HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Serege Gábor
serege.gabor@zmne.hu

HEKKERTÁMADÁSOK A TÁVOL-KELETRŐL

Absztrakt

Az elmúlt évek során bizonyos változásokat figyelhettünk meg a hekkertámadások jellemvonásaiban. A világ „legtehetségesebb" hekkereit adó USA és Oroszország mellett új hekker generáció jelent meg a távol-keletről. Ezzel párhuzamosan egyre több ország esett áldozatul a kínai a régióból indított támadásoknak. Az elkövetők kilététére utaló nyomok felkutatása szinte lehetetlen, azonban mégis sokan nyíltan a kínai rezsimet állítják az akciók hátterébe.

By inspecting the past years, we could realize the changing of the features of hacker attacks. A new hacker generation has appeared from the Far East besides the classical American and Russian hackers. Since this time more and more nations have felt a victim to hacker attacks from region of China. In most cases finding evidence is impossible, but in the face of this fact, they suspect the governance of the People's Republic of China.

Kulcsszavak: *hekkertámadás, Kína, hálózati biztonság, Internet ~ hacker attack, China, network security, Internet*

BEVEZETÉS

Az információs technológia rohamléptékű fejlődésének eredményeként olyan új infokommunikációs berendezések tulajdonosaivá válhatunk, amelyek néhány évvel ezelőtt még csak tudományos elképzelésként szerepeltek a médiában és elérhetetlennek tűntek. Az információs társadalom befogadóképessége, illetve az új csúcskategóriás eszközök iránti igény nyújtja az IT szektor mozgatórugóját, amely cserébe elárasztja a piacokat a mindennapi életünket kényelmesebbé tevő szolgáltatásokkal és berendezésekkel. Példaként említhetjük a navigációs berendezéseket, az okostelefonokat, az internetes bankolást, illetve fizetési lehetőségeket, melyeket valószínűleg már használjuk is, vagy jövőbeli használatuk a terveink között szerepelnek.

A könnyen megszerezhető kényelemnek azonban hatalmas ára is lehet. Az említett eszközök és szolgáltatások közös jellemzője, hogy működésük alappillérét az Internethez való csatlakozás jelenti, ami egyrészt utat nyit számunkra a világ felé, másrészt potenciális

célponttá tesz bennünket. Az országok népességéhez viszonyított internetes csatlakozások számát felmérő kutatásban Észtország az elsők között szerepel, amely egyben utal lakosságának Internetes szolgáltatásoktól való függőségére is. A történelem során Észtországnak kellett elsőként szembesülnie a hálózati kapcsolatra épülő csúcstechnológia sötét oldalával, amikor 2007 májusában elvesztette az IT infrastruktúrája ellen indított hekker hadjáratot. [1]

A jól szervezett hekkertámadások jellemzője, hogy a támadó kiléte ismeretlen marad. Eljutni a tényleges kiindulópontig szinte lehetetlen, azonban meghatározni a földrészt, országot vagy épp régiót már könnyebb feladat. Amíg a XXI. század első éveiben a támadások meghatározó részét egyértelműen amerikai vagy épp orosz területekről hajtották végre, addig a 2005-ös évtől kezdve egyre gyakrabban indulnak támadások távol-keleti szerverekről. Ez a tény arra enged következtetni, hogy a távol-keleti informatikai „szakemberek" képzettségben, tudásban és technikai támogatottságban egyre jobban felzárkóznak a legkiemelkedőbbek csoportjába. [2]

A hekkertámadások kiemelt jelentőségéből adódóan vizsgálatom célja egyrészt megadni a hekker szó napjainkban használt jelentését, másrészt összefoglalni az utóbbi évek legjelentősebb távol-keleti szerverekről indított offenzíváit. Továbbá a megtámadott országok által kiadott jelentések alapján beazonosítani a támadók nemzetiségét és röviden bemutatni az Amerikai Egyesült Államok álláspontját megfogalmazó „Műveletek a cybertérben" elnevezésű doktrínát.

KI AZ A HEKKER?

Az elmúlt évek során a hekker szó jelentése gyökeres változáson ment keresztül, ezért ebben a fejezetben be kívánom mutatni, hogy mit takart ez az elnevezés a múltban és mit értünk alatta most, a jelenben.

Áttekintve a média szóhasználatát megállapítható, hogy a mindennapi szóhasználatban a hekker elnevezést hallhatjuk minden olyan esetben, amikor a számítógép rendszerek biztonsági réseit felismerő emberekről közölnek híreket. Egyszerűen a hekker elnevezés, mint gyűjtőnév terjedt el, ezért általában csak a hír tartalmából derül fény arra, hogy az esemény mögött ténylegesen milyen szándékú, illetve képzettségű személy vagy személyek állnak.

Meglátásom szerint azonban érdemes különbséget tenni, főleg azért mert a múltban a hekker elnevezést csak a kiemelkedő tudással rendelkező szakemberek érhették el. Ezek a szakemberek nem feltétlenül csak az informatika területéről kerülhettek ki, hanem egyéb más, mint például elektronikai, műszaki szakterületekről is. Köztük a kapocs a kimagasló alkotói szakértelem, az elismertség és a köztisztelet volt.

Ezzel ellentétben a mostani jelentés nem ennyire egyértelmű. Az előbb említett hagyományos értelemben vett használata megszűnni látszik. A hekker egyre inkább valamilyen számítógépes bűnözőt takar, aki tevékenységével az informatikai biztonság egyes összetevői ellen indít offenzívát. Céljai között elsőként szerepel az adatok ellopása, módosítása, törlése vagy épp az adott szolgáltatást biztosító informatikai rendszer rendelkezésre állásának a negatív befolyásolása. Azonban ez a leírás, a hekker szó által aggregált 3+1 csoportok egyes részeire igaz csak.

A hekker szó a következő csoportokat foglalja magába:

1. *Fekete kalapos (Black-hat) hekker:* Tevékenységére a fentebb leírtak jellemzők. Motivációs eszközök a pénz, az elismertség (alvilági körökben) és egyes esetekben a szélsőséges meggyőződés.[1]

[1] A fekete kalapos hekkerek műveleti területe az információs társadalom informatikai infrastruktúrájával együtt növekvő cyber-tér, amely egyben lehetőséget biztosít az aszimmetrikus hadviselés országhatárokat átlépő megvívására is.

2. *Fehér kalapos (White*-hat) hekker: kiemelkedő informatikai tudását legális megbízás alapján használja fel. Célja az adott számítástechnikai rendszer sebezhetőségének vizsgálata a szerződésben meghatározott kritériumok alapján. Feltárja a biztonsági hiányosságokat és javaslatot tehet azok kijavítására. A fehér kalapos hekker másik elterjedt elnevezése az etikus hekker.
3. *Szürke kalapos (Grey*-hat) hekker: mind fehér, mind fekete kalapos hekker megbízásokat is elvállal, így tevékenységére a kettősség jellemző.
4. *Script kiddie*[2]*:* az előző három csoport képviselőivel ellentétben nem rendelkezik kimagasló informatikai tudással. Tevékenységének alapját az Internetről letölthető és testre szabható kártékony alkalmazások adják. Általában iskoláskorú számítógépes vandálnak tekinthető, akinek célja az adott informatikai hálózat (például: iskola) szolgáltatásainak a támadása, illetve az abban való károkozás. Motivációs tényező a vandalizmus, a csínytevés.[3]

Összefoglalva megállapítható, hogy a hekker szó jelentése elvesztette eredeti tartalmát. Jelenleg kizárólag csak az informatikához kapcsolható, illetve gyűjtőnévként használva nem tesz különbséget a különböző céllal és motivációval rendelkező csoportok között. Az egyes csoportok jól elkülöníthetők egymástól, azonban érdemes megemlíteni, hogy az esetek jelentős százalékában a fehér kalaposok közé olyanok kerülnek, akik a fekete kalapos oldalon már bizonyítottak. [4]

AZ ELMÚLT ÉVEK HEKKERTÁMADÁSAI

Az első hekker támadás John Draper nevéhez köthető, aki az 1960-as évek elején elsőként generált olyan speciális telefon hangimpulzust, amellyel annak nem várt működését tudta előidézi. A kezdeti, kizárólag telefonhálózatokhoz köthető hackelések a 4. generációs számítógépek széles körű elterjedésétől számítva az informatikai hálózatok irányába tolódtak el. Napjainkra a hekkertámadásokról szóló hírek a média állandó szereplőjévé váltak, ami alátámasztja azt a tényt, hogy azok mindennapos események, illetve számuk ugrásszerűen megsokszorozódott.

A támadások döntő része amerikai vagy orosz hekkerek tevékenységéhez volt köthető. Az ezredforduló második felétől, azonban megfigyelhető egy fontos változás: új hekkercsoportok kezdtek megjelenni a Távol-Keletről.

Ebben a fejezetben össze kívánom foglalni mindazon kiemelkedő jelentőségű hekkertámadásokat, amelyek az elmúlt 3 év során kerültek nyilvánosságra és a kiinduló pontjuk a Távol-Keletre tehető. Fontosnak tartom hangsúlyozni, hogy a támadások hátterében állók pontos adatai (név, nemzetiség, megbízó) igen ritkán fedhetők fel, éppen ezért az általam bemutatott esetekben is csak feltételezni tudták a támadók kilétét.

A TÁVOL-KELETRŐL INDÍTOTT LEGJELENTŐSEBB HEKKERTÁMADÁSOK 2007-2010 KÖZÖTT

2007. augusztus: A „Sárga kémek” címmel jelent meg egy cikk a „Der Spiegel” német napilapban, amely arról számolt be, hogy a kormányzati informatikai hálózat több szegmensében trójai faló típusú programra bukkantak. A számítógépekhez hátsó kaputnyitó kódok Microsoft Office dokumentumokba rejtve kerültek a célhálózatba.[5]

[2] A „script kiddie” angol elnevezésnek magyar megfelelője még nem ismert.

A kémkedési ügy hatalmas felháborodást keltett Németországban, mondván Kína így akarja ellopni a technológiai újdonságokat.

A támadás kiindulási pontját pontosan nem tudták meghatározni, azonban egyértelműen Kínát állították az eset hátterébe.[6]

2007. szeptember: A brit külügyi iroda számolt be távol-keleti támadásokról, mintegy csatlakozva a németországi incidenshez. A hivatalos értesítők alapján a kormányzati szektort nap, mint nap érik informatikai támadások, azonban a Távol-Keletről kiindulók száma jelentősen megnőtt.[7]

Ez év végén a brit biztonsági hivatal vezetője levelet küldött a magasabb beosztású állami alkalmazottaknak, illetve a polgári szféra jelentősebb vezetőinek, amelyben felhívta figyelmüket a kínai informatikai kémtevékenységre.[8]

2007. október: Az Amerikai Egyesült Államok nemzeti laboratóriumának informatikai rendszerében fedeztek fel illetéktelen alkalmazásokat. A németországi támadáshoz hasonlóan a fő cél az adatok eltulajdonítása volt az állomásokon nyitott hátsó ajtókon keresztül. Ez az intézmény kiemelt fontossággal bír a mai napig is, hiszen több olyan szigorúan titkos technológiai dokumentációt tárolnak itt, mint például a nukleáris fegyverekkel kapcsolatos információkat.

A betörés körülményeit vizsgáló csoport jelentése alapján a támadás, amely az alkalmazottak elektronikus levelezésének a felderítésével, majd a megfelelő csatolmánnyal ellátott email elindításával kezdődött egy jól szervezett és irányított hekker csoportra utalt. John Markoff biztonsági szakértő nyilatkozata alapján a támadás nyomait felkutatva Kínába vezető szálakat találtak, ami természetesen nem bizonyíték arra, hogy kínaiak követték volna azt el.[9]

2008 április: Belgium és India csatlakozott azon országokhoz, amelyek az interneten indított támadások miatt nyíltan kezdték vádolni a kínai rezsimet. Belgium álláspontja szerint az akciók hátterében Kína állt. A fő okként Brüsszel kiemelt fontosságát emelték ki a NATO-ban és az Európai Unióban betöltött szerepe alapján.[10]

Indiai nyilatkozatok szerint az országot naponta több száz hálózati támadás érte a szomszédos államból, amelyek célja a kormányzati informatikai hálózat folyamatos figyelése és térképezése volt. Ez a tevékenység nem csak az információk megszerzésére irányult, hanem a kritikus informatikai infrastruktúra gyenge pontjainak a felderítésre is.

2008 november: Távol-Keletről származó támadás érte a Fehér Ház levelező rendszerét. Ugyan ebben a hónapban látott napvilágot a NASA rendszerét 2005-ben ért támadásról tudósító beszámoló is, amelyet addig titokban tartottak. A taiwani szerverekről kiinduló akció során a behatolók több hónapon keresztül zavartalanul másoltak titkos adatokat az űrközpont szuper titkos számítógépeiről, illetve ki tudták terjeszteni hozzáférésüket más kiemelt fontosságú adatbázisokhoz is. A végeredmény 20 GB letöltött adat, mintegy 30 millió oldalnyi csúcstechnológiát tartalmazó dokumentáció.

Az eltulajdonított adatokból származó károk mellett érdemes kiemelni a morális veszteséget is. Az Amerikai Egyesült Államok csúcs kategóriájú informatikai biztonsági rendszerrel ellátott hálózata veszteségként került ki a cybertérben indított támadásból.

2009. április: A támadások középpontjában ismételten Németország állt. A hivatalos tájékoztatók alapján az országot igen jelentős mennyiségű támadás érte távol-keleti szerverekről. Az akció forgatókönyve a már ismert eljárást tartalmazta: a kijelölt célpontok

levelezési címeinek felderítése után megfelelő csatolmánnyal ellátott levelek által kívántak hozzáférni az adatokhoz.

Németországon kívül a hónap során hasonló támadás érte az ausztráliai elnököt is, valamint a dél-koreai kormányzati szektor pénzügyi részét is.[11]

2010. január: Támadás érte a Google rendszerét. Az eddig számbevett esetekkel ellentétben a célpont nem állami rendszer volt, hanem a Kínában jelentős részesedéssel bíró külföldi keresőóriás. Elemzők véleménye alapján a háttérben a Google és Kína nézetkülönbsége állt, ugyanis a vállalat meg akarta szüntetni a keresőmotor „cenzúráját".

A januárban felröppent hírek szerint az akció nem csak a Google-t érintette, hanem másik 34 óriásvállalatot is. Az elkövetés módja ismételten kiemelkedő szervezettségre, szaktudásra és anyagi forrásokra utalt: a támadók olyan szervereket hoztak létre, amelyek weboldalaiba az Internet Explorer biztonsági hiányosságát kihasználó kódot injektáltak.

Összegezve megállapítom, hogy a bemutatott esetekben több hasonlóság is felfedezhető:

- a célpontok meghatározó része a különböző államok kormányzati, kutatási, és technológiai informatikai hálózatai voltak. Ezek a rendszerek különböző szintű minősítéssel rendelkező fontos dokumentumokat tároltak;
- biztonsági szakértők véleménye alapján a behatolások hátterében összehangolt, magasan képzett hekkerek álltak;
- a támadóknak nem csak a kimagasló szakértelemre, hanem jelentős anyagi háttérre is szükségük volt az akciók kivitelezéséhez;
- a támadások kiinduló pontjára utaló nyomok a Távol-Keletre, azon belül is főleg Kína négy nagy városára, illetve Taiwanra mutatnak;
- valamennyi megtámadott ország bizonyos mértékben a kínai államot állította az akciók hátterébe.

KÍNA RÉSZESEDÉSE A HEKKERTÁMADÁSOKBAN

Az előzőekben számba vett hekker műveletek egytől egyig professzionális elkövetőkre utaltak, akik nagy hangsúlyt fektettek az árulkodó nyomok álcázására, illetve megsemmisítésére. A konkrét bizonyítékok ellenére a megjelenő nyilatkozatok a kínai államot tüntették fel megbízóként és az anyagi, technikai háttér biztosítójaként is. Az alfejezet célja bemutatni azokat a tényeket, amelyek a kínai szerepvállalást támasztják alá, illetve cáfolják azt.

Egy informatikai biztonsággal foglalkozó kanadai csoport (Secdev Group) 2009 márciusában egy világméretű „kémhálózat" létét fedezte fel. A rendszer irányításáért felelős szerverek azonosítása által a nyomok egyértelműen egy kínai, rádióelektronikai felderítést végző katonai egységhez vezettek. Ez a „gh0st RAT" trójai alkalmazásra épülő rendszer a világ 103 országára terjedt ki, és mintegy 1300 követségi, kormányzati, gazdasági intézményi célpontot tartalmazott.

A trójai alkalmazás önmagában egy viszonylag egyszerű működési mechanizmuson alapult, amely során először létrehozott egy dll kiterjesztésű file-t, majd elindított egy szolgáltatást, aztán végrehajtotta a szükséges módosításokat a regisztrációs adatbázisban és végül nyitott egy portot. A támadók így teljes hozzáférést kaphattak a „fertőzött" gépekhez, amelyekről nem csak a tárolt adatokat másolhatták le, hanem a csatlakoztatott hang és képrögzítő perifériák vezérlésével meg is figyelhették az adott felhasználót.

A GhostNet leleplezése világszerte óriási felháborodást váltott ki. A kémkedési botrány ugrásszerűen megnövelte azok számát, akik nem csak ezen ügy kapcsán, hanem a többi Távol-Keletről indított támadás esetében is már nyíltan a kínai rezsimet tették felelőssé. Kína

hivatalosan még az egyértelmű bizonyítékok[3] ellenére sem ismerte el a vádakat, ellenben többször hangot adott stratégiai elképzeléseinek, amelyben egyértelműen kinyilvánította álláspontját a cybertérben megvalósítható műveletekkel kapcsolatban.[12]

Véleményem szerint ezek a tények nem elégségesek ahhoz, hogy a kínai állam szerepvállalását egyértelműen bizonyítsák. Kína az elmúlt évtized során hatalmas beruházásokat hajtott végre informatikai infrastruktúrájának fejlesztése érdekében. Jelenleg Kína rendelkezik az egy országra eső legtöbb internet-felhasználóval (400 millió), így a nagy számok törvényét alapul véve feltételezhető, hogy számos kiemelkedő tudású hekker is van közöttük. A rezsimhez köthető szálak nélkül más nemzetek megbízása alapján, vagy szélsőséges ideológiai nézetekkel vezérelve is indíthatták ezeket a támadásokat. Továbbá érdemes megfigyelni az 1. számú táblázatot, amely azokat az országokat mutatja, amelyek a világon a legtöbb ártalmas kódot bújtató webszerverrel rendelkeznek. A lista alapján a kínai szerverek 44,8%-a tartalmazott olyan kódokat, amelyek az adott weboldal meglátogatása során vagy adathalászatra specializálódtak, vagy egyéb alkalmazást próbáltak futtatni a gyanútlan látogató számítógépén. Meglátásom szerint ebből két következtetés vonható le:

1. az adott állami szabályzók nem voltak képesek féken tartani az újdonságként megjelenő kínai hekker generációt;
2. Kína vált a legjobb kiindulóponttá a hekkertámadások végrehajtására, ugyanis a kialakult nemzetközi morál alapján elsőként a kommunista vezetést vádolták.

Top malware-hosting countries

Position	Last month	Country	Percentage of reports
1	1	China (inc. HK)	44.8%
2	2	United States	20.8%
3	3	Russia	11.3%
4	4	Ukraine	7.7%
5	8=	Poland	2.4%
6	5	Germany	1.6%
7	Re-entry	Netherlands	1.1%
8	Re-entry	Italy	0.9%
9=	8=	Canada	0.8%
9=	7	United Kingdom	0.8%
Others			7.8%

1. táblázat. Ártalmas kódokat tartalmazó webszerverek országos megoszlása 2008-ban (Forrás: www.sophos.com)

[3] A nyomozás során feltárt bizonyítékok: egy kínai egyetemista hekkert sikerült beazonosítani és felderíteni a kapcsolatait, amelyek az irányításért felelős központhoz vezettek, a vezérléshez szükséges szálak egy katonai szervezethez vezettek, az óriási mennyiségű információ feldolgozásához kiemelkedő informatikai infrastruktúrára volt szükség, amelynek rendszerben tartása óriási anyagi hátteret feltételez.

Végkövetkeztetések

Összegezve megállapítható, hogy a cybertében végezhető műveletek jelentősége és súlya folyamatosan növekszik. Az információs társadalmat kiszolgáló informatikai infrastruktúra védelmi vonala nem képes megállítani az olyan hekkertámadásokat, amelyek hátterében kimagasló tudású emberek állnak megfelelő anyagi és technikai támogatással. Az elkövetők kilétéhez vezető nyomok felkutatása sokszor lehetetlen. Az alkalmazott titkosító algoritmusok és útvonalvezérlések személytelenné teszik a támadókat.

Az elmúlt évtizedben Kína jelentős lépéseket tett az országa informatikai hálózatának a kiépítésére. Napjainkra fejlett hálózata 400 millió felhasználót szolgál ki. Az infrastrukturális beruházást szakmai felzárkózás követte, amely hatására jelentősen megnőtt a kínai hekkerek száma. Illegális tevékenységük folytatására kedvező táptalajt szolgáltatott az országban kiépülő szerverfarmokon elhelyezhető törvénytelen alkalmazások lehetősége. Természetesen ez az állapot más nemzetek hekkerei számára is „szinte" kihagyhatatlan alkalmat jelentett.

Az említett esetek során a támadást elszenvedett országok igaz változó formában, de mind a kínai vezetést állították az akciók hátterébe. A vádak mögött konkrét bizonyítékokkal- egy eseten kívül (GhostNet)-, nem tudtak szolgálni, mivel csak a távol-keleti kiindulópontot sikerült beazonosítani.

A cybertér „kalózai" között vitathatatlanul megjelent a távol-keleti hekker generáció is, amely eredményeként Bruce Scheiner világhírű biztonsági szakember szavainak aktualitása megnövekedett. Véleménye szerint: „A technológiai fejlődés néha a támadást könnyíti meg, máskor pedig a védekezést. Rohamosan változó technológiai világunkban fontos, hogy figyeljünk az új biztonsági egyensúlyhiányokra."[13, [12 pp.]]

A felbomló egyensúly olyan változásokat idézett elő, amelyek megkövetelték az internetes bűnözés felderítésére alkalmas világméretű monitor hálózat rendszerbeállítását, vagy épp a cybertérhez köthető műveletek doktrinális szabályozását.

Irodalom

[1] Észtország: tájkép hekkercsata után, letöltve: 2010-11-25
http://index.hu/tech/net/eszt2060807/

[2] US report: China is expanding its corporate cyber espionage, letöltve: 2010-11-25
http://www.h-online.com/security/news/item/US-report-China-is-expanding-its-corporate-cyber-espionage-838173.html

[3] Hekker, letöltve: 2010-11-14
http://hu.wikipedia.org/wiki/Hekker

[4] USA Defense Department Recruits New Hekkers From DEFCON Hacking Conference, letöltve: 2010-11-23
http://scforum.info/index.php?PHPSESSID=a975e5c9e872b996cb791807f98cc01c&topic=3069.msg6940#msg6940

[5] Ulf Gartzke: Outrage in Berlin Over Chinese Cyber Attacks, letöltve: 2010-11-24
http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp

[6] Southern Weekend: Chinese hekkers are "black"?, letöltve: 2010-11-22
http://www.tekbar.net/hekkers-and-security/southern--weekend-chinese-hekkers-are-black.html

[7] Titan Rain: How Chinese Hekkers Targeted Whitehall, letöltve: 2010-11-23
http://www.buzzle.com/articles/151328.html

[8] MI5 alert on China's cyberspace spy threat, letöltve: 2010-11-22
http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

[9] China suspected in hacking attempt on Oak Ridge National Lab, letöltve: 2010-11-24
http://www.industrialdefender.com/general_downloads/news_industry/2007.12.10_china_suspected_in_hacking_attempt_on_oak_ridge_national_lab.pdf

[10] Is China attacking Belgian computers?, letöltve: 2010-11-05
http://www.upi.com/Top_News/2008/05/03/Is-China-attacking-Belgian-computers/UPI-70831209790694/

[11] John Goetz – Marcel Rosenbach: 'Ghostnet' and the New World of Espionage, letöltve: 2010-11-20
http://www.spiegel.de/international/world/0,1518,618478,00.html

[12] Tracking GhostNet, letöltve: 2010-11-10
http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[13] Bruce Schneier: Schneier a biztonságról, HVG Kiadó Zrt, Budapest, 2010, ISBN: 978-963-304-026-3