolgáltatásokat kínál. Küldetéséből adódóan kiszolgálja a magyar kritikus információs infrastruktúra szolgáltatóit incidens esetén, de hosszabb távon törekszik a szolgáltatások értékesítésére is. Kapcsolatait továbbra is a bankok és kritikus infrastruktúra szolgáltatók felé próbálta bővíteni. Ennek eredményeként új szolgáltatási szerződést sikerült kötni 3 hazai bankkal és szolgáltatás kialakítására irányuló tárgyalásokat kezdeményezni a Nemzeti Infrastruktúra Fejlesztő Zrt-vel konkrét, speciális vizsgálati eljárás bonyolítása mellett.

➢ eSec.hu konzorcium

A PTA CHK a 2008. évben is fontosságot tulajdonított a hazai iparági együttműködésnek. Ennek keretében vett részt a magyar informatikai biztonsági cégek által alapított e-Sec.hu konzorcium munkájában. A konzorcium tagjai közösen szervezték meg az Internet Hungary 2008 rendezvény informatikai biztonsági szekcióját, valamint elindultak az NKTH szoftverfejlesztési pályázatán. Az eSec.hu konzorcium célja, hogy a magyar IT biztonsági iparágnak elismertséget és piacot szerezzen a közös fellépések során. A tagok mind magyar tulajdonú KKV-k.

➢ Tudatosítási tevékenység



A tevékenységek között külön említést érdemel a 2008-ban folytatott tudatosítási program. Ennek keretében a PTA CHK működteti a www.biztonsagosinternet.hu honlapot, amely közérthető módon ismerteti meg az informatikai biztonság alapvető kérdéseit, valamint gyakorlati tanácsokkal látja el az érdeklődőket. A honlapra támaszkodva a PTA CHK kidolgozta az általános iskolák számára az informatikai biztonság tananyagát, amelyet kísérleti jelleggel egy általános iskolában, valamint a Budapesti Művelődési Központ "SZÜNIDÖDÖ" továbbképzésén oktattak a PTA-CHK szakemberei.

Ezen kívül a PTA-CHK vezetői előadásokat tartottak a Budapesti Műszaki Főiskola és a Budapesti Műszaki Egyetem biztonsági tudatossági kurzusain, illetve tudományos szervezetek előadás sorozatán (pl. HTE).

A tudatosítási munka egyben kiterjedt a hagyományos médiában történő megjelenésre is, így a PTA CHK képviselői több alkalommal adtak rádióinterjút, illetve jelentek meg országos lefedettségű tévék adásaiban.

➢ Információ megosztó munkacsoportok

A PTA CERT-Hungary hosszú távú célja, hogy a Zöld Könyvben meghatározott kritikus szektorokkal működő kapcsolata legyen. Ennek megfelelően és a nemzetközi trendeket is követve kezdeményezte önkéntes alapon szerveződő információ megosztó munkacsoportok létrehozását.



Az első ilyen munkacsoport a bank és pénzügyi szektor résztvevőivel jött létre a 2006. év végi spam hullám egyik következményeként (Incidens Kezelési Munkacsoport – IKMCS). A munkacsoport résztvevői a Bankszövetség, a PSZÁF, az NNYI, bankok, és a PTA-CHK. A negyedévi rendszerességgel megtartott ülések célja, hogy a felek tájékoztassák egymást az aktuális hírekről, veszélyekről, trendekről. A PTA-CHK szerepe az együttműködésben a nemzetközi CERT hálózatokból tudomásra került informatikai veszélyek hazai terjesztése. Az IKMCS évente szervez gyakorlatot, amelynek egyik célja a bankok és a PTA-CHK közötti munkakapcsolatok elmélyítése. A 2008-ban megrendezett gyakorlat forgatókönyve "egy adatszivárgást előidéző malware" következményeinek felszámolása volt. A gyakorlat növekvő sikerét mutatja, hogy 6 bank vett részt a gyakorlaton.

A 2008-as év nagy előrelépése volt, hogy a GKM kezdeményezésére, a MEH-el, és az NHH-val együttesen, egy munkacsoportba (KIV – Kritikus Infrastruktúra Védelmi Munkacsoport) hívtuk a hazai energiaellátás jelentősebb képviselőit, azzal a céllal, hogy egymás tevékenységét és sajátosságát megismerve egy gyakorlatra vonatkozó forgatókönyvet állítsunk össze az energia szektor és a távközlési szektor interdependenciáit vizsgálva. A forgatókönyv elkészült, a gyakorlat lebonyolítására várhatóan 2009 első felében kerül sor.

Az információ megosztó hálózatok hatékonyabbá tétele céljából a PTA-CHK létrehozott egy olyan információs- és tudásbázis koncepciót és próba verziót, amely képes a kritikus infrastruktúra védelem területéről elérhető lehető legtöbb információt rendezett és kereshető formában, az érzékeny információk megosztási alapelveivel összhangban, a felhasználók rendelkezésére bocsátani.

Az információs- és tudásbázis, azaz a kritikus információs infrastruktúra védelmi portál próba verziója jelenleg publikus formában elérhető a www.kiiv.hu címen. A PTA-CHK biztosítja a portált kiszolgáló technikai eszközöket (pl. szerver(ek), környezet, áram, stb.) és alkalmazásokat (pl. webszerver, adatbázis, stb.), valamint üzemelteti azokat. A próba verzió, a felhasználók és a finanszírozó szervezetek igényei szerint, koncepció szerint vagy attól eltérően bármikor tovább fejleszthető.

A PTA CHK által 2007-ben első alkalommal, sikeresen megrendezett Kritikus Infrastruktúra Védelmi Konferencia folytatásaként, 2008. november 12-14. között a MeH Infokommunikációért és Elektronikus Közigazgatásért felelős szakállamtitkársága, a Nemzeti Fejlesztési és Gazdasági Minisztérium, a Közlekedési, Hírközlési és Energetikai Minisztérium, valamint a Puskás Tivadar Közalapítvány CERT-Hungary Központjának szakmai támogatásával került megrendezésére „Az elektronikus hírközlés kritikus infrastruktúrája és annak védelmi kérdései" elnevezésű gyakorlat (workshop).

A fórumon a résztvevőknek lehetősége nyílt a Nemzeti Kritikus Infrastruktúra Védelmi Program, valamint a kritikus informatikai/hírközlési infrastruktúra védelmére vonatkozó program kidolgozási alapelveinek, a védelmi igazgatási feladatok, az európai kritikus infrastruktúra védelmi feladatok – CIWIN hálózat, a kormányzati ügyeleti rendszer aktuális kérdéseinek, a kritikus infrastruktúra védelmi gyakorlat, valamint a Nemzeti Hírközlési Hatóság (NHH) veszélyhelyzeti tervekkel kapcsolatos ajánlásainak egyeztetésére.

A kritikus infrastruktúrák védelme témájában a konferencia napirendjén szerepelt továbbá a PTA-CHK által működtetett Incidenskezelési Munkacsoport jövőbeli tevékenységének egyeztetése, amely az internetes bankolás biztonságának fokozása érdekében gyakorlatokat szervez, ajánlásokat készít elő, és egyeztető fórumot biztosít a PSZÁF, a Bankszövetség és a Nemzeti Nyomozóiroda közreműködésével.

Pályázati tevékenység

2008-ban a PTA-CHK rendkívül sikeres évet zárt hazai és nemzetközi pályázatok területén. Európai szinten két vonatkozásban nyújtott be sikeres pályázatot, melyek:

- a FISHA (Framework for Information Sharing and Alerting) projekt egy európai információmegosztó, figyelmeztető és riasztó rendszer modelljének kialakítása egyéni felhasználók és KKV-k számára. A projektben a koordinációt és a technikai fejlesztés egy részét is a PTA-CHK végzi. További konzorciumi tagok a lengyel akadémiai CERT (CERT Polska) és a német gelsenkircheni egyetem. A projekt költségvetése kb. 610.000 EUR 2 évre.
- a Safer Internet HU projekt. A projekt célja, hogy felhívja a figyelmet az interneten leselkedő veszélyekre, és ezekre segítséget is nyújtson egy forródrót, egy segélyvonal, és egy tudatosságnövelő központ segítségével. A projekt megvalósításában a PTA-CHK technikai fejlesztéseket biztosít, és támogatja a további partnereket, a Nemzetközi Gyermekmentő Szolgálatot, a Kék-Vonal Segélyvonalat, és a Magyar Tartalomipari Szövetséget. A projekt futamideje 2 év, költségvetése kb. 450.000 EUR.



- Nemzeti Technológiai Platform pályázat: A BME IK szervezésében létrejött NESSI HU platformban a PTA-CHK vállalta fel az informatikai biztonsági munkacsoport vezetését és képviseletét a platform elnökségében. A NESSI HU platform az NKTH "Technikai Platform" pályázatán támogatást nyert a szoftver- és szolgáltatásfejlesztések keretrendszerének és stratégia tervének kidolgozására, működtetésére.
- PSZÁF pályázat: A PTA-CHK a Pénzügyi Szervezetek Állami Felügyelete által kiírt pályázaton nyerte el azt a támogatást, amely az internetes banki tevékenység kockázatainak felmérésére, valamint a védekezés lehetséges eszközeinek kimutatására irányul. A felmérés eredménye egy tanulmány keretein belül kerül nyilvánosságra (megvalósításra) .

Nemzetközi tevékenységek, 2008

Tagi közreműködés a meghatározó hálózatbiztonsági és kritikus infrastruktúra védelmi nemzetközi szervezetek működésében.

A PTA-CHK nemzetközi tevékenysége során képviseli a hazai hálózat- és információ biztonsági, illetve kritikus információs infrastruktúra védelmi területet a téma meghatározó nemzetközi szervezeteiben. Több nemzetközi szervezetben a kizárólagos nemzeti kapcsolati pont szerepét is betölti. A 2008. év során a következő fontosabb rendezvényeken vett részt és/vagy szervezett a PTA-CHK:

- 2008. január: TF-CSIRT/TI (Task Force-CSIRT/Trusted Introducer – európai CERT fórum) éves közgyűlés (Prága). Eredmények: akkreditált tagként részvétel a zárt üléseken is, szavazás személyi kérdésekben, szakmai eszmecsere, kapcsolatépítés.
- 2008. január (Budapest), április (Helsinki), szeptember (Rotterdam): részvétel az EGC (European Government CERTs) soron következő ülésein. Januárban Budapesten láttuk vendégül az EGC tagokat. Fő témák az év során: tagbővítés (Spanyolország felvétele), szakmai fejlesztések bemutatása, megosztása, közös fejlesztési koncepció – kapacitás megosztás.
- 2008. március: IWWN Cyber Storm II megfigyelő program (Washington D.C.). A 15 IWWN tag meghívást kapott az amerikai Cyber Storm gyakorlat megfigyelésére. A meghívás jelentősége, hogy a következő gyakorlatban Magyarország is aktívan részt vehet. Az IWWN (International Watch and Warning Network) hálózat a 15 tagország döntéshozói, incidens kezelési és bűnüldözési szakértőinek kezdeményezésére létrejött zártkörű információmegosztó fórum.
- 2008. március (Amszterdam), november (Budapest): részvétel az EUSCSIE (European SCADA and Control Systems Information Exchange – európai irányítási rendszerek információmegosztó csoportja) soron következő ülésein. Márciusban, új tagként először vettünk részt a SCADA és irányítási rendszerek biztonsági csoportjának ülésén. A tagság célja, hogy a PTA-CHK is közreműködjön a hazai kritikus infrastruktúra szolgáltatók felé a SCADA és irányítási rendszerek sérülékenysége területén. Novemberben Budapesten került megrendezésre az ülés. A csoportban szerzett tapasztalatok megosztásra kerülnek a hazai szakma és az NGFM (korábbi GKM) képviselőivel.
- 2008. április (Szófia), június (Budapest): a PTA-CHK és az ENISA (Európai Hálózat- és Információ Biztonsági Ügynökség) egy kétfordulós közös képzési programban részesítette a bolgár Információ Technológia Ügynökség munkatársait, a bolgár kormányzati CERT létrehozása céljából. A bolgár CERT 2008 végére elindította szolgáltatásait.
- 2008. június: éves FIRST konferencia részvétel (Vancouver). Akkreditált tagként részvétel az éves közgyűlésen, kapcsolatépítés, nemzetközi trendek áttekintése. A FIRST (Forum of Incident Response and Security Teams) a CERT-ek világszervezete, amely globális szinten képes fellépni a fenyegetettségek ellen.
- 2008. június: éves CERT/CC-USA, nemzeti CERT-ek ülése (Vancouver). A CERT/CC által szervezett éves rendezvény célja, hogy építse a nemzeti/kormányzati CERT-ek hálózatát. A saját tevékenységek, fejlesztések bemutatása mellett, szakmai eszmecserére, új nemzeti CERT-ek megismerésére került sor.

- 2008. szeptember: IWWN konferencia (Rotterdam). Részben magyar kezdeményezésre került megszervezésre az idei IWWN konferencia. A cél a középtávú stratégia meghatározása volt, melyre a PTA-CHK is tett javaslatot. Ennek eredményeként került bevezetésre a titkárság, melynek szerepét a PTA-CHK tölti be a következő időszakig. A konferencia további témái közé tartozott a rendszeres IWWN gyakorlatban való részvétel, eredmény. A jövőre vonatkozóan, a PTA CHK a gyakorlatok összetettségének növelését javasolta, amelyet a tagok elfogadtak.
- 2008. október: Meridian kormányzati kritikus információs infrastruktúra védelmi (CIIP) konferencia (Szingapúr). A konferencia szervezőbizottságának tagjaként a PTA-CHK aktív szerepet vállalt a konferencia megvalósításában, amely először került Európán kívül megrendezésre. A Meridian folyamatot a PTA-CHK által szerkesztett negyedéves hírlevél is támogatta, amely nemzeti és nemzetközi CIIP újdonságokat hivatott bemutatni.
- 2008. november: financial ISAC workshop (Budapest). A holland pénzügyi ISAC-el, a holland és magyar bankszövetségekkel, és az ENISA-val közös szervezésű kezdeményezés célja, hogy a bankok, CERT-ek, és bűnüldözési szervek közös összefogásával egy európai információ megosztó platform támogassa a pénzügyi szektor biztonságosabb működését. A rendezvényt a PTA CHK szervezte és részt vesz a további szervezési munkában is.

Egyéb nemzetközi tevékenységek

A PTA-CHK testületi elnöke ellátta az ENISA igazgatótanácsának alelnöki tisztjével kapcsolatos feladatokat, valamint az igazgatótanács külön munkacsoportjában működött közre az ENISA 2009-2011. évi stratégiájának kidolgozásában. Az ENISA munka keretében összefogta az ENISA-ról szóló tanácsi rendelet módosítására adott magyar vélemény kialakítását, részt vett az IDC által végzett "EU informatikai és hálózati biztonsági piacfelmérés" tanácsadó bizottságában, valamint az EU Bizottsága által elindított "Új EU információ biztonsági szabályozás" -ról szóló konzultációs folyamat ülésein.

Nemzetközi vonatkozásban említést érdemel a PTA-CHK törekvése a kétoldalú megállapodások kialakítására. Ennek egyik eredménye, hogy a PTA-CHK kétoldalú együttműködési megállapodást kötött a kínai kormányzati CERT-tel (CNCERT/CC). A megállapodás értelmében a két szervezet rendszeresen oszt meg egymás között információt incidensekről, sérülékenységekről, illetve egyéb nemzetközi, tudatosítási tekintetben.

A kétoldalú együttműködés másik példája az osztrák kormányzati CERT-tel (CERT.at) való egyeztetés, amelynek következményeként a két szervezet kölcsönösen képviseli egymás érdekeit releváns kérdésekben.

A nemzetközi tevékenység további eredménye Európai Uniós forrás elnyerése egy pályázat kapcsán. A lengyel CERT-tel és a gelsenkircheni (Németország) egyetemmel közös pályázatot nyújtott be a PTA-CHK az Európai Bizottság Justice, Freedom, and Liberty főosztályára egy európai információmegosztó és riasztó rendszer modelljének létrehozására, egyéni felhasználók és KKV-k számára.

2008-ban, a PTA CHK a működése során felhalmozott tudást nemzetközi szinten is próbálja kamatoztatni. Egy négyoldalú megállapodás keretében, az amerikai George Mason Egyetemmel, az amerikai CERT/CC-vel, és a japán JPCERT-tel együtt egy CERT kapacitásbővítő kezdeményezést indít, amelynek célja, hogy regionális workshop-ok szervezésével olyan országokban is támogassák CERT-ek létrejöttét, amelyekben még nem léteznek.

Ilyen típusú tevékenység a korábban említett bolgár együttműködés is, illetve a görög akadémiai CERT FIRST akkreditációjában való szponzoráció/szakértői részvétel, amely a működési folyamatai megbízhatóságát hivatott igazolni a nemzetközi CERT fórum felé.

Elérhetőségeink

Puskás Tivadar Közalapítvány

PTA CERT-Hungary Központ

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 PTA CERT-Hungary ügyelet adatai:

E-mail:cert@cert-hungary.hu
Tel.: +36-1-301-2079
Fax: +36-1-353-1937