A kiberbűnözés a drognál is nagyobb üzlet

Számítógépes kémkedés vadnyugati módszerekkel · A hazai törvények – elméletileg – védelmet jelentenek a támadók ellen

A különféle kiberkémkedési ügyek miatt bizalmatlansági válság uralkodik a világban – mondta lapunknak Bencsáth Boldizsár kibervédelmi szakértő, a CrySyS Lab munkatársa. A számítógépes bűnözés többek szerint mára nagyobb üzletté vált, mint a drogkereskedelem.

Ruzsbaczky Zoltán

A közelmúltban ötmillió gmailes e-mail címet loptak el és hoztak nyilvánosságra jelszavakkal együtt. Mennyire vannak ma biztonságban a magánemberek adatai?

– A konkrét esetben valószínűleg több módszer együttes használatával, köztük például kémszoftverrel – vagyis olyan programmal, amely a számítógépekbe férkőzve képes adatokat szerezni – szedtek össze jelszavakat az érintett felhasználók gépéről. A baj mégis az, hogy maga a jelszó gyenge elem: az emberek rosszat választanak, könnyű ellopni, nehéz rá emlékezni, vagy több helyen ugyanazt használják. Más módszereket kellene kitalálni helyette, sokan próbálkoznak is ezzel, elérkezettnek látszik az idő, hogy túlhaladjuk a jelszavakat. Más szempontból ijesztő, hogy egyre több a feltörés, de erre számíthatunk, hiszen ahogy az életünkbe befurakodik a kibervilág, miután egyre több adatunk van az interneten, úgy egyre nagyobb értékekhez lehet jutni egy feltörés során. Az elektronikus pénztárgépekkel például az adócsalás számítástechnikai problémává vált, a bűnözők célja a rendszer feltörése lehet majd. A támadások egyre nagyobbak lesznek, mert a rendszereink is egyre nagyobbak. A védekezés is egyre nagyobb hangsúlyt kell hogy kapjon, de nem mindig látszik tisztán, hogy miként tudunk előrelépni, és ez nagy baj. Ha nem tudjuk megvédeni magunkat, az emberek nem fogják az internetes rendszert – például az internetbankot – biztonságosnak érezni. Ha pedig nem online, hanem személyesen intézik majd a dolgaikat, elveszhet sok minden, amiért küzdöttünk.

– A hackerek mindig egy lépéssel előttünk járnak?

– Előrébb is kell járniuk, hiszen sok előnyük van, és ha nem járnának előttünk, nem lehetnének sikeresek. Nekik csak egy hibát kell találniuk a védelmen, nekünk viszont az összes hibát ki kell javítanunk. Emellett fontos, hogy a támadónak elemi érdeke vigyázni a saját biztonságára.

– A már említett Gmail-jelszavak ellopásáért felelős embereket megtalálhatják?

– Előfordulhat, de több probléma is van. A legnagyobb általában a nemzetközi környezet és a jogrendszer. Európában talán könnyebben el lehetne ítélni a felelőst, de lehet, hogy más kontinensen van, esetleg csapatban követte el a lopást. Ha a bűnesethez használt szerver Brazíliában található, a támadó Oroszországban, az adatokat viszont Hollandiába vitték, az áldozatok pedig mondjuk angolok, akkor még az sem világos, melyik ország jogrendszere szerint kellene eljárni. És ez csak egy a jogi és szervezési problémák közül.

– Van esély az összehangolásra?

– Törekvés van, de nem egyszerű a helyzet. Ennek ellenére előfordulnak sikerek: ha a támadó nem volt elég okos – nyomokat hagyott maga után –, és európai, akkor előfordulhat, hogy összehangoltan felderítik, és az elkövető ellen eljárás indul. Más szervezetek mellett a különböző országokban több területen működő Cyber Emergecy Response Teamek tudnak talán legjobban ilyen incidenseket kezelni. Ezek célja, hogy az egyes országok kapcsolatot tartsanak egymással, és megpróbáljanak információt cserélni, együttműködni a bűnüldöző szervekkel, tehát a bűnözők ne számítsanak semmi jóra.

– Tud példát említeni nemzetközi támadásra?

– A legjobb példa a kéretlen reklámlevelekben hirdetett gyógyszerek esete, itt szinte mindig több ország érintett. *Félegyházi Márk* kollégám korábbi csapatával megvizsgálta, hogy mi történik a kéretlen reklámok fogadásától kezdve: hol van a megrendeléshez használt kiszolgáló, vagy például hogyan jut el a pénz a bűnözők által használt bankokba. Arra jutottak, hogy általában több ország is érintett: az egyik országban gyártott gyógyszert egy másik országban lévő weboldalon rendelték meg, egy harmadik országból küldték ki, a pénzt elfogadó bank pedig egy negyedikben volt. Rájöttek, hogy a folyamatot leginkább a pénzintézeteknél lehetne megfogni: az általuk vizsgált üzletek esetében csupán néhány banknál csoportosult az összes pénz, noha több különböző támadó volt.

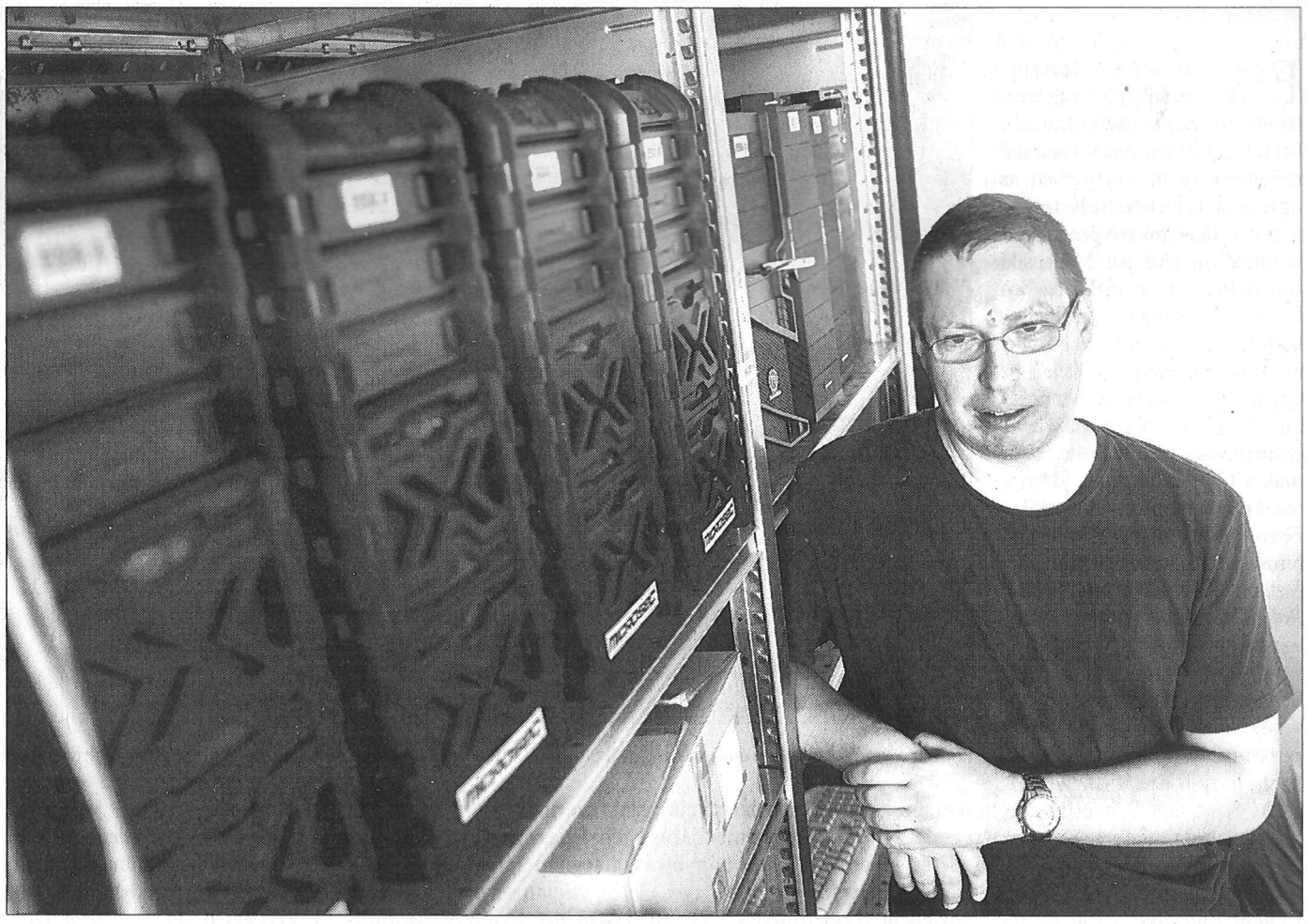
– A bankok tudtak erről?

– Hivatalosan, gondolom, azt mondanák, hogy nem tudtak róla, de ők is észrevehetnek furcsa dolgokat. Amíg azonban ez nem érdekük, addig nem biztos, hogy észre fogják venni. Az illegális gyógyszerüzletnél viszont nyilván komolyabbak a hitelkártyalopások. Más lopja el, más az, aki utángyártja, és egy harmadik ember használja fel, ezért is nehéz megfogni ezeket a támadásokat. Érdekes a money mule-ok, az úgynevezett pénzöszvérek szerepe, akik a hitelkártyán lévő, virtuális pénzt készpénzzé váltják. Ők jutalékért cserébe vállalják a lebukás esélyét is. Az FBI egyszer egy pénzlopásra használt kémszoftverhálózat ügyében képtelen volt előrelépni, kémprogramszakértők viszont rájöttek, hogy Ukrajnából mozgatják az egész szervezetet. A bűnözők több embert is alkalmaztak arra, hogy átutazzanak Amerikába számlát nyitni, és hogy az odaérkező, hitelkártyáról kicsalt pénzt felvegyék, majd hazarepüljenek vele Ukrajnába, mondjuk tízszázalékos jutalékért cserébe. Egy amerikai professzor csapatával azonban kiderítette, milyen elektronikus címek állnak az egész ügy mögött. Kizárólag interneten is rendelkezésre álló eszközökkel akadtak a nyomukra, egy seregnyit sikerült is azonosítaniuk, voltak a bűnözők közt olyan ostobák, akik a Facebook-oldalukra feltett fotókon pózoltak a rengeteg lopott pénzzel. Az információkat végül átadták az FBI-nak, a tettesek egy részét pedig még Amerikában sikerült letartóztatni.

– Milyen mértékben használja a szervezett bűnözés a számítógépes vírusokat és kémprogramokat?

– Egyes kutatások szerint a világ teljes GDP-jének akár fél–egy százalékát teheti ki a számítógépes bűnözésből származó kár. Többek szerint a kiberbűnözés ma már nagyobb üzlet, mint a drogpiac.

– Mennyiben érinti a kiberbűnözés Magyarországot?



Bencsáth Boldizsár: Ha egy bűnesethez használt szerver Brazíliában található, a támadó Oroszországban, az adatokat viszont Hollandiába vitték, az áldozatok pedig mondjuk angolok, akkor még az sem világos, melyik ország jogrendszere szerint kellene eljárni FOTÓ: BÉRES ATTILA

– Ugyanúgy benne vagyunk, mint minden más ország. A mi hitelkártyaadatainkat még talán ritkábban próbálják ellopni, mert kisebb piac vagyunk, önálló, bonyolult nyelvvel. Amikor viszont a nagy piacok már kiesnek, mert egyre több kiberbűnöző lesz, akkor a magyar hitelkártyák is elég értékessé válhatnak majd ahhoz, hogy tőlünk is megpróbálják ellopni az adatokat. Viszonylag jó helyzetben vagyunk, a törvényeink ugyanis – elméletileg – védelmet jelentenek a támadók ellen, tehát itthon legalább a jogi környezet adott a fellépésre. Ami van a világban, az viszont mindenképpen beszivárog hozzánk is, statisztikák szerint ráadásul a gépeink nem is állnak jól fertőzöttség szempontjából. Ha nem is tőlünk lopnak, attól még ugyanúgy probléma, ha bűnözők itt futtatnak különböző szervereket vagy feltört weboldalakat, amivel egy másik ország polgárait támadják meg. Ezért is felelősek vagyunk, ugyanúgy fel kell lépni ellene.

– A Stuxnet nevű kártevő jelentős változást hozott 2010-ben: képes volt számítógépes vírusként a valós, fizikai világban is jelentős kárt tenni egy iráni dúsítóban található uráncentrifugák tönkretételével. Hogyan lehet ezek ellen védekezni?

– A hatásos védelmet nagyon nehéz definiálni. Amikor a Stuxnet tönkretette a centrifugákat, volt, aki felvetette, hogy akár fel is robbanthatott volna egy erőművet. Ez azonban nem ilyen egyszerű, egy erőműben nagyon sokféle védelmi eszköz van, egy részük nem is a számítógépen múlik. Annak az esélye, hogy pusztán egy kóddal felrobbantsanak egy ilyen létesítményt, nagyjából nulla, de vélhetően sajnos súlyos károkat okozhatnak sok ipari rendszerben. Hagyományosan az összes ilyen ipari rendszer le volt választva az internetről, ez pedig védettséget adott. Nem fejlesztették viszont a belső biztonságot, és most ebből lett a gond. Idővel egyre nagyobb arányban kötötték rá ezeket a rendszereket az internetre vagy valamilyen más hálózatra, így pedig elérhető célponttá váltak.

– Elmondhatjuk, hogy fokozódik a kiberhadviselés?

– Az biztos, hogy megnövekedett a számítógéppel elkövetett támadások mennyisége, komolysága és súlya is az elmúlt években. A hadviselés szóval viszont gondok vannak; nehogy túl korán mondjuk azt, hogy kiberháború van, és amikor tényleg katasztrofális, emberéleteket követelő esemény lesz, nem lesz rá szavunk.

– Miként befolyásolhatja mindez az államközi kapcsolatokat?

– Bizalmatlanságot szül, pedig az országoknak együtt kell működniük a kibertámadások terén, ez viszont bizalomra épül. A Snowden-ügy, a támadások, a folyamatosan felmerülő kémügyek és kémprogramok miatt ugyanakkor egyértelműen bizalmi válság van. Megjegyzem, hogy kémek mindig is voltak a hagyományos világban is, így egyáltalán nem meglepő, ha a kibervilágban is történik ilyesmi. Újdonság viszont a mértéke, hogy milyen módon és kik ellen csinálják, hogy barátok és szövetségesek kémkednek egymás ellen.

– Lát kiutat a bizalmi válságból?

– Természetesen vannak biztató folyamatok. Sok ország dolgozik a téma büntetőjogba történő beemelésén, különböző szervezeteket alakítanak, katonai szövetségek, például a NATO foglalkozik a témával, szabályzatok, eljárásrendek, ajánlások, megegyezések születnek. Alulról is dolgoznak: a kutatók kutatnak, a biztonsági cégek megpróbálnak egyre jobban együttműködni, bővítik az információmegosztást, a nyilvánossá váló eredmények pedig segítik a helyzet megértését. A problémát viszont nem oldjuk meg egyik napról a másikra. Kicsit még vadnyugati a helyzet a kémprogramok és kibertámadások kapcsán. Egy nagyon evidens kérdés: vissza lehet-e támadni egy külső ország támadóit, hogy megtudjuk pontosan, mit akarnak? A magyar törvények szerint a civil szférában egyértelműen nem, viszont Amerikában vannak cégek, amelyek ezt szolgáltatásként árulják. Grúz hackereket például visszatámadtak, és a saját webkamerás felvételeikkel leplezték le őket, a róluk készült képeket még az internetre is kirakták. Ez erősen jogsértőnek tűnik, de nincs kialakult, kifinomult jogrendszer, nincs kialakult kultúra. Vadnyugatiság van, ahol az erősebbnek van igaza. Idővel viszont az igazi vadnyugaton is létrejött egy társadalom, ahol már nem lövöldöznek egymásra az emberek következmények nélkül.

– Az említett Stuxnet hátterének felderítése is nemzetközi együttműködést igényelt.

– A támadások fontosságának felfedezése sem triviális. A Stuxnet esetében sem rögtön értette meg a világ, hogy a támadásnak milyen nagy a jelentősége. Először egy belorusz cég talált valamit, ami Iránban gondot okozott, és csak hónapok múlva jöttek rá arra, hogy ez milyen komoly, országok közötti konfliktusban felhasznált támadás. Sok-sok apróságból, részletből kellett összerakni a mozaikot, és ez máskor is előfordulhat.

– Mennyire technikai kérdés a hatékony védekezés?

– Egy kémprogram vizsgálatának nem csak technikai vonulatai vannak. Volt, hogy a támadásban történt változást valamilyen politikai eseményhez lehetett kötni. Képben kell lenni a világpolitikával, de akár a helyi szintűvel is. Ha a feltételezés szerint mondjuk Ukrajnában erősödött egy támadás, akkor meg kell nézni, mi történt abban az időben ott és a szomszédos államokban. Kell hozzá földrajzi, technikai tudás, társadalom- és nyelvismeret, hiszen a kódban lehet egy szó vagy kifejezés, amely elárulhatja a készítőket – és amely persze ugyanúgy belekerülhet átverésből is. Nem egy szűk technikai terület ez, hanem az életünk része.

– Tudna példát mondani politikai eseményre, amely érezhetően befolyással volt a kibervilágbeli támadásokra?

– Például az iráni helyzet, az orosz–grúz konfliktus, az ukrán helyzet, Szíria, Gáza: szinte minden komolyabb konfliktusnak van már ilyen vetülete. A kutatók azonban nagyon vigyáznak az olyan következtetésekkel, hogy egy bizonyos ország volt a támadó. Ezek ugyanis nagyon törékenyek, nehéz biztosat, megalapozottat mondani. Egy legutóbbi támadás esetében – Uroburos néven is említik – szinte mindenki egyetért, hogy orosz nyelvű támadóról lehet szó, és a támadások erősödése összefüggésbe hozható az ukrán helyzettel. Ugyanakkor ezek az orosz nyelvű támadók akár Hawaiin is lehetnek, ki tudja, milyen háttérrel, és az ukrajnai helyzetet is kihasználhatják a tevékenységük leplezésére. Nagyon nehéz biztosat mondani, de nyilván ez nem is feltétlenül a civilek dolga. 2012 májusában lelepleződött egy kémprogram Flame néven, amelynek sok célpontja volt Iránban, Szudánban, de a palesztin területeken is. Vajon csupán véletlen, hogy ugyanazon az őszön Izrael támadásokat intézett a palesztin területek ellen, vagy elképzelhető, hogy a támadások tervezése és kivitelezése során felhasználtak olyan információkat, amelyeket ezzel a kémprogrammal gyűjtöttek, különösen egyes hadifelszerelésekről, amelyek a fenti három területet érinthetik? Ez azonban csak találgatás és sejtés, nem tudhatjuk biztosan, hogy ki kémkedett a Flame-mel. Ki kell emelni, hogy ma ezek a számítógépes támadások már a mindennapjaink és a legfelsőbb politika részei, nem távoli mendemondák.

– Átvehetik valaha a kibertámadások az igazi katonai támadások helyét?

– Részben már át is vették. Tudjuk, hogy folyamatosan kibercsapások zajlanak, de nem tudjuk, mikor nem indítottak azért bombázókat, mert más módon oldották meg a kérdést. Ez nem feltétlenül azt jelenti, hogy kibereszközzel romboltak le valamit, hanem esetleg az eszközzel olyan információhoz jutottak, hogy más módszerrel, nyílt katonai erő felhasználása helyett például valakinek a letartóztatásával, vagy hatóságok együttműködésével meg lehetett oldani a problémát. Rengeteg eset van, amikor nem tudjuk, mi megy a háttérben.