Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2010. III. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2010. évi III. negyedéves jelentését, mely 2010. legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a VirusBuster Kft. összefoglalóját 2010. aktuális IT biztonsági trendjeiről. A hangsúly most is az aktuális informatikai biztonsági trendeken van.

Többek között olvashatnak azokról a hitelesítési eljárásokról, amelyek fejlesztésével érezhetően visszaszorítható lenne a cyber-bűnözés és a napjaink internethasználatát megnehezítő hálózatbiztonsági támadásokról. Megemlítjük azokat a potenciális veszélyforrásokat, amelyek felismerésével és feltérképezésével csökkenthetjük a támadók fizikai célpontjait. Szó esik még a nemzeti és országhatárokon átívelő összefogásról, valamint a gyors reagálás fontosságáról és az ezt erősítő országos és nemzetközi gyakorlatokról.

A Nemzeti Hálózatbiztonsági Központ igyekszik minél több szinten informálni szakmai közönségét: amellett, hogy idén elindította az IT biztonsági szakoldalát a Tech.cert-hungary.hu-t, külön hírfórumot működtet TECH-blog elnevezéssel, amely naponta többször frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven. A TECH-blog RRS feed-en keresztül is elérhető a következő címen: http://tech.cert-hungary.hu/rss.xml.

A TECH-blog-on kívül a sérülékenységi publikációk is elérhetőek RSS csatornán keresztül melynek címe: http://tech.cert-hungary.hu/vulnerabilities/rss.xml

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

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

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

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

Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
testületi elnök

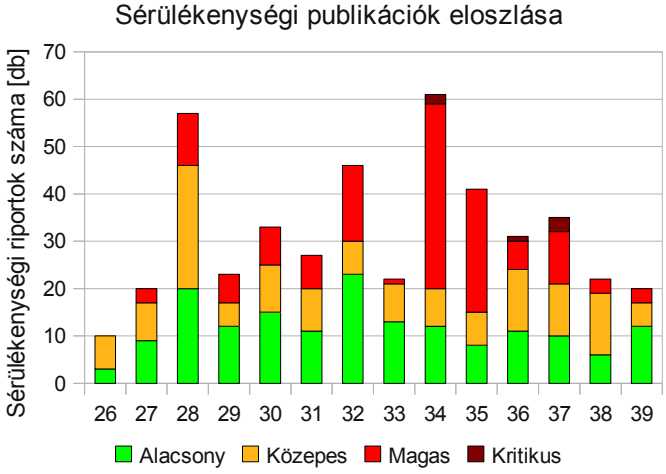
Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

Szoftver sérülékenységek

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

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ** a 2010. III. negyedéve során 448 **db szoftver-sérülékenységi információt** publikált, amelyekből 165 db alacsony, 137 db közepes, 140 db magas és 6 db kritikus kockázati besorolású.

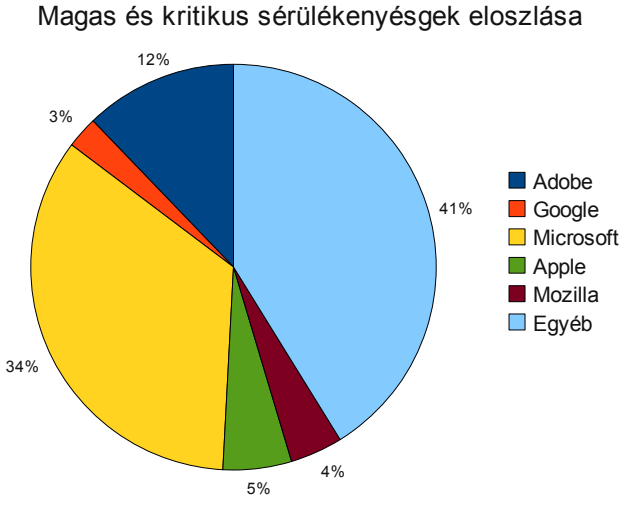


A sérülékenységi információk eloszlása, a 28., 32. és 34. heteken kimagasló értékeket mutat. Ennek oka a 32. héten a Microsoft patch Tuesday, a 28. héten a Oracle, SUN és HP termékek, valamint a 34. héten Microsoft és Adobe termékek kapcsán kiadott sérülékenységi publikációk magas száma.

A negyedév a kritikus sérülékenységek terén eléggé egyoldalú képet mutatott, a hat kritikus esetből öt (83%) az Adobe valamely széles körbe használt termékét (Reader, Flash, Shockwave) érintette, míg a hatodik a Google böngészőjét a Chrome-ot érintette.

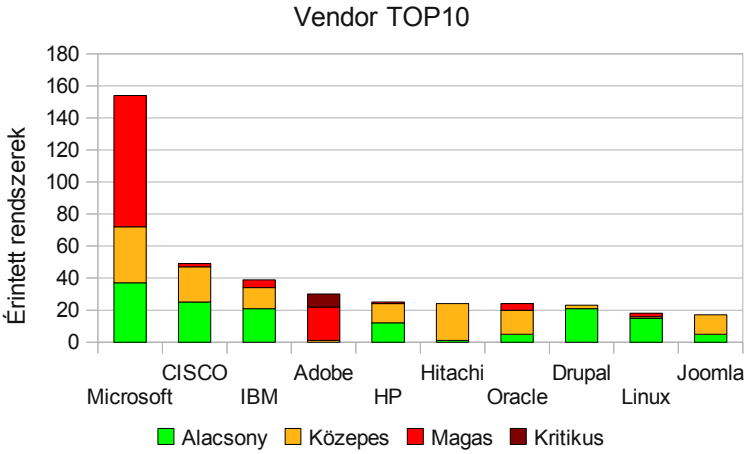
- Adobe Acrobat és Reader sérülékenység - CH-3506
- Adobe Shockwave Player többszörös sérülékenység - CH-3527
- Adobe Reader és Acrobat betűkészlet elemzés puffer túlcsordulás sérülékenysége - CH-3626
- Adobe Flash Player ismeretlen kód futtatási sérülékenység - CH-3641
- Google Chrome Flash Plugin ismeretlen kód futtatási sérülékenység - CH-3642
- Adobe Reader/Acrobat Flash Player ismeretlen kód futtatási sérülékenység - CH-3643

A súlyos sérülékenységekkel együtt vizsgálva a halmazt az előző negyedévhez hasonlóan a Microsoft termékei vezetnek (34%), a további helyeken viszont átrendeződés figyelhető meg a specifikusabb szoftvertermékek felől az általánosan használt területek irányába. Ez ha lehet még nagyobb kockázatot jelent, hiszen nem üzleti szféra specifikus szoftverek hordozzák a kiemelkedő sérülékenységeket – ahol van is kapacitás és szakértelem az esetleges problémák elhárítására – hanem az összes szektort érintik ezek a hiányosságok. A második helyen az Adobe (12%), majd az Apple (5%), a Mozilla (4%) és a Google (3%) állnak.



Ez a 4 nagy gyártó az összes súlyos és kritikus hiba közel 25%-áért felelős. Az előző negyedhez képest jóval diverzifikáltabb a terület, hiszen ott az első három helyezett közel 60%-os lefedettséget jelentett. A sebezhetőségek száma és a szoftverek elterjedtsége között továbbra is szignifikáns összefüggés mutatható ki.

A Microsoft esetében különösen nagy veszélyt rejt magában, hogy a legszélesebb körben használt asztali operációs rendszerek és az Office termékcsalád a leginkább érintettek. A Microsoft termékek frissítéseinek alkalmazására érdemes odafigyelni, hiszen ezen termékek érintettek a legnagyobb számban a Központunk által kiadott sérülékenységi publikációkban is, mint ahogy az a jobboldali grafikonon is jól látszik.



A többi kiemelt gyártó pedig főleg az internethasználathoz és/vagy böngészéshez köthető termékei a kockázathordozók. A Google, a Mozilla és az Apple esetében is érintettek a böngészők; az Apple esetében az operációs rendszerek (iOS, MacOS) valamint az Apple hardverek és a PC együttműködését biztosító iTunes volt jelentősebben érintett; az Adobe esetében, pedig különösen nagy kockázatot jelent, hogy a szinte minden böngészőbe beépülő (Flash, Shockwave), illetve a minden PC-n megtalálható dokumentumolvasó (Reader) alkalmazásokat érintették a legsúlyosabb hibák.

Ez azt jelenti, hogy ezen széles körben elterjedt szoftverek sérülékenységeinek kihasználása az egész nemzetgazdaság szintjén súlyos és nehezen elhárítható problémákat eredményezhet.

IT-biztonság a vállalati szektorban

Az eszközök szintjén némi fejlődés, de a szemléletben továbbra is súlyos lemaradás foglalja össze a BellResearch[1] a hazai vállalatok többségének IT-biztonsági gyakorlatát. A vállalatokra is jellemző, hogy gyakran az arányos, átgondolt védelem helyett csak annak illúzióját keltő, egyes részterületeket lefedő eszközöket használják fel, miközben a valódi biztonságot nyújtó, egész szervezetet átható stratégiai szemlélet meglehetősen ritka. Az eddigi trendek alapján a közeljövőben aligha lehet jelentős fejlődésre számítani, ahhoz ugyanis szemléletváltásra lenne szükség.

Az utóbbi évek során, ahogy a vállalatok mind több kritikus üzleti folyamat támogatására alkalmaznak különböző informatikai megoldásokat, mind nagyobb adatvagyonnal gazdálkodnak, a rendszerekkel szembeni kitettségük is fokozódott. Így még abban az esetben is nagyobb kockázattal néznének szembe, ha mindeközben az IT-biztonsági fenyegetések nem nőttek volna.

A mobilitás iránti igény erősödése és a hordozható eszközök terjedése szintén növeli a kockázatokat. A notebookok, amelyek a tolvajok kedvelt célpontjának számítanak, a vállalati pc-állomány mind nagyobb hányadát adják. Megfelelő óvintézkedések nélkül egy ingzsebben elférő pendrive-on vagy egy mobiltelefon memóriájában ma több adatot lehet szinte észrevétlenül kicsempészni a vállalattól, mint amennyit egy évtizeddel ezelőtt egy közepes méretű cég fájlszerverein összesen tároltak.

Az informatikai biztonság kérdése messze túlmutat a sebezhetőséget csökkentő szoftver- és hardverkomponenseken, több azoknál. Stratégiai szemléletben előkészített terven alapuló döntések

1 Bellresearch: Magyar Infokommunikációs Jelentés 2009., http://www.ictreport.hu/

sorozata, rendszeresen felülvizsgált és következetesen betartatott szabályok összessége, amelyek megvalósítási eszközei között találunk hardver- és szoftvereszközöket is.

A BellResearch kutatási eredményei szerint a legalább 10 főt foglalkoztató vállalkozások többsége (56 százalék) nemcsak hogy alkalmaz valamilyen üzleti célszoftvert, de ezeket valamely üzletileg kritikus folyamatának támogatására (is) használja, és az e téren érintett vállalkozások aránya a közepes és nagyvállalatok körében még magasabb.

Bár az IT-biztonsággal foglalkozó cégek portfóliójában megtalálható a megoldások széles palettája, ezek az eszközök is csak megfelelő alkalmazás mellett lehetnek valóban hatásosak. Ennek előfeltétele a mind felkészültségében, mind számosságában megfelelő IT-biztonsági csapat rendelkezésre állása. A szükséges humánerőforrást a vállalatok jellemzően teljes egészében házon belül allokálják. A BellResearch kutatási adatai alapján a cégek 60 százaléka egyáltalán nem vesz igénybe külső specialistát, és az ilyen partner alkalmazása a nagyvállalati szegmensben az átlagosnál is ritkább.

A Jelentés legfrissebb adatai szerint a hazai cégek IT-biztonsági aktivitásai jellemzően az eszközszintű védelmi megoldásokban merülnek ki. Antivírus-szoftvert és valamilyen tűzfalat a vállalatok nagy többsége alkalmaz, sőt ma már a spamszűrés is elterjedtnek tekinthető. A számok azonban viszonylagosak. E téren a 95 százalékos penetráció is alacsonynak számítana.

Ráadásul a legjobb szoftverek sem érnek sokat, ha konfigurálásuk, rendszeres frissítésük nincs megfelelően megoldva. Azt is figyelembe kell venni, hogy az egyes vállalati szegmensek között jelentős szakadék húzódik. Míg levélszemét-szűrést a nagyvállalatok 91 százaléka alkalmaz, addig a mikrocégek mindössze kétötöde, és számos más IT-biztonsági megoldás esetében az olló még szélesebbre nyílik.

IT-biztonsági beruházások

A vállalatok informatikai függősége az elmúlt évek során egyre erősebbé vált. Megfelelő informatikai rendszerek nélkül már kisvállalati szinten sem képzelhető el tartósan sikeres működés. A biztonsági kockázatok növekedésével a sokáig alkalmazott kényelmes felhasználó szemlélet viszont át kell, hogy alakuljon a tudatos menedzsment irányába. Ez minden gazdasági szereplőre vonatkozik, hiszen az internet elterjedésével, a felelősség egyre inkább kollektívvé válik. Ha valaki nem figyel oda, nem csak magát, de a partnereit és az egész szektort is veszélybe sodorhatja. (Lásd például a NHBK – PTA CERT-Hungary 2010. I. negyedéves jelentésének botnetekkel foglalkozó írásait.)

Ebben a környezetben a jelenlegi tendencia az, hogy a világ informatikai beruházásokra fordított összegeinek egyre nagyobb szeletét rabolja el az informatikai biztonság. Ez a Gartner Group előrejelzése szerint a következő években elérheti a 10-12%-ot, szemben a korábbi 4-5 százalékkal.

A Gartner felmérései[2] szerint a következő egy év során a vállalatok teljes informatikai

2 Gartner Group: Gartner Says Efficient and Secure Enterprises Will Safely Reduce the Share of Security in their IT

költségvetésüknek átlagosan mintegy 5 százalékát fogják információbiztonsági technológiákra költeni. Ez valamivel kevesebb, mint a tavalyi 6 százalék, viszont az informatikai összköltségvetések közel 2 százalékkal emelkednek, így a biztonsági szakemberek nagyjából pénzüknél maradnak. A felmérések szerint a vállalati szektor 40%-a allokál a megelőző időszakhoz képest több forrást a biztonsági megfontolásokra.

A Gartner adatai[3] szerint egy átlagos (amerikai) vállalat alkalmazottanként 525 dollárt költ információbiztonságra. Ugyanakkor az egyes iparágak között nagy eltérés van. A biztosítóknál ez az összeg 886 dollár, a kormányzatnál 671 dollár, a pénzügyi szolgáltatóknál pedig 637 dollár.

Nem biztos azonban, hogy ezeket a pénzeket okosan költik el. Egy másik felmérésben a Forrester Research arra az eredményre jutott[4], hogy a pénzek aránytalanul nagy hányadát fordítják az ügyfelek személyes adatainak és a bankkártya-adatoknak a védelmére. Miközben az ilyen információk – amelyeknek a cég csak őrzője – a vállalati információvagyon alig több mint egyharmadát teszik ki, a biztonsági költségvetés fele ezek védelmére megy el. A cégek csak a költségvetés másik felét fordítják a céges adatvagyon kétharmadát adó vállalati titkok (stratégiai tervek, értékesítési előrejelzések, pénzügyi eredmények) védelmére.

Általában elmondható, hogy a cégek csak valamilyen káresemény (adatvesztés, vírustámadás, a levelezőrendszer leállása, információk kikerülése, hacker-támadás) **után kezdenek el foglalkozni a biztonsági kérdésekkel.** Ez - bár jellemzően emberi viselkedés - semmiképpen nem nevezhető preventívnek, ami pedig ma minden cégnek és szervezetnek alapvető érdeke lenne.

A cégek többségének - talán csak a legnagyobbakat kivéve - általában nincs olyan informatikai stratégiája, ami meghatározná, hogy az informatika milyen módon szolgálja ki a tervezett üzleti célokat, folyamatokat. **Gyakran előfordul, hogy a felső vezetésben egyáltalán nem tudatosul, hogy az informatikát milyen módon tudnák a legjobban használni.**

Komoly hiányosság, hogy a cégek többségénél nincsenek tisztában **a céget fenyegető kockázatok** és az üzleti folyamatok fenntarthatósága közötti összefüggésekkel, illetve ennek kapcsán azzal, hogy **az informatikai rendszerek hibái** milyen óriási **közvetlen károkat okozhatnak.** Az elvégzett kockázatelemzések eredményei az esetek többségében hatalmas meglepetést okoznak a felső vezetésnek.

Még a legnagyobb cégekre is jellemző, hogy hamis illúziókat táplálnak, különösen akkor, ha a cégnél már történtek lépések az informatikai biztonság megteremtésére. Az ilyen rendszerek számtalan esetben sok helyen lyukasak. A hamis biztonságérzet ezeknél a cégeknél is azt eredményezi, hogy valamilyen káreseménynek kell bekövetkeznie ahhoz, hogy a szükséges lépésekre rászánják magukat.

A legproblémásabb területek: a jogosultságok és jelszavak feladatorientált, hierarchikus kezelése, a vezetők bizalmatlansága az üzemeltetőkkel szemben, a jelszavak könnyű visszafejthetősége illetve nyílt kezelése, a felhasználóknak indokolatlan jogok biztosítása, a tűzfalak, routerek nem megfelelő beállításai, a mentések laza és szabályozatlan kezelése, a megfelelő informatikai szabályozások és fegyelem hiánya.

Az első számú prioritás az informatikai vezetők szerint a felhasználói identitáskezelés (identity management) volt: 20 százalékuk számára volt ez az elsődleges beruházási célpont.

Budgets by 3 to 6 Percent of Overall IT Budgets Through 2011, 2010.06.10. http://www.gartner.com/it/page.jsp?id=1384214

3 Gartner Group: Gartner Says Security Software Market is Poised for 11 Percent Growth in 2010; 2010.08.16., http://www.gartner.com/it/page.jsp?id=1422314

4 IT-business: Mostohagyerek a biztonság, 2010.06.11. http://www.itbusiness.hu/hirek/legfrissebb/gartner_security.html

Összefoglalóan a legnagyobb gondot az okozza, hogy a felmerülő problémákat a legtöbb helyen nem átfogóan, rendszerben gondolkodva közelítik meg, hanem **csak egyes részterületeken próbálnak meg eredményeket elérni –** leggyakrabban a „gyorsan valamit vegyünk minél olcsóbban" szűklátókörű és rövidtávú gondolkodás mentén **– és ezek megvalósítására sokszor még mindig elegendőnek tartják az eszközök megvásárlását.** A rendszerben gondolkodás egyik összetevője az is, hogy a **cég üzleti stratégiájába az informatikának és az informatikai biztonságnak szervesen bele kell illeszkednie.** Azonban ezek a stratégiai kérdések ma még nem kapták meg a jelentőségükhöz méltó helyet.

Másrészt még mindig komoly hiányosságokkal küzd az a két terület, amelyik pedig a legnagyobb eredményt hozhatná. Ezek az emberi tevékenységek szabályozása és az oktatás. A statisztikák és az eddigi tapasztalataink is azt mutatják, hogy **a biztonsági problémák túlnyomó része (legalább 70-80 százaléka) a nem megfelelően szabályozott emberei tevékenységekre és a szükséges ismeretek hiányára vezethető vissza.**

Paradigmaváltás

Az IFUA Horváth & Partners és a Budapesti Corvinus Egyetem közös IT benchmarking kutatása[5] alapján a biztonság emelése azonban várhatóan 2011 során sem fog elsődleges prioritást élvezni az informatikai beruházások piacán. Amikor a különböző informatikai projektek fontosságáról kérdezték a vezetőket, a biztonság csak a kilencedik helyen tudott megkapaszkodni, és olyan, manapság divatosnak számító technológiák előzték meg, mint a virtualizáció, a számítási felhő vagy a mobil technológia.

Míg az előző kutatási forduló (2007/2008) eredményei alapján a szervezetek és intézmények többsége a belső informatikai célok elérésére koncentrált, ma már a válaszadók egyharmada kifelé tekint, és az ügyfélkapcsolat-kezelési (CRM), valamint a velük összefüggő e-megoldások fejlesztésére fókuszál. Viszonylag sokan tartják még fontosnak az üzleti intelligencia-megoldásokat is (a CRM segítségével begyűjtött adatok elemzése a fókuszpont), illetve a folyamatirányító (workflow) rendszereket.

Eközben az informatikai vezetők korábbi 53 %-a helyett csak 16 százalék tartja fontosnak az IT-biztonságot, és több más, néhány éve még lényegesnek tartott terület (mint például a vállalatirányítási rendszerek, a szerverkonszolidáció, a belső vállalati portál vagy éppen a szolgáltatási szintek kérdése) a háttérbe szorult. A változás jelentős, de korántsem meglepő, mert teljes mértékben összhangban van a nemzetközi trendekkel. Ezek szintén az értékesítést szolgáló technológiák előtérbe kerülését mutatják, párhuzamosan az informatikai költségek visszaszorításával és az IT-hatékonyság növelésével. **Az elemzési szoftverek azért is kerülhettek most az előtérbe, mert megfelelnek a válság idején az informatikai beruházásokkal szemben támasztott talán legfontosabb követelménynek, a gyors megtérülésnek.**

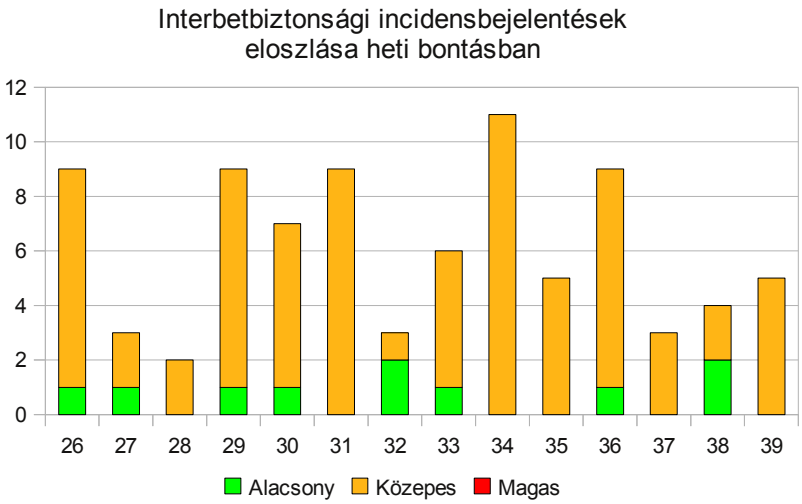
5 Schopp Attila: Biztonság helyett inkább az ügyfél, 2010. 09. 13., http://www.itbusiness.hu/hirek/legfrissebb/ifua_crm.html

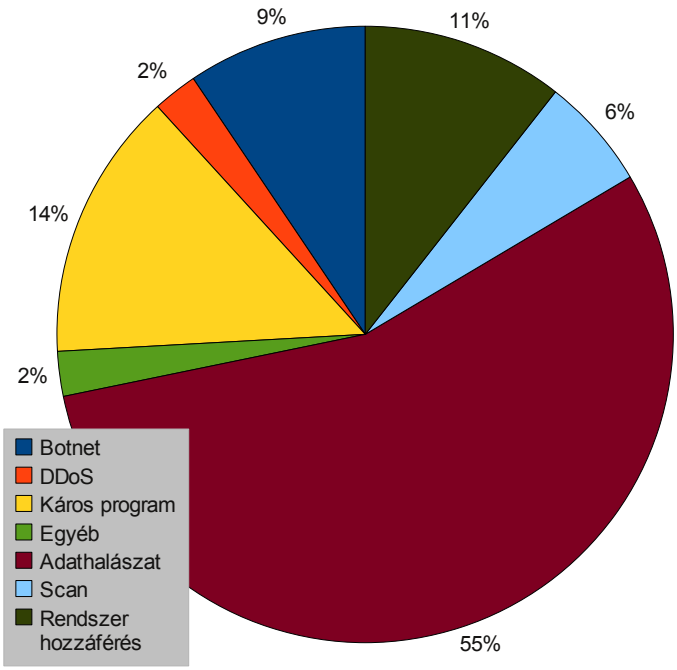
Internetbiztonsági incidensek

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

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2010. év harmadik negyedéve során összesen **85 db incidens bejelentést** regisztrált és kezelt, ebből 10 db alacsony és 75 db közepes kockázati besorolású.

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





2010 III. negyedévében a legnagyobb számban adathalász tevékenység (55%), káros szoftverek terjesztése (14%) kapcsán érkeztek bejelentések, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket. Számottevőek voltak még a rendszer hozzáférési kísérletek kapcsán beérkezett bejelentések, melyek mindösszesen 11%-át teszik ki az összes bejelentésnek.

A bejelentések több mint 90%-a hazai forrású káros tevékenységgel vagy tartalommal állt összefüggésben, és túlnyomó részt külföldi partner-szervezetektől érkezett. Az egyes incidensek elhárítása kapcsán összesen 25 hazai és 2 külföldi szolgáltató került bevonásra.

Az internet otthon

Az adat-információ biztonságnak nem a műszaki-technikai feltételek, hanem a műszaki-technikai eszközöket üzemeltető, a dokumentumokat, adatokat, információkat kezelő személyzet, az ember a legnagyobb kockázata. A mai munkavégzés, szervezés, irányítás, végrehajtás és ellenőrzés jelentős része elektronikusan zajlik, számítógépeken illetve távközlő, számítógépes hálózatokon.

Felnőttek

A Symantec 13 országra kiterjedő nemzetközi felmérése[6] szerint a felnőttek nagy része (99 % a nemzetközi átlag, 98,5 % a magyar) véli úgy: tett lépéseket a személyes információinak megvédése érdekében. 84%-uk pedig úgy nyilatkozott, hogy tisztában van a biztonságos online jelenlét szabályaival. Ugyanakkor a nem biztonságos böngészés, a felelőtlenség mindennapos, a feltört számítógépek száma pedig riasztóan magas. Az internetező felnőttek fele szándékosan keres fel nem megbízható webhelyeket, nem készít mentést adatairól, és nem használ biztonságos jelszavakat. Egyharmaduk jelezte, hogy valaki már betört a számítógépébe.

Annak ellenére, hogy a felnőttek 99 százaléka úgy véli, hogy tett lépéseket a biztonsága érdekében, az idei beszámolóból az derül ki, hogy sok fogyasztó nincs teljesen védve az internetes flörtölés vagy barátkozás közben. Bár az átlagos fogyasztó tudatában van az internetes biztonság fontosságának, sokan csak ritkán használnak víruskeresőt, vagy nincs kellő védelmük a mai veszélyek ellen. Az internetező felnőttek közel fele már megtapasztalta a merevlemez tönkremenetelével járó problémákat, és egyharmaduk már vesztett el értékes zenét, fényképet, videót vagy pénzügyi dokumentumokat. Még aggasztóbb, hogy 10 közül két felnőtt egyáltalán nem használ védelmi szoftvert.

Magyarországon a felnőttek 74,5 százaléka telepített védelmi szoftvert, ugyanakkor tízből két felnőtt még mindig kiadja a neten a bizalmas adatait, mint például a bankkártyája számát vagy a személyi igazolványa számát.

A megkérdezett magyar felnőttek 56,6 százaléka nem használ bonyolult jelszót, 41 százalék pedig bevallottan nem csak megbízható internetes oldalakat keres fel. **A magyarok 85,6 százaléka nem jelzi a gyanús e-maileket vagy internetes tevékenységeket.**

Gyerekek

A gyerekek sokkal inkább igénybe veszik az informatika nyújtotta lehetőségeket, különösen az online kapcsolattartás területén, globálisan egy gyerek átlagosan havi 39 órát tölt online, míg ez a szám szüleik esetében bő fele: 21 óra. Egyre fontosabb területe az informatikai biztonságnak a gyerekek védelme.

Minden ötödik gyerek ismerte be, hogy olyan dolgokat néz, vagy olyasmit tesz az interneten, amit a szülei nem néznének el neki. A megkérdezett gyerekek húsz százalékát rajta is csípték, hogy olyasmit nézeget a neten, amit nem lenne neki szabad.

A nemzetközi átlag kétszerese, a 7-17 éves magyar gyerekeknek 42 százaléka válaszolta, nem igaz az az állítás, hogy a szülei mindig tudnák, mit nézeget, ha internetezik. Ráadásul a magyar gyerekeknek csak harmada használ bonyolult jelszót, százból nyolc vált gyakran jelszót, 87 százalék nem jelez, ha gyanús e-maileket vagy internetes tevékenységeket tapasztalt, 26 százalék pedig gond nélkül kiadja a személyes adatait idegeneknek.

Bár majdnem minden szülő azt mondja, hogy ők felelősek gyermekük online biztonságáért, sokan szívesen megosztják ezt a felelősséget.

6 Symantec: Norton online living report 2009, 2010.10.02. http://www.nortononlineliving.com/

A cyber-bűnözés növekszik, de a hitelesítés fejlesztésével ez legyőzhető

A cyber-bűnözés a mai modern élet velejárója, egyre kifinomultabbá válik, amire már felfigyelt a média, különböző politikusok, sőt még az állampolgárok is. Egyelőre itt tartunk, de az biztos, hogy a jövő háborúja kiterjed a cyber hadviselésre is, így az amerikai kormány már sürgeti a számítógépekkel kapcsolatos védelmi képességek kifejlesztését.

Ennek az új keletű tevékenységnek a hatásait már megtapasztalhattuk 2010. elején, például az Aurora[7] nevű sérülékenységet kihasználó kód esetén, ami a Google-t és másokat is célba vett. Az otthoni felhasználók kezdik megtapasztalni a cyber-bűnözés velejáró hatásait az alapvető üzleti tevékenységek folyamán, különös tekintettel a pénzügyi szektorra, de gyakran előfordul máshol is.

A cyber-bűnözési mutató folyamatos emelkedéséhez vezetett az utóbbi öt évben a szervezett bűnözői csoportok által a viszonylag gyorsan alkalmazott technika. A cyber-bűnözés többé már nem a szülői ház pincéjében „dolgozó" a fiataloktól indul ki – ez most már egy üzletág, törvényekhez alakítva, amely gazdag és érdekeltségekkel rendelkező szervezeteken alapul, amely megszerzi a világ legtehetségesebb számítógépes szakembereit is.

A cyber-bűnözés nagyjából két kategóriába sorolható be: a célzott támadásokra és a tömeges támadásokra. A célzott cyber-bűnözésről semmi új nem mondható el, habár gyakran hasonlatos a tömeges támadásokhoz, amik az utóbbi években emelkedő tendenciát mutatnak. A célzott támadás alatt az értendő, amikor a bűnözők célpontja egy egyén vagy cég, és a támadók gyakran speciális ismeretekkel rendelkeznek a kiszemelt áldozatról. Legújabban a belülről induló (bennfentes) támadások tartoznak az utóbbi kategóriához.

Ezek a támadások kapcsolatban állnak a tömeges bűnözés kirobbanásával is. Ehhez például olyan eszközöket használnak fel, mint a Zeus káros szoftver program, így például a bűnözők képesek egyszerre óriási számosságú támadást elindítani a célpontok ellen, akik általában előzetesen sem ismerik a támadókat. A Zeus még három évvel a kezdeti azonosítása után is aktív maradt, a becslések szerint 2010. júliusában 3,6 millió számítógépet tartott ellenőrzése alatt kizárólag csak Amerikában.

A tömeges támadások olyan gondokat okoztak 2009. végére, hogy az FBI az Amerikai Bank Szövetséggel együtt kidolgozott egy kézikönyvet az összes online bankolást használó cég részére, melyben azt javasolta, hogy az online bankoláshoz kizárólag hitelesített (dedikált) számítógépet használjon, és semmi mást. Ezzel próbálták megakadályozni az ilyen típusú káros szoftverekkel való megfertőződést. Ugyan ez a javaslat csökkenthette a fertőzöttség mértékét, de ez, a probléma nagyságának hallgatólagos beismerését is jelentette, valamint azt, hogy nincs gyors és hatékony megoldás.

Különböző szoftver sérülékenységek elleni védelmi eljárások kerültek kidolgozásra az évek folyamán, ilyenek például a tűzfalak, az IDS rendszerek és a káros szoftverek elleni alkalmazások. Ezek a védelmi módszerek egy ideig valóban hatékonyan csökkentették a szoftver sérülékenység kihasználását, de ahogyan fejlődtek ezek a védelmi eljárások, a támadók úgy egyszerűen egy másik nézőpontot vagy hozzáállást kerestek. Emelkedést mutatnak a felhasználói hitelesítési eljárások ellen irányuló támadások is.

7 2010 elején egy Microsoft Internet Explorer sérülékenységet kihasználó exploit megnevezése

Több tényezős hitelesítés

Mivel bonyolultabbá vált a szoftver hibák kihasználása, a támadók egy könnyebb célpontot kerestek: ezek a hitelesítő rendszerek. Az ilyen típusú támadások több évre visszavezethetőek, amelyek a korai billentyűzet leütések naplózásával megszerzett jelszavakkal kezdődtek, majd az e-mail alapú phishing támadásokkal folytatódtak, amelyek már a támadók számára ezerszám biztosította a megszerzett tanúsítványokat. A hitelesítés ellen irányuló támadások egyre kifinomultabbak lettek az évek folyamán, a napjainkban jelentett súlyos, tömeges támadások alapját képezik.

Amikor problémák vannak a hitelesítéssel, akkor erre az a természetes reakció az, hogy erős hitelesítési megoldásokat fejlesztenek ki, mint ahogyan az elmúlt évek folyamán az ilyen rendszerek széleskörű fejlődésén lehetett tapasztalni. Az erős hitelesítési rendszer egzakt fogalmának pontos meghatározása az adott helyzettől függően változhat. Néhány területen az erős hitelesítés egyszerűen azt jelenti, hogy válaszokat kérnek a biztonsági kérdésekre (például „Mi a kedvenc színe?"). Más összefüggésben, más területeken ide tartozik a biometrikus hitelesítés, hely meghatározás, az idő-alapú hitelesítés stb.

Az erős hitelesítési technológiák részét képezik a „több tényezős"[8] technológiák, amelynek alapja, hogy a felhasználó egynél több hitelesítési tényezővel rendelkezzen, egy speciális listán felsorolt lehetőségek közül, melyek közé tartoznak a „valami, amit Ön ismer csak" típusúak (jelszavak, PIN kódok stb.), a „valami, amivel Ön rendelkezik" típusúak (telefonok, okos / smart kártyák, biztosítékok és tokenek), vagy a „valami, ami Te vagy" típusúak (biometrikus azonosítók, mint a retina vizsgálat, hang minta, új lenyomat stb.). A több tényezős megoldásoknál, akár két tényezősről, akár három tényezősről van szó, a tényezők típusainak különbözniük kell egymástól – azaz nem lehet például a „valamit, amit csak Ön ismer" kategóriából két lehetőséget együttesen alkalmazni, mint például a jelszó és a PIN kód.

Vannak olyan rendszerek, amelyeket „több tényezős" hitelesítési rendszernek tekintenek, de nem felelnek meg a fenti meghatározásnak. Habár ezek a rendszerek használják a web böngésző jellemzőit, mint az IP alapú helymeghatározás, használati minták, idő alapú azonosítás és így tovább – ezek mindegyike hasznos információ a felhasználók azonosítására, de ezek korántsem olyan elfogadottak a biztonsággal foglalkozó közösségekben, mint a három hagyományos kategória.

Out-of-band hitelesítés

Mostanában tűnt fel a „több tényezős" rendszerek között: a sávon belüli kontra sávon kívüli hitelesítés (in-band versus out-of-band). A sávon belüli (in-band) rendszerek mindegyik tényezőjüket (kettő vagy három) egyetlen logikai csatornán keresztül szerzik meg, a sávon kívüli (out-of-band) rendszerek legalább két csatornát használnak a tényezők begyűjtéséhez. Egy közismert példája a sávon kívüli rendszereknek (out-of-band) a token alapú hitelesítés – a felhasználók közölnek valamit amit csakis ők tudnak (például a PIN kódjukat), azzal együtt amijük van (ezzel bizonyítják, hogy rendelkeznek a tokennel, ideiglenes token kód formájában), az Interneten keresztül ugyanazon a csatornán.

A sávon belüli (in-band) rendszerek gyengesége abban van, hogy egyetlen káros szoftverrel a rendszeren egyszerre lehet megtámadni mindkét tényezőt. A token esetén például a rendszer megtámadásához egy káros szoftverrel meg kellene szerezni a bemeneti adatokat (a PIN kódot és a token kódot), és továbbítani azt a támadónak egy másik eszközön vagy csatornán keresztül, mint például az IM[9]. Amikor a támadó megkapja az információt, akkor egyszerűen felhasználhatja a

8 „multi-factor"

9 Instant Messaging – azonnali üzenetküldő rendszer, mint pl.: MSN, IRC stb.

bejelentkezésre azt, és a szerver nem tud különbséget tenni a támadó és a törvényes felhasználó ugyanonnan történő bejelentkezése között.

A problémára megoldást jelent a sávon kívüli (out-of-band) hitelesítés használata, ahol a tényezők begyűjtése különböző logikai csatornákon keresztül történik. A telefon alapú hitelesítés a legelterjedtebb és a legszélesebb körben használt a sávon kívüli (out-of-band) hitelesítési eljárásokban. Ez úgy működik, hogy begyűjt valamit az Interneten keresztül, amit csak Ön ismer és ellenőrzi azt, ami Önnek van (a telefon megléte) a telefonhálózaton keresztül, így lehetetlen egyetlen káros szoftverrel megtámadni egyszerre mindkét tényezőt.

A tranzakciók megerősítése

A bejelentkezések hitelesítése kritikus folyamat, de a legújabb, legkifinomultabb támadások miatt ez nem elégséges. Amennyiben bekövetkezik az, hogy egy támadás elindítása túl bonyolulttá válik, akkor a bűnözők egyszerűen keresnek egy másik könnyű utat, a támadás kivitelezéséhez. Amennyiben túl nehéz megtámadni a hitelesítést, akkor a támadók egy káros szoftverrel egyszerűen megkerülik azt. Ezek a támadások egyáltalán nem elméletek, számos esetben jelentettek káros szoftverekhez, mint például a Zeus-hoz és a Clampi-hoz kapcsolódó hitelesítés utáni támadásokat.

Egy ilyen támadás a következőképpen működik: a felhasználó gépe egy káros szoftverrel fertőzött, ami türelmesen várakozik mindaddig, amíg a felhasználó be nem jelentkezik az online bankoláshoz használt oldalra. Nem tudja megkerülni az oldalt, az erős hitelesítő eljárás alkalmazása miatt, de nincs is rá szükség – egyszerűen megvárja a felhasználó bejelentkezését. Amikor a bejelentkezés megtörtént, akkor a káros szoftver parancsokat ad a banknak például pénz átutalásra, anélkül, hogy a felhasználó látná, hogy mi is történik, aki ezalatt például próbálja ellenőrizni az egyenlegét vagy belép egy online számlafizető kérésbe.

A bank nem tud különbséget tenni a csaló tranzakciók és a törvényesek között, kivéve ha a felhasználó különösen elővigyázatos a bankszámla műveletekkel, a tranzakciót könnyű elhibázni, mielőtt az törlésre kerülne. Ezen a ponton nem lehet megállapítani egyértelműen, hogy ki a felelős a veszteségért, de ekkor főképpen a banki ügyfelek felelőssége merül fel, nem pedig a banké. (Megjegyzendő, hogy ez a törvénykezés egy gyorsan fejlődő területe, és megegyezést legalább egy megkezdett polgári perben született állásfoglalás hozhatna.)

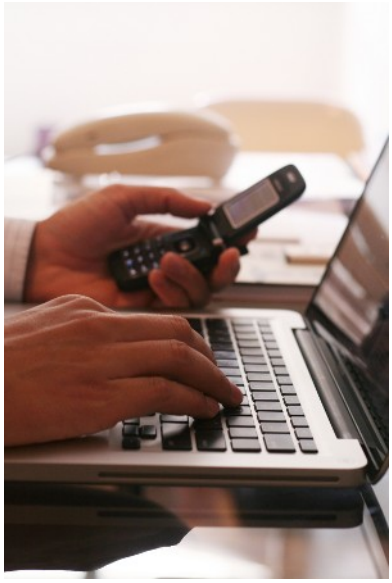
Sőt mi több, belülről indított támadások is lehetségesek. Képzeljünk el egy olyan káros szoftvert, amely egyszerűen csak várakozik az ACH[10] tranzakciókba belépő online bankoló ügyfelekre, azután a káros program megváltoztatja a cél ABA[11]-t és a bankszámla számokat. Az ügyfél bankszámlájának egyenlege még mindig helyesnek látszik, kivétel az az eset, ha az ügyfél különösen elővigyázatos (és részletekre figyelő) könyvelő típus, mert a probléma csak hetek múlva derülne ki, amikor a jogos címzett reklamálni kezd az elmaradt kifizetés miatt.

A probléma gyökere ismételten egy hitelesítési hiba. Azaz a tranzakciót nem a hitelesített felhasználó indította - hanem egy jogosultsággal nem rendelkező, ami biztonsági elvi hibából ered, amit a káros szoftver testesített meg. A megoldás az, hogy a felhasználónak a tranzakció ideje alatt újra azonosítania kell magát. Magának a tranzakciónak a hitelesítése megelőzi, hogy a káros szoftver nem kért tranzakciókat bonyolítson le.

10 Automated Clearing House (Automatikus Klíring Ház): Pénzügyi intézmények és vállalatok közötti pénzátutalások, állami értékpapír ügyletek elektronikus feldolgozását végzi

11 American Bankers Association (Amerikai Bankár Szövetség): Nemzetközi egyezmény szerint ez a szerv működik a kártyakibocsátói azonosító számok regisztrációs hatóságaként

A fenti példát alapul véve, tegyük fel, hogy az online banki alkalmazásokat telefonon keresztül történő tranzakciójóváhagyás védi. A fenti példában, a beérkezett ACH átviteli kérés nyugtázásakor a banki szerver kezdeményezne a felhasználó felé egy telefon hívást, mivel (látszólag) ő indította az adott kérést, visszajátszaná neki a tranzakció részleteit, és kérné annak jóváhagyását. Természetesen a felhasználó megtagadhatná a tranzakciót, így a pénz semmi esetre sem hagyná el a számlát.



A tranzakciójóváhagyás kérdése több annál, mint egy egyszerű felhasználói hitelesítés. Még így is van lehetőség arra, hogy kiderítsék a fent leírt bankszámlaszám kapcsolót, mialatt a felhasználó újra begépeli a cél bankszámlaszámot a jóváhagyás hívás alatt. Ez egy egyszerű kérés, a felhasználó a hívás ideje alatt látja a cél bankszámla számot, így hatékonyan megelőzhető a bankszámla szám kapcsoló támadás. Valójában mindkét eset a tranzakció adatainak aláírása (TDS[12]). Azzal, hogy a felhasználótól kérik az újra azonosítást, vagy aláírást, minden egyes tranzakcióhoz, így a bank egészen biztos lehet a kérés hitelességében. Egy teljes TDS kérésnek tartalmaznia kellene a dátumot, a forrás és cél bankszámlaszámokat, a tranzakció összegét az azonosító kóddal együtt. A bankok ezen információk egy részhalmazának használatával elérnék a megfelelő szintű biztonságos hitelesítést.

A tranzakciójóváhagyás túlmutat az online bankoláson, ami természetesen minden olyan esetre vonatkozik, ahol érzékeny információk vannak. Ezt a koncepciót lehetne alkalmazni a fájl szervereken a fájlok megváltoztatásához, vagy például a speciális weboldalakhoz történő hozzáféréskor az adatok olvasásakor.

A közös weben az egyedi bejelentkezési és hitelesítési megoldások a már megszokott módon választják szét a dokumentumokat a megkövetelt hitelesítési szint alapján, már két közösségi rendszer, az IBM Tivoli Access Manager és a Computer Associates SiteMinder is támogatja a fokozatos hitelesítést, amihez használja a telefon alapú azonosítást. Egy alkalmazáson belül igen bonyolult lehet a megfelelő hozzáférési szintek meghatározása. A biztonsági adminisztrátoroknak meg kell találniuk az egyensúlyt az elérni kívánt biztonságos hitelesítés és a felhasználók felé intézett újrahitelesítési kérések normál üzletmenetet zavaró mivolta között.

Különböző eszközök jelennek meg, amelyek megtartják a felhasználók által közösen használt eszközök egyszerűségét, ugyanakkor a biztonságot is megfelelő szinten tartják, beleértve az IP alapú „fehér listákat” (whitelist), ahol a hitelesítés a megbízhatónak tekintett számítógépekről érkezett, vagy a tranzakcióhitelesítő gyorsító tárakat, ami az egymást követő hasonló tranzakcióknál kiküszöböli az újraazonosítást. Például, nincs értelme az újraazonosításnak azoknál az ACH átutalásoknál, ahol a megadott cél bankszámlaszám esetén az első azonosítás már sikeres volt.

A tranzakció jóváhagyás számos módon implementálható. A telefonos hitelesítést az egyik lehetőségként írtuk le, egy másik módszer az SMS alapú hitelesítés, ahol a tranzakció részletei SMS szöveges üzenetként kerülnek elküldésre a felhasználó mobil telefonjára. A felhasználó az SMS-re sávon kívül (out-of-band) tud válaszolni, hogy jóváhagyja a tranzakciót. Továbbá számos smart kártyán alapuló megoldás is van, ahol az összes tranzakciós adat aláírással rendelkezik, még nem vizsgáltuk a fejlesztések költség és logisztikai vonatkozásait.

Ezeknek a rendszereknek a használatához smart kártya olvasóra van szükség, numerikus billentyűzettel, ahol begépelhetőek és aláírhatóak a tranzakció részletei. Számos ellentmondást vet fel a tranzakciójóváhagyás. A legtöbb alkalmazásnál (kivételek egyes kormányzati esetek) hiányzik a tranzakció megfogalmazása vagy az események jóváhagyása. Ezek az alkalmazások egyszerűen nem rendelkeznek a munkafolyamat tetszőleges pontjaihoz kötődő azonosítási eljárással. Az

12 Transaction Data Signing (Tranzakciós adatok aláírása): egy előállított kód, amelyet a hitelesítési és a tranzakció azonosítási folyamat részeként használnak.

alkalmazásoknál szükség lehet a forrás kód módosítására vagy egy proxy megoldásra. Az alap képességek között a rendszerre vonatkozó tranzakciójóváhagyás beállítások igen bonyolultak lehetnek, mert a viszonylag mindenre kiterjedő szabálykészlet határozza meg, ha további hitelesítés szükséges, valamint a használat egyszerűsége és a hitelesítés biztonsága közötti feszültség. A központosított hozzáféréskezelő rendszerek segíthetnek a heterogén webes környezetben, bár a biztonsági adminisztrátorok csak magukra hagyatkozhatnak, ha egyedi üzletági alkalmazást használnak.

A jövő

Változik a világ. A cyber bűnözők kitűnő, életképes hitelesítő rendszerek elleni támadásokat hajtanak végre, ezért a biztonsági adminisztrátoroknak igen nehéz feladat a felhasználóikat megvédeni ezektől a támadásoktól. Így merre is induljunk? A cégeknek minden részletre kiterjedő hitelesítésbiztonsági elemzést kell végezniük a cégnél alkalmazott minden jelentősebb új alkalmazás esetén. Központi kérdés, hogy az alkalmazás egy eseményalapú hitelesítést támogat vagy a proxy alapú megoldásokat. Keresni kell a sávon kívüli (out-of-band) hitelesítési eljárásokat, amik védelmet jelentenek a párhuzamos fenyegetettségek ellen.

Végül, elemezni kell a meglévő alkalmazások hitelesítés rendszerének lehetséges gyenge pontjait. A magas kockázatot jelentő tranzakciókat tranzakció jóváhagyással kell védetté tenni; nyomást kell gyakorolni a forgalmazókra a tranzakció jóváhagyás támogatásáért vagy ezt saját maguknak kell megtenniük.

Java kliensek támadása I.

A dokumentum Stephen de Vries “Attacking Java Clients: A tutorial” című prezentációjára épül, melyet a szerző 2010. július 20-án publikált, és 2010-ben Las Vegas-ban a Blackhat konferencián prezentált. A prezentáció terjedelme miatt a tartalom bemutatása két részre tagolódik, ahol első ízben az információgyűjtésbe, valamint az analízisbe nyerhetünk bepillantást. A későbbiekben a kiaknázás kerül górcső alá, ahol megismerkedhetünk egy példaprogramon keresztül a Java kliensek gyenge pontjainak kihasználási módszereivel, a kliens biztonsági kontrolljainak megkerülésével, befecskendezési technikákkal és a szerver oldali funkciók támadási módjaival.

Áttekintés

A Java klienseket gyakran a szerver oldali alkalmazások lehetőségekben gazdag klienseiként használják. Biztonsági tesztelők szempontjából, számos akadály gátolhatja a Java kliens/szerver alkalmazások alapos felmérését:

- A kommunikációs réteg lehallgatása és manipulálása komoly kihívást jelent (gyakran SSL[13] kapcsolaton át RMI[14]-vel találkozhatunk)
- A kliens által végrehajtott bevitel ellenőrzése gátolhatja a befecskendezési módszereket, megnehezítve például az XML vagy az SQL befecskendezéses támadásokat.
- A kliens oldali biztonsági kontrollok behatárolhatják a rendelkezésre álló funkciókat.
- A grafikus felhasználói felületek korlátozhatják az automatikus tesztelést, mint például a brute force[15] vagy a szótár alapú jelszótörések alkalmazását.

13 Secure Soceket Layer (SSL) – Kriptográfiai protokollok, melyek biztonságos hálózati kommunikációt szolgáltatnak.
14 Java Remote Method Invocation (RMI) – Java alkalmazás programozási interfész, mely objektum-orientált ekvivalens távoli eljárás hívásokat (RPC) hajt végre.
15 Brute force – Jelszó töréseknél használatos módszer, mely az összes lehetőség kipróbálását jelenti.

Módszertan körvonalakban

1. Információgyűjtés
   - Osztályok azonosítása
   - Az alkalmazás darabokra szedése a funkciók mélyebb megértése érdekében
2. Próbálkozás és analízis
   - Szekvencia diagram készítése az interakciók alapján
   - Dinamikus nyomkövetés alkalmazása a végrehajtási folyamat megértése érdekében
   - Potenciális támadási vektorok megállapítása
3. Kiaknázás
   - Shell[16] befecskendezés
   - A kliens oldali biztonsági kontrollok megkerülése
   - Szerver oldali funkciók támadása
     - Befecskendezéses támadások
     - Brute force és/vagy szótár alapú támadások
     - Hozzáférés vezérlés
     - Logika

Eszközök

A fenti megközelítést elősegíti számos, szabadon elérhető fejlesztő eszköz. Az analízis számottevő része, valamint a nyomonkövetés Eclipse IDE[17] alkalmazásával történik. A tesztelési környezet leggyorsabb kialakításának módja az Eclipse Test & Performance Tools Platform Project (TPTP) csomag letöltése a http://www.eclipse.org/tptpt/ oldalról, majd a fennmaradó plugin-ok telepítése az Eclipse update manager használatával. A következő plugin-ok szükségesek:

- JD Eclipse decompiler: http://java.decompiler.free.fr/?q=jdeclipse
- AspectJ Development tools: http://eclipse.org/ajdt/

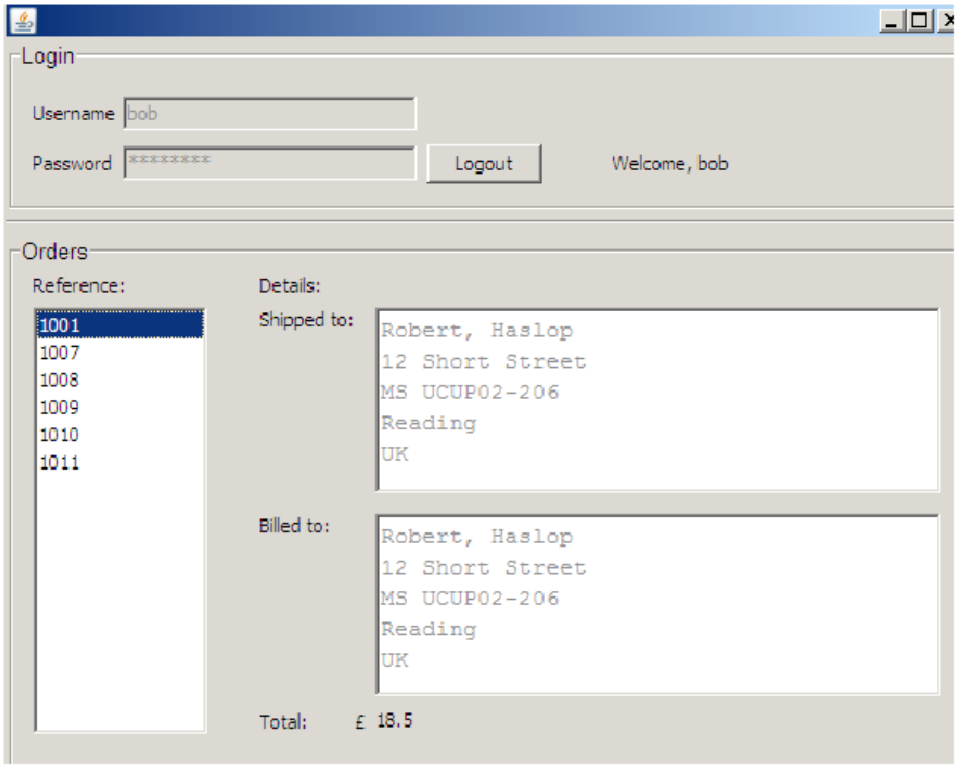
A BeanShell csomag (http://beanshell.org/) és a Java Object Inspector (http://www.programmers-friend.org/download/) szintén szükségesek a befecskendezésekhez. Az AspectJ a TPTP alternatívájaként is használható a Java alkalmazások befecskendezésekor (http://www.eclipse.org/aspectj/downloads.php).

A demo alkalmazás bemutatása

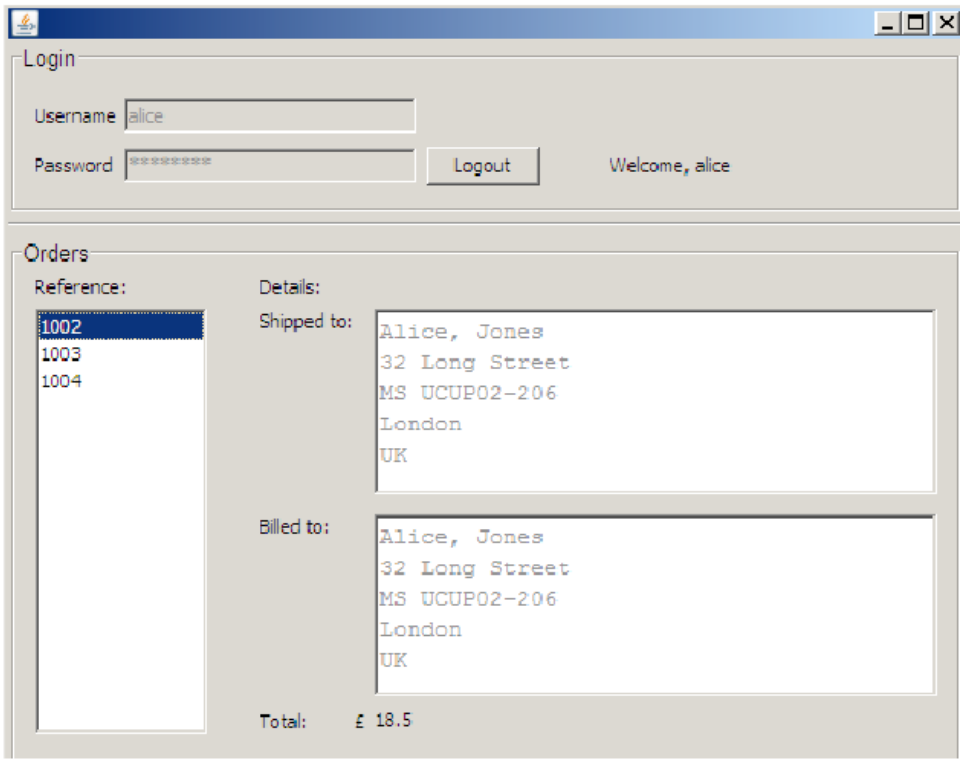
Az alkalmazás lehetővé teszi a felhasználók számára, hogy megtekintsék rendeléseiket, melyeket egy adott online shop felé adtak le. Implementált egy elérési kontroll, melynek feladata, hogy adott felhasználó csak a saját rendeléseibe nyerhessen bepillantást.

16 Shell – A felhasználók számára nyújtott csatlakozási felület, mely elősegíti a rendszermag szolgáltatásainak elérését.
17 Integrated Development Environment (*IDE*) – integrált fejlesztői környezet

Például a “bob” nevű felhasználó a következő rendeléseket láthatja:



Míg “alice” az alábbiakat láthatja:



Potenciális támadások

A kliens által nyújtott egyszerű szolgáltatások, nevezetesen a belépési és a rendelési funkciók számos támadási formát tesznek érdekessé:

- a kliens manipulálása, illetéktelen rendelési információk elérésének céljából
- szerver oldali támadások (pl.: SQL befecskendezés)
- automatikus brute force, vagy szótár alapú támadások a hitelesítési igazolványok, azaz a felhasználónevek és jelszavak felderítésének céljából

A dokumentum további részének tárgya a fenti támadások tesztelése.

Információgyűjtés

Mindenekelőtt azonosítani szükséges, hogy mely JAR fájlok, vagy osztály fájlok érdekesek biztonsági szempontból. Java kliensek esetén igen gyakori, hogy számos osztály könyvtárat tartalmaznak, ezért elengedhetetlen, hogy megkülönböztessük ezeket a könyvtárakat a szóban forgó kódtól. A példában, a run.bat fájl a com.corsaire.ispatula.Main osztályt hívja meg, így tudhatjuk, hogy legalább ez az osztály (és az ispatula csomag) érdekes a számunkra.

Ajánlatos a többi JAR fájl osztályainak áttekintése is:

```
-rw-r--r-- 1 stephen stephen   217289 2009-08-21 16:31 appserv-deployment-client.jar
-rw-r--r-- 1 stephen stephen   591616 2009-08-21 16:31 appserv-ext.jar
-rw-r--r-- 1 stephen stephen 15699295 2009-08-21 16:31 appserv-rt.jar
-rw-r--r-- 1 stephen stephen   545182 2009-08-21 16:32 AdminBean.jar
-rw-r--r-- 1 stephen stephen   545182 2009-08-21 16:31 AdminClient.jar
-rw-r--r-- 1 stephen stephen      353 2009-08-21 16:31 j2ee.jar
-rw-r--r-- 1 stephen stephen  1101181 2009-08-21 16:31 javaee.jar
-rwxr-xr-x 1 stephen stephen      191 2009-08-21 16:31 run.sh
-rw-r--r-- 1 stephen stephen   118103 2009-08-21 16:31 swing-layout-1.0.3.jar
```

Ezt a műveletet a jar program segítségével hajthatjuk végre, melynek a szintaxisa nagyon hasonlít a tar-hoz. A fájlok és a tartalmuk áttekintése jobb rálátást biztosít a releváns információk megállapításához:

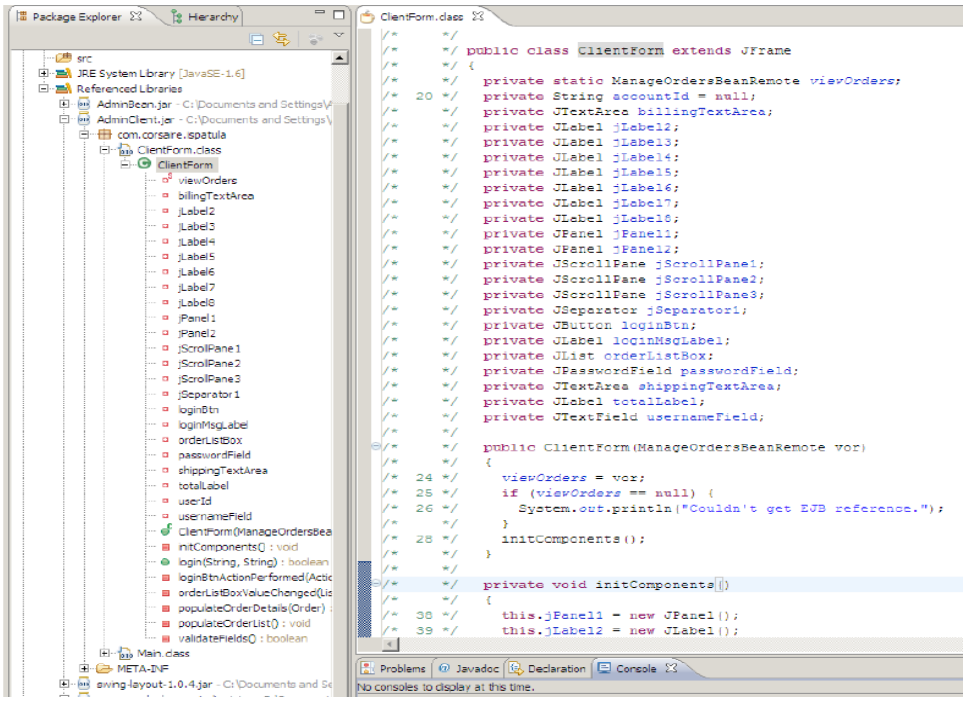
```
for i in `ls *.jar` ; do echo "INSPECTING JAR: " $i|less; jar tvf $i|less; done
```

Azok a csomagok, melyek java.* javax.* és com.sun.* nevekkel kezdődnek, nyilvánvalóan nem a keresett kódot tartalmazzák. Ennek megfelelően azokat a csomagokat érdemes keresni, melyek olyan nevekkel rendelkeznek, amik valószínűleg a kliens fejlesztőjétől származnak. A keresés után, a következő fájlok tűnnek érdekesnek:

- AdminBean.jar
- AdminClient.jar

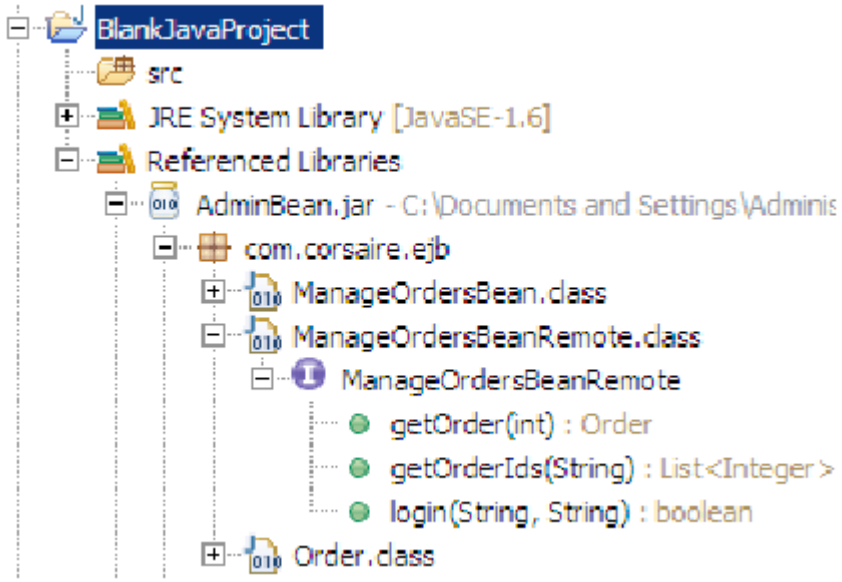
Egy még kényelmesebb eljárás a JAR archívumok vizsgálatára az Eclipse JD Decompiler plugin használata. Egy új Java projekt létrehozásával és az érdekes JAR fájlok könyvtárként való hozzáadásával, majd kinyitva a JAR állományt és az osztályokra kattintva, megjelenik a kinyert tartalom az ablakban.

A *package explorer* megjeleníti az osztály mezőit és a metódusait.



Egy futólagos pillantással a ClientForm osztály mezőire, figyelemre méltó információkat szerezhetünk. Feltárhatjuk a login(String,String) metódust, ami a későbbi nyomozás során érdekes lehet. A ClientForm GUI[18] osztályokat is tartalmaz, mint például a panelek, címkék és gombok.

A ManageOrdersBeanRemote osztály ugyancsak lényeges:



A "Remote" név egy nyomravezető jel, valószínűleg egy EJB[19] stub interfészt takar, mely távoli metódusok hívására használatos a szerver oldali EJB komponenst illetően. A feltárt kód:

```
import javax.ejb.Remote;

@Remote

public abstract Interface ManageOrdersBeanRemote
```

Az annotáció és az import megerősíti azt, hogy egy EJB-vel van dolgunk.

18 Graphical User Interface (GUI) – grafikus felhasználói felület

19 Enterprise JavaBean (EJB) – Az Enterprise JavaBean-ek moduláris vállalati alkalmazásokban használt szerveroldali komponensek. Általában az üzleti logika implementációját tartalmazzák.

A javap parancs használható ugyanezen információ megszerzésére IDE használata (pl.: Eclipse) nélkül. A legtöbb JDK[20] tartalmazza a javap-ot.

```
javap -classpath AdminClient.jar -private com.corsaire.ispatula.ClientForm
Compiled from "ClientForm.java"
public class com.corsaire.ispatula.ClientForm extends javax.swing.JFrame{
    private static final java.util.logging.Logger log;
    private static com.corsaire.ejb.ManageOrdersBeanRemote viewOrders;
    private java.lang.String accountId;
    private javax.swing.JTextArea billingTextArea;
    private javax.swing.JLabel jLabel2;
    private javax.swing.JLabel jLabel3;
    private javax.swing.JLabel jLabel4;
    private javax.swing.JLabel jLabel5;
    private javax.swing.JLabel jLabel6;
    private javax.swing.JLabel jLabel7;
    private javax.swing.JLabel jLabel8;
    private javax.swing.JPanel jPanel1;

    private javax.swing.JPanel jPanel2;
    private javax.swing.JScrollPane jScrollPane1;
    private javax.swing.JScrollPane jScrollPane2;
    private javax.swing.JScrollPane jScrollPane3;
    private javax.swing.JSeparator jSeparator1;
    private javax.swing.JButton loginBtn;
    private javax.swing.JLabel loginMsgLabel;
    private javax.swing.JList orderListBox;
    private javax.swing.JPasswordField passwordField;
    private javax.swing.JTextArea shippingTextArea;
    private javax.swing.JLabel totalLabel;
    private javax.swing.JTextField usernameField;
    public com.corsaire.ispatula.ClientForm(com.corsaire.ejb.ManageOrdersBeanRemote);
    private void initComponents();
    private void orderListBoxValueChanged(javax.swing.event.ListSelectionEvent);
    private void loginBtnActionPerformed(java.awt.event.ActionEvent);
    public boolean login(java.lang.String, java.lang.String);
    private void populateOrderList();
    private void populateOrderDetails(com.corsaire.ejb.Order);
    static void access$000(com.corsaire.ispatula.ClientForm,
java.awt.event.ActionEvent);
    static void access$100(com.corsaire.ispatula.ClientForm,
javax.swing.event.ListSelectionEvent);
    static {};
}
```

Megjegyezzük, hogy az EJB egy mező a ClientForm osztályban. A javap használatával ugyancsak rálátást nyerhetünk a rendelkezésre álló metódusokra:

```
javap -classpath ..\AdminBean\dist\AdminBean.jar com.corsaire.ejb.ManageOrdersBeanRemote
Compiled from "ManageOrdersBeanRemote.java"
public interface com.corsaire.ejb.ManageOrdersBeanRemote{
    public abstract java.lang.String login(java.lang.String, java.lang.String);
    public abstract java.util.List getOrderIds(java.lang.String);
    public abstract com.corsaire.ejb.Order getOrder(int);
}
```

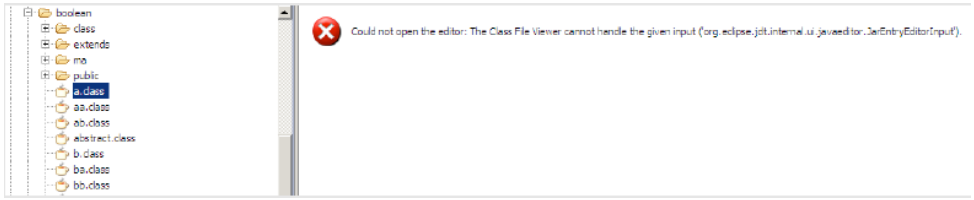
20 Java Development Kit (JDK) – Java fejlesztői csomag

Megjegyzés

Léteznek olyan "obfuscation" módszerek, melyek összezavarhatják, elhomályosíthatják számunkra az alkalmazás működését. Ezek az eljárások módosíthatják a metódusok neveit, a mezőket és az alkalmazás osztályainak neveit is. Számos obfuscator[21] a logikát is módosítja és optimalizálja a bájtkódot, teljesen összezavarva a visszafejtő programokat. A JD Decompiler ennek ellenére megbirkózik a legtöbb összezavart osztállyal. Mindamellett a kód mögött rejlő jelentés megfejtése jóval bonyolultabb lehet. Elhomályosított bájtkód biztonsági tesztelésekor két fő technika használható: a könyvtárakra vonatkozó referenciák keresése (kiváltképpen a JEE könyvtárakat illetően), valamint a futó alkalmazás aktív nyomonkövetése.

Az alkalmazás aktív nyomonkövetésével következtethetünk a biztonsági perspektívából lényeges osztályokra. Nem szükséges a kód minden egyes sorának megértése, mindössze az érdekes metódusok hívásának azonosítására van szükség.

Ahol az IDE és a JD Decompiler csődöt mond, ott a javap eszköz még további információt szolgáltathat. Például a következő osztályt az Eclipse, illetve a decompiler[22] már nem képes megvizsgálni:



Ugyanakkor a javap megoldást nyújt a fenti problémára:

```
C:\Documents and Settings\Administrator\tutorial\xyz\xyz\boolean>javap -private -
classpath . aa

class xyz.boolean.aa extends xyz.boolean.bb{

    xyz.boolean.aa(xyz.interface.private.for);

    private void if(java.util.List);

    public java.lang.String if(xyz.class.StringBuffer, int);

}
```

Az információgyűjtés fázisa után a következő ismeretekkel rendelkezünk:

- Két JAR fájl érdekes (AdminBean.jar; AdminClient.jar). Egyikük EJB interfészt tartalmaz, mely meghatározza a szerver oldalon meghívott metódusokat.
- Az alkalmazás EJB technológiát használ a szerverrel való kommunikációja során.
- A ClientForm osztály tartalmazza a GUI logikát.
- A ClientForm egy EJB stub referenciát tartalmaz.
- A stub által felfedett metódusok:
  - String login(String username, String password);
  - List<Integer> getOrderIds(String accountId);
  - Order getOrder(int id);

Továbbá az osztályok visszafejtéséhez további két technikát alkalmazunk a kliens működésének mélyebb megértéséhez:

- Profil készítés az Eclipse Test & Performance Tools Platform segítségével
- Dinamikus nyomonkövetés.

21 Obfuscator – olyan szoftver, eljárás, mely elhomályosítja az alkalmazás működését, nehezítve a kód, illetve a működés logikájának visszafejtését.
22 Decompiler – kódvisszafejtő szoftver

Mindkét módszer használható, illetve egyes esetekben elegendő csak az egyik alkalmazása, amennyiben az összes szükséges információ kinyerhető vele.

Próbálkozás és analízis

Az analízis céljai a következők:

- a program logikájának megértése.
- az érdekes osztályok és metódusok azonosítása.
- a BeanShell számára alkalmas befecskendezési pontok azonosítása.

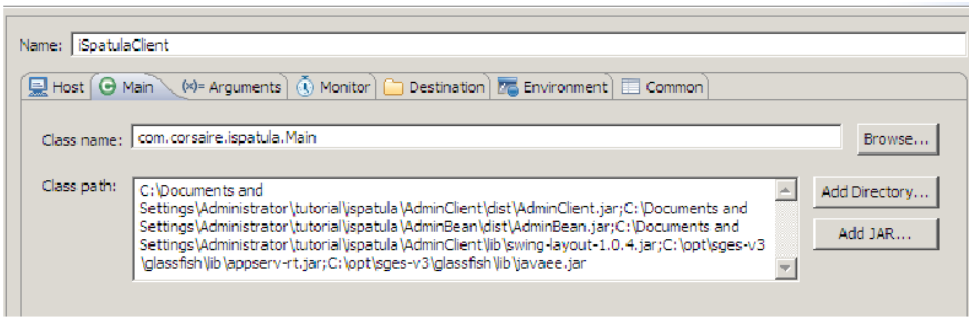
Profil készítés Eclipse TFTP-vel

A TPTP plugin-nal indított Eclipse *Run* menüjéből a *Profile Configurations* kiválasztása szükséges. Itt új konfiguráció készíthető egy külső Java alkalmazás számára. A Main szekcióban szükséges meghatározni a futtatandó osztályokat és a használatos classpath-t. Mindezek már adottak a run.bat szkriptben, így mindösszesen az értékek átmásolását kell végrehajtani.

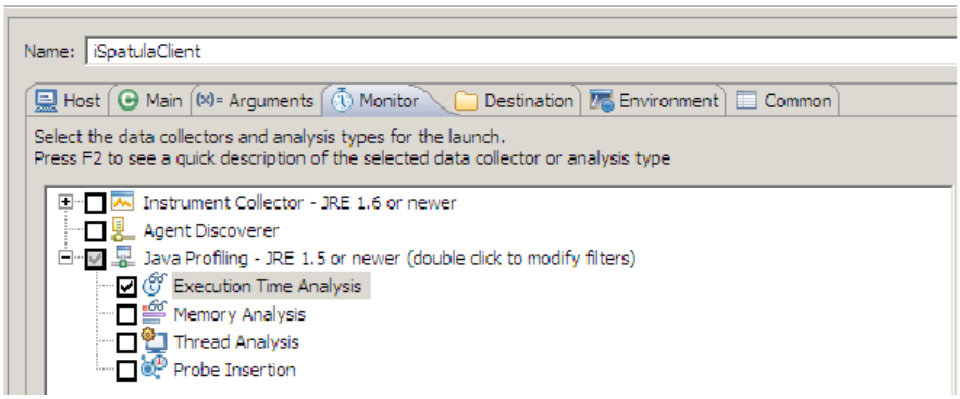
A run.bat a következőket tartalmazza:

```
java -classpath lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-
1.0.4.jar;..\AdminBean\dist\AdminBean.jar;dist\AdminClient.jar
com.corsaire.ispatula.Main
```

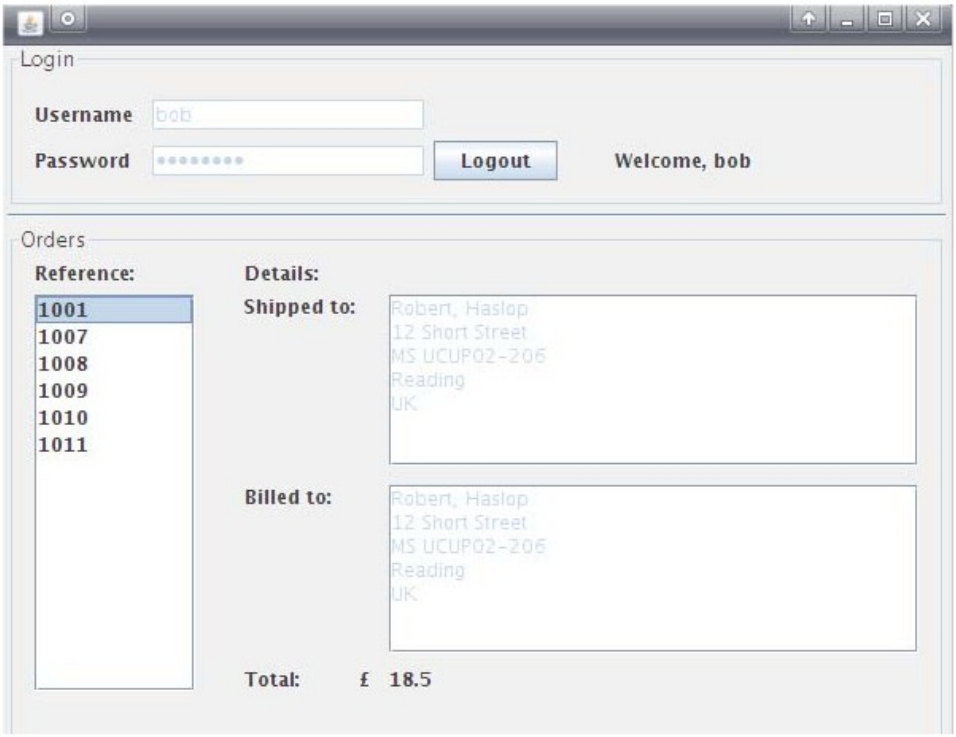
Ugyanezeket a main és JAR fájlokat kell meghatározni az Eclipse profil konfigurációjában:



Az alkalmazásnak nincs szüksége argumentumokra. Már csak a *Monitor* tab alatt az *Execution Time Analysis* kiválasztására van szükség, hogy készen álljunk a profilozáshoz.

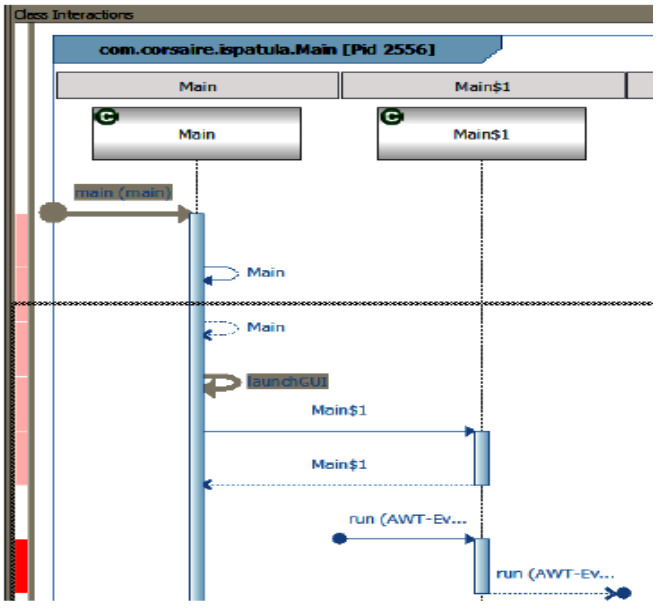


Az alkalmazás indulása eltarthat egy darabig, de amikor elindult, az ismert GUI alkalmazással találkozhatunk.



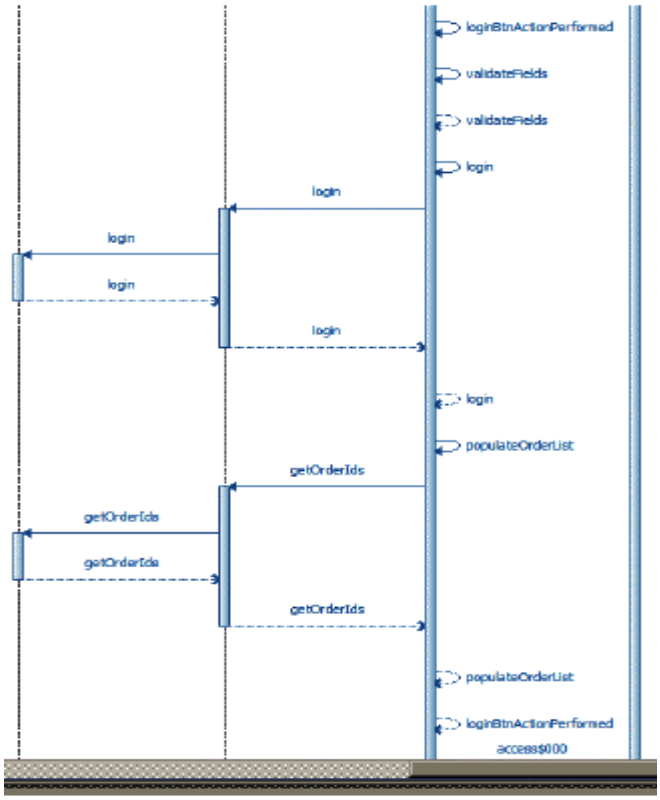
Egyszer átfutunk az alkalmazáson, hogy megfigyelhessük hogy miket is hív meg futása során. Miután megtörtént a sikeres belépés "bob" felhasználóval, és kiválasztásra került az egyik rendelési referencia, kilépünk, és bezárjuk az alkalmazást.

Az Eclipse-en belül, jobb klikk a profilozott alkalmazásra, a *Profiling Monitor* mezőben, majd "Open with.." UML2 Class Interactions. Az eredmény egy UML2 szekvencia diagram az osztályok közti interakciókkal kapcsolatosan a metódus hívások során.

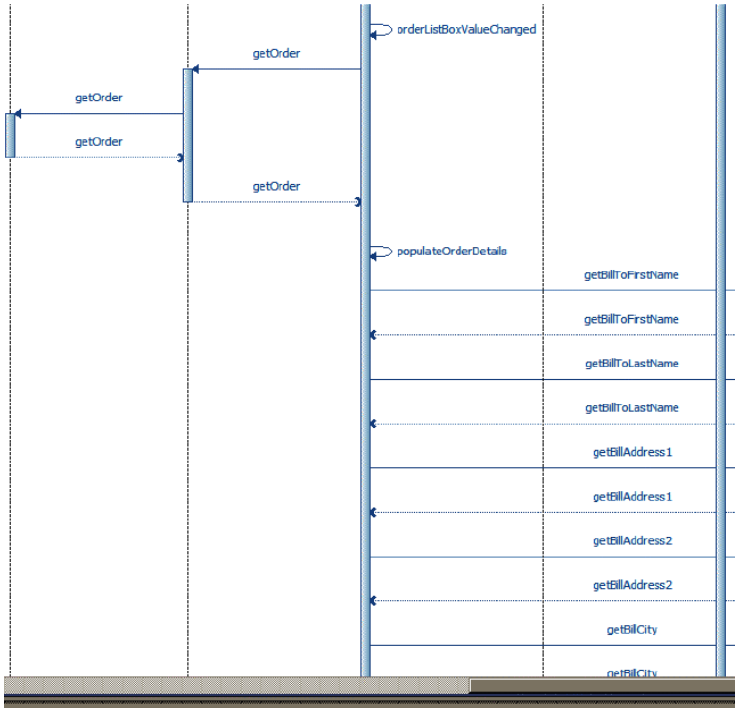


Az osztályokon át történő horizontális navigáció, rálátást biztosít a GUI osztály és a korábban azonosított EJB osztály közti interakciókra.

A bejelentkezési folyamat – ideértve a megrendelési azonosítók (order ID) meghatározását – tisztán kivehető az alábbi ábrán:



Úgy tűnik, hogy a megrendelési azonosítók népesítik be a megrendelési mezőket:



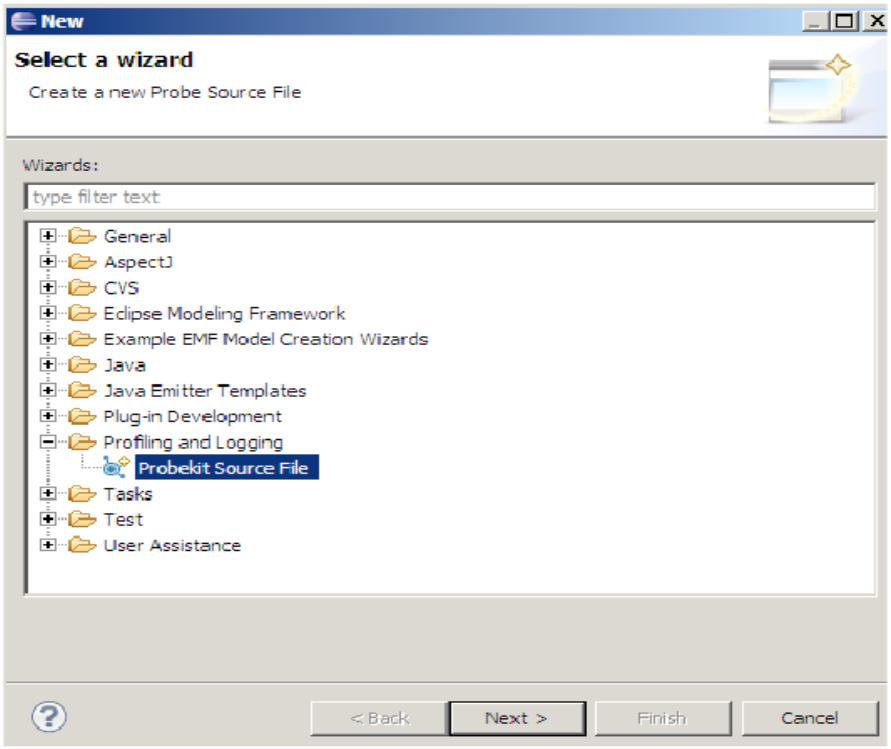
A végrehajtási folyamat mellett a szekvencia diagram megmutatja, hogy a ClientForm tartalmaz referenciát a ManageOrdersBean EJB-re. Más szavakkal, a ClientForm egy kitűnő hely olyan kódok befecskendezésére, melyekkel EJB-t érintő metódusokat hívunk.

Összegezve, az Eclipse profilozó eszköz értékes betekintést biztosított a végrehajtási folyamatba, és megismerkedhettünk azzal, hogy mely metódus, mely osztályon került meghívásra. A szekvencia diagram tisztán tükrözi a kapcsolatot – melyet már korábban felfedeztünk a javap eszközzel – a ClientForm osztály és a ManageOrdersBeanRemote EJB stub között. A ClientForm osztálynak létezik egy EJB példánya, és közvetlenül hív meg metódusokat rajta.

Dinamikus nyomkövetés TPTP-vel

Egy program végrehajtásának nyomonkövetése kiíratással vagy naplózással, ugyancsak hasznos technika lehet a végrehajtási folyamat megértéséhez. Természetesen a kiíratás nem minden esetben célravezető, amikor nem rendelkezünk a forrással natív alkalmazások esetén, de a Java-ban nem hogy célravezető, de igen könnyen kivitelezhető is.

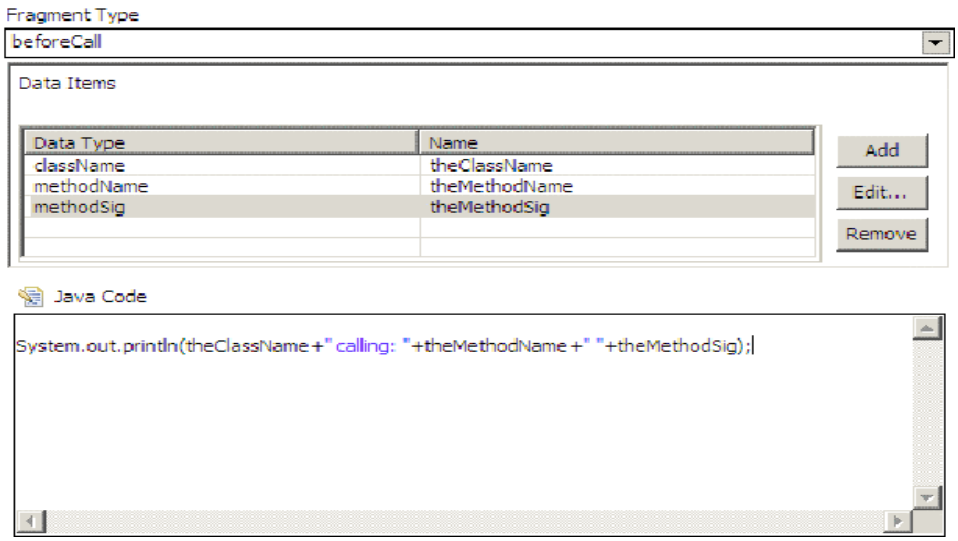
Az Eclipse TPTP projekt használatával kiíratást helyezhetünk el minden egyes metódus hívásban, így megérthetjük a hívási folyamatot. Ez maga után vonja a próbálkozások kialakítását és a próbák elhelyezését az általunk érdekesnek tartott JAR fájlokban. Mindenekelőtt, mentsük el az eredeti JAR fájlt, mielőtt megkezdenénk a módosításokat a próbáinkkal! Majd szükségünk lesz egy üres Java projekt létrehozására, és a cél JAR fájlok referencia könyvtárként való hozzáadására. Ezek után létrehozunk egy “Probekit source” Java projektet és rámutatunk az előzőleg létrehozott, üres Java projektre.



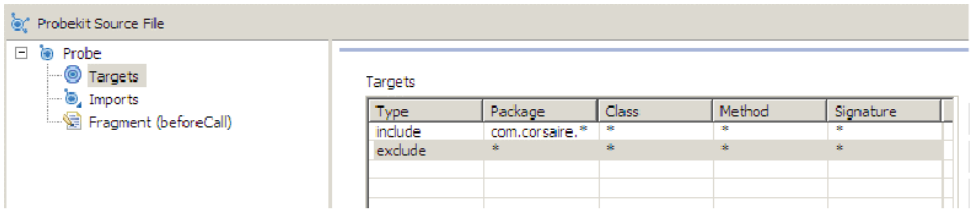
Válasszunk egy “Callsite” próbát és helyezzük el a következő kód fregmentet, majd győződjünk meg arról, hogy a fregment típusa “beforeCall”.

```
System.out.println(theClassName+" calling: "+theMethodName+" "+theMethodSig);
```

A kód kiírja a hívó osztály nevét, a meghívott metódus nevét és a metódus aláírását. Szükséges még a változók definiálása:



Még mielőtt finomhangolhatnánk a JAR fájlt, szükségünk van a próba céljának beállítására. A szabályoknak tartalmazniuk kell az “include” és az “exclude” szabályokat:



Majd jobb klikk az AdminClient.jar fájlra, és válasszuk ki az *Instrument* ponton belül a *Static Instrumentation* opciót. Az Eclipse így statikusan elhelyezi a kód fregmentet minden egyes metódus hívás előtt, az összes osztályban a JAR fájlban, amelyre érvényes a tartalmazási kritérium.

A próba fordítása egy osztály fájlba történik. Mielőtt végrehajthatnánk a módosított alkalmazást, szükségünk lesz arra, hogy a futtató szkript classpath beállítását módosítsuk esetünkben a következőképpen:

```
java -classpath lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-
1.0.4.jar;..\AdminBean\dist\AdminBean.jar;dist\AdminClient.jar;"C:\Documents and
Settings\Administrator\workspace\probe\bin" com.corsaire.ispatula.Main
```

Az alkalmazás futtatása, és a bejelentkezési művelet, valamint egy rendelési azonosító kiválasztása a következő kiíratást eredményezi:

```
com/corsaire/ejb/Order calling: getBillAddress2 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillCity ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillCountry ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipToFirstName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipToLastName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipAddress1 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipAddress2 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipCity ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipCountry ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getTotalPrice ()D
com/corsaire/ispatula/ClientForm calling: access$100
(Lcom/corsaire/ispatula/ClientForm;Ljavax/swing/event/ListSelectionEvent;)V
com/corsaire/ispatula/ClientForm calling: orderListBoxValueChanged
(Ljavax/swing/event/ListSelectionEvent;)V
com/corsaire/ejb/ManageOrdersBeanRemote calling: getOrder (I)Lcom/corsaire/ejb/Order;
com/corsaire/ispatula/ClientForm calling: populateOrderDetails
(Lcom/corsaire/ejb/Order;)V
com/corsaire/ejb/Order calling: getBillToFirstName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillToLastName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillAddress1 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillAddress2 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillCity ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillCountry ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipToFirstName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipToLastName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipAddress1 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipAddress2 ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipCity ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getShipCountry ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getTotalPrice ()D
com/corsaire/ejb/Order calling: getBillToFirstName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillToLastName ()Ljava/lang/String;
com/corsaire/ejb/Order calling: getBillAddress1 ()Ljava/lang/String;
```

A felhasználó alapján visszakeresett rendelések megértésének céljából a fentiek következő két részletére fókuszálunk: azonnal az autentikáció után, amikor a rendelések listázásra kerülnek, illetve a részletesen megjelenítendő rendelések kiválasztására. Annak érdekében, hogy a metódus aláírásokat tisztábban lássuk, az alábbiakban található egy jobban olvasható konverzió:

```
void ClientForm.populateOrderList()

List ManageOrdersBeanRemote.getOrderIds(String)
```

Majd a megrendelésre való kattintáshoz tartozó kiíratás, melyet a GUI esemény fogadhat:

```
com/corsaire/ispatula/ClientForm calling: access$100
(Lcom/corsaire/ispatula/ClientForm;Ljavax/swing/event/ListSelectionEvent;)V
```

A nyomonkövetés kiíratása a következőképpen fordítva:

```
Order ManageOrdersBeanRemote.getOrder (int)
Void ClientForm.populateOrderDetails (Order)
```

Elemezve a metódusokat és a folyamatot, a következő konklúziókat vonhatjuk le:

- Mivel a bejelentkezési metódus a szerver oldalon String típust ad vissza, ezért lehetséges, hogy ez egy eszköz az állapot tárolásának a kliens oldalon. A getOrderIds híváshoz egy String argumentumra van szükség, mely megerősíti ezt a feltételezést.
- A getOrderIds eljárás egy listát ad vissza és feltehetően csak azok az elemek kerülnek megjelenítésre, amelyek a belépett felhasználóhoz kapcsolódnak. A getOrder eljárás egy Integer típust fogad el paraméterként és egy Order objektumot ad vissza.

A getOrder(int) metódus elsődleges célpont lehet az elérési kontroll helyes implementációjának ellenőrzésére a szerver oldalon.

Dinamikus nyomkövetés AspectJ használatával

A TPTP csomag funkcionalitása nagyon hasonlít az AOP[23] koncepciójához, mely lehetővé teszi a fejlesztők számára, hogy olyan összefésülődéseket definiáljanak, melyeket az alkalmazás különböző részein alkalmazhatnak az osztályok szerkesztése nélkül. Az AspectJ egy elterjedt Java AOP keretrendszer, amely tökéletes a nyomkövetési feladatokra. Reverse engineering[24] célokból egy fontos jellemvonással rendelkezik, mely nem mondható el a TPTP-ről, azaz képes elfogni a mező összefésüléseket.

A következő nézet elkapja a metódus hívásokat (hasonlóképpen, mint ahogyan azt korábban a TPTP példa mutatta) és mező összefésüléseket:

```
public aspect Tracer {
	protected static int callDepth = 0;
	protected static void traceEntry(String str) {
		callDepth++;
		printEntering(str);
	}
	protected static void traceExit(String str) {
		printExiting(str);
		callDepth--;
	}
	protected static void traceInfo(String str) {
		printIndent();
		System.out.println(" [*] " + str);
	}
	private static void printEntering(String str) {
		printIndent();
		System.out.println("--> " + str);
	}
	private static void printExiting(String str) {
		printIndent();
		System.out.println("<-- " + str);
	}
```

23 Aspect Oriented Programming (AOP) – aspektus-orientált programozás

24 Egy adott architektúra, működési elv, vagy algoritmus elemzése és dokumentálása az eredeti tervek ismerete nélkül, pusztán a működés és a tárgykód analizálásán keresztül.

```
    private static void printIndent() {
        for (int i = 0; i < callDepth; i++)
            System.out.print("  ");
    }

    pointcut myClass(): within(com.corsaire..*) && !within(com.corsaire.aop..*);

    pointcut myConstructor(): myClass() && execution(new(..));// Any constructor

    pointcut myMethod(): myClass() && call(* *(..)); // Any method call

    pointcut setter(): myClass() && set(* *); // Field assignment

    before(): myConstructor() {
        traceEntry("" + thisJoinPointStaticPart.getSignature());
    }

    after(): myConstructor() {
        traceExit("" + thisJoinPointStaticPart.getSignature());
    }

    before(): myMethod() {
        traceEntry("" + thisJoinPointStaticPart.getSignature());
    }

    after(): myMethod() {
        traceExit("" + thisJoinPointStaticPart.getSignature());
    }

    before(Object newVal): setter() && args(newVal) {
        if (newVal != null) {
            traceInfo("" + thisJoinPointStaticPart.getSignature() + " = "
                    + newVal);
        }
    }
}
```

A kiemelt szöveg mutatja a mező összefésülésért felelős kódot. Miután a nézet megírása megtörtént, összefésülhető a meglévő JAR fájllal, és egy új JAR fájl kapható kimenetként az ajc parancs és az aspectjrt könyvtár használatával.

```
c:\opt\aspectj1.6\bin\ajc -cp "c:\opt\aspectj1.6\lib\aspectjrt.jar";bsh-2.0b4.jar;pf-
joi-full.jar;lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-1.0.4.jar;AdminBean.jar
TracingAspect\src\com\corsaire\aop\Tracer.aj -inpath AdminClient.jar -outjar
NewAdminClient.jar
```

Az új JAR fájl, a “NewAdminClient.jar” már futtatható és a classpath-ban az aspectjrt-t is tartalmazza:

```
java -classpath c:\opt\aspectj1.6\lib\aspectjrt.jar;bsh-2.0b4.jar;pf-joi-
full.jar;lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-1.0.4.jar;AdminBean.jar;NewAdminClient.jar
com.corsaire.ispatula.Main
```

A programot futtatva és végrehajtva a már jól ismert műveleteket: belépés “bob” felhasználóként, majd az első rendelés kiválasztása egy halom kimenetet eredményez – ideértve az összefűzéseket és a GUI hívásokat. A belépési metódus nyomonkövetése érdekes hozzárendelési műveleteket jelez:

```
--> boolean com.corsaire.ispatula.ClientForm.login(String, String)
  --> String com.corsaire.ejb.ManageOrdersBeanRemote.login(String, String)
  <-- String com.corsaire.ejb.ManageOrdersBeanRemote.login(String, String)
 [*] String com.corsaire.ispatula.ClientForm.accountId = A093633
  --> boolean java.lang.String.equals(Object)
  <-- boolean java.lang.String.equals(Object)
<-- boolean com.corsaire.ispatula.ClientForm.login(String, String)
```

Mindez azt mutatja, hogy a ClientForm bejelentkezési metódusa hívja meg az EJB belépési eljárását, majd egy belső mezőhöz hozzáfűz egy string értéket. Ez erősen arra utal, hogy az állapot a kliensen kerül tárolásra!

Továbbá az látható, hogy a rendelési azonosítók kinyerése a szerverről hogyan történik és, hogyan kerülnek megjelenítésre:

```
--> void com.corsaire.ispatula.ClientForm.populateOrderList()
  --> List com.corsaire.ejb.ManageOrdersBeanRemote.getOrderIds(String)
  <-- List com.corsaire.ejb.ManageOrdersBeanRemote.getOrderIds(String)
  --> Object[] java.util.List.toArray()
  <-- Object[] java.util.List.toArray()
  --> void javax.swing.JList.setListData(Object[])
  <-- void javax.swing.JList.setListData(Object[])
<-- void com.corsaire.ispatula.ClientForm.populateOrderList()
```

Összefoglalva, az információgyűjtés valamint az elemzés során feltérképeztük az alkalmazás végrehajtási folyamatát, megállapításra kerültek a számbavehető támadási formák és azonosítottuk a támadási pontokat. A későbbiekben a megszerzett információk alapján mutatjuk be a demo alkalmazás gyengeségeinek kiaknázását, a kliens oldali biztonsági kontrollok megkerülésétől, egészen a szerver oldali funkciók támadásáig.

Referenciák

Attacking Java Client: A tutorial	https://media.blackhat.com/bh-us-10/whitepapers/deVries/BlackHat-USA-2010-deVries-Attacking-Java-Clients-wp.pdf
Assessing Java clients with the BeanShell	http://research.corsaire.com/whitepapers/060816-assessing-java-clients-with-the-beanshell.pdf
AspectJ	http://www.eclipse.org/aspectj/docs.php
BeanShell	http://www.beanshell.org/manual/contents.html
Eclipse TPTP	http://www.eclipse.org/tptp/
Java Object Inspector	http://www.programmers-friend.org/JOI/

A VirusBuster Kft. összefoglalója 2010 harmadik negyedévének IT biztonsági trendjeiről

Mi történt a harmadik negyedévben az informatikai biztonság területén? Beszámolónkban a trend értékű híreket, adatokat igyekszünk sorra venni, majd a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk a 2010. július-szeptember időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól.

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

Jósolt rémségek, mai veszteségek

Az IT-biztonsági helyzet egyre fokozódik - állítja *Ian Pearson,* aki a Fujitsu megrendelésére írt tanulmányt *"Az élet és ahogyan majd éljük - A felhő alapú számítástechnika várható szerepe egy változó társadalomban"* címmel.

"Nemsokára elég lesz egy csipetnyi intelligens port beszórni a szellőzőrácson ahhoz, hogy lehallgassák az adatainkat - akár mielőtt azok [az irodában alkalmazott] titkosító berendezéshez jutnának. Az információ aztán észrevétlenül a kém vezeték nélküli memóriaegységére kerülhet. - írja a szerző. - Picit okosabb intelligens porral még nyomtatóra jutása előtt módosíthatják a kinyomtatni kívánt dokumentumot. Valószínűleg nem lesz könnyű megtalálni az ilyen kémeszközöket."

Új kártevőgyártási és -terjesztési technikákra számíthatunk. A kórokozók apró darabkákból állhatnak össze, amelyek csak a végrehajtás pontján egyesülnek. Ezeket a rosszindulatú programokat nehezebb lesz felismerni.

Az adott rendszer fizikai jellemzőire alapozott támadási formák jelenhetnek meg. Egy ilyen hálózat-rezonanciás támadás arra épülhet, hogy mennyi idő alatt jut el a jel egyik pontból a másikba. Lehetővé válnak az összehangolt forgalomra és információhullámokra alapozott támadások is.

Tovább súlyosbítja a biztonsági problémákat, hogy hamarosan a web lesz a politikai kampányoknak vagy akár a cégek elektronikus bojkottjának az elsődleges színtere.

"Mindebből következőleg egyre több [szervezet] elsősorban biztonsági megfontolásból dönt majd az IT kiszervezése mellett. Egy cég önmagában ugyanis aligha lesz képes felvenni a kesztyűt az új fenyegetésekkel szemben" - hangsúlyozza Ian Pearson.

De szálljunk alá a jövő felhőiből a jelenbe! Épp elég kárt okoznak a számítógépes bűnözők már ma is, mindenfajta intelligens por nélkül. Évről évre dollármilliókat veszítenek a szervezeteknek a kártevők, a webes és belső támadások miatt.

Átlagosan évi 3,8 millió dollárjába került a kiberbűnözés annak a 45 amerikai szervezetnek, amely részt vett a Ponemon Intézet közelmúltban zárult felmérésében. Elemzésükben a szakemberek igyekeztek minden, a számítógépes bűnözők által okozott kárt felbecsülni: a közvetlen és indirekt, külső és belső költségeket egyaránt. Külső költségnek az ellopott vagy elveszett információ értékét, az üzletkiesést és az anyagi kárt, belsőnek a védekezésre fordított összeget tekintették. Az utóbbi részeként figyelembe vették a készenlét, a felderítés, a vizsgálatok költségét, valamint a problémák elszigetelésére, a helyreállításra, a támadások utáni intézkedésekre költött dollárokat.

A legdrágább belső tevékenységnek a cselekmények felderítése és a helyreállítás bizonyult, míg a külső költségek közül az elvesztett információ értéke vitte el a pálmát.

A kutatásba bevont szervezetek összesen heti 50 incidensnek estek áldozatul, azaz átlagosan mindegyik cég valamivel több mint heti egy sikeres támadást szenvedett el. Az összes kár több mint 90 százalékát webes támadások, rosszindulatú programok vagy dolgozók okozták.

Egy-egy kibertámadás következményeinek felszámolása átlagosan 14 napig tartott, s minden egyes nap 17.696 dollárba került - olvasható a tanulmányban. Ugyanakkor a belső támadások jóval több időt: legalább 42 napot raboltak el a szervezetek életéből.

"Miért sikeresek a hackerek?" - teszi fel a kérdést *John Stewart,* a Cisco biztonsági főnöke egy, a cége által nemrég közzétett tanulmányban. Majd megadja a választ: "Szerencséjük van, türelmesek és tehetségesek. És pénzzel is jobban el vannak látva [mint a másik oldal]". Egyre pontosabban célozzák meg áldozataikat, gondosan ki tudják választani azokat, akiknek hozzáférésük van a megszerezni kívánt adatokhoz.

Hat esztendő alatt 900-nál is több esetet dolgoztak fel a Verizon évről évre kiadott adatbetörési nyomozati jelentései. Az elemzett bűntényeknek áldozatul esett adatrekordok száma meghaladja a 900 milliót.

Nemrég jelent meg a cég 2009-et áttekintő anyaga, amelybe - most első ízben - az amerikai titkosszolgálat (US Secret Service) által gyűjtött információk is bekerültek, így a beszámoló még pontosabb képet fest az adatbetörési frontról. A szakemberek a tavalyi év 141 bizonyított adatbetörését elemezték. A feldolgozott esetekben összesen 143 millió adatrekord került illetéktelen kezekbe.

Kik álltak a 2009-es bűntények mögött? A jelentés szerint:

- 70 százalékban külső támadók,
- 48 százalékban házon belüli elkövetők.

Az esetek

- 11 százalékában üzleti partner,
- 27 százalékában pedig több fél is érintett volt.

Ami az elkövetés módját illeti, az elemzésből kiderül, hogy:

- 48 százalékban jogosultsággal való visszaélés,
- 40 százalékban feltörés,
- 38 százalékban kártevő révén jutottak célba a bűnözők.

Az esetek

- 28 százalékában alkalmaztak félrevezető, manipulatív (social engineering) taktikát, s
- 15 százalékában fizikai támadást.

Egy másik cég, a Trustwave jelentése (Web Hacking Incidents Report) 160, nyilvánosságra került webtámadás következményeit és körülményeit dolgozza fel. Felmérésük talán legfigyelemreméltóbb eredménye, hogy az esetek nem kevesebb, mint 15 százalékában SQL befecskendezéses technikát alkalmaztak a bűnözők. A támadások gyakran azért lehetnek sikeresek, mert a szervezetek rosszul konfigurálják rendszereiket.

Milyen szervezetek kerülnek leggyakrabban a támadók célkeresztjébe? Nos, a tanulmány szerint "legnépszerűbb" a kormányzati szektor, amely a támadások 20 százalékát vonzotta magához. Második helyen - 15 százalékkal - a közösségi portálok és más Web 2.0-s cégek állnak. A bronzérmet a pénzintézetek szerezték meg, a támadások 12 százalékával.

Aggasztó - állapítja meg a Trustwave -, hogy a jelek szerint a cégek nem képesek megfelelően

megvédeni magukat. Nem egyszer még eseménykezelő vagy naplózó eszközük sincs, miközben a számítógépes bűnözők egyre kifinomultabb technológiát vetnek be. A kutatók azt ajánlják a szervezeteknek, hogy kezeljék nyíltabban az őket érő támadásokat. Ha ugyanis titkolóznak, "nem lehet a probléma igazi okát orvosolni".

És milyen tipikus hibákat követnek el biztonságuk rovására az egyéni felhasználók? Nos, egy brit hitelképesség-vizsgáló cég, az Experian felmérése például lehangoló képet fest a jelszóhasználati szokásokról.

Ugyanazt a jelszót használja valamennyi vagy több, általa igénybe vett online szolgáltatáson a szigetországbeli szörfösök több mint fele, akik azt is beismerték: csak felszólításra változtatnak belépési azonosítóikon. A válaszadók 57 százaléka olyan adatot választott jelszóként, amelyet közösségi portálon is közzétett.

Mint a kétezer fős kutatásból kiderült: a jelszóként leggyakrabban választott adatok - a születési hely, idő és az illető valamelyik iskolájának neve - nagy valószínűséggel megjelennek valamely közösségi site-on, hiszen ugyanezek az információk ott vannak a portálokon leggyakrabban közzétett személyi adatféleségek tízes toplistáján.

Érdekes ellentmondás: miközben a válaszadók 18 százaléka jelentetné meg születési helyét közösségi portálbeli profiljában, egy idegennek telefonon csak 3 százalékuk adná meg ezt az információt...

Közösségi kórkép

Korunkban három trend jelenti a legnagyobb kockázatot - állapítja meg a Cisco 2010. félévi összefoglaló tanulmánya. Ezek:

- a mobil és az internetre kapcsolódó eszközök rohamos terjedése,
- a virtualizáció előretörése és végül, de nem utolsósorban
- a közösségi portálok térhódítása.

Az utóbbit illetően a kutatók azt találták: a dolgozók fele a céges rendszabályokra fittyet hányva a munkahelyén is belép az online közösségekbe. Több mint negyedük (27 százalékuk) manuálisan módosította gépén a biztonsági beállításokat, hogy hozzáférjen ezekhez a hálózatokhoz. Sokan játszanak is a portálokon - a „facebookozók” 7 százaléka például napi 68 percet tölt játékkal.

Ha egy online szolgáltatásnak világszerte félmilliárd látogatója van, természetes, hogy a bűnözők előszeretettel veszik célba. Így hát - csakúgy, mint az előző negyedévekben - az utóbbi három hónapban is többször hallhattunk a Facebook sérülékenységeiről, vagy éppenséggel a portálon garázdálkodó kártevőkről.

Különösen nagy port vert fel, amikor kiderült: egy e-mail címet és bármilyen jelszót beírva a Facebook-on megkaphattuk a cím tulajdonosának nevét, képét - feltéve, hogy a cím a félmilliárd felhasználó valamelyikéhez tartozik. Mindez akkor is megtörtént, ha a fiók tulajdonosa megfelelően állította be az adatvédelmi opciókat. A hibát gyorsan kijavították, de nyilván előszeretettel lovagolták meg adathalászok, online csalók - egyáltalán bárki, aki kíváncsi volt: ki is rejtőzik egy ismeretlen e-mail cím mögött.

Ugyancsak figyelmet keltett az eset, amikor hamis "Nem tetszik" alkalmazás indult terjedésnek a Facebook-on. A bűnözők azt használták ki, hogy - sok felhasználó kérése ellenére - a fejlesztők nem tettek "Nem tetszik" gombot tenni a közösségi portálra. Így hackerek hamis "Nem tetszik" programot készítettek, amely féregként felhasználói profilról felhasználói profilra terjedt, s spammelni kezdett.

Levélszemét-özön

Persze az előbb említett Facebook-féreg észrevehetetlenül piciny forrással járult hozzá csupán az elmúlt negyedévben is hömpölygő spam-áradathoz. "És végül is mit számít egy kis spam? - mondják sokan. - Legfeljebb töröljük." Nos, mi sem bizonyítja jobban az efféle okoskodás veszélyét, mint *Szappanos Gábornak,* a VirusBuster víruslabor-vezetőjének egy nemrég megjelent cikke. A szakember egy, a nyári labdarúgó világbajnokságot meglovagoló spamkampányól közölt részletes elemzést a *Virus Bulletin* című rangos nemzetközi szakfolyóirat októberi számában. Kimutatta: az az üzenet, amely a felszínen, a laikus felhasználó számára egyszerű levélszemétnek tűnt, valójában a hírhedt Bredolab kártevőt is terjesztette, mégpedig a még ennél is elhíresültebb Gumblar terjesztő-architektúra bevetésével.

És hányféle spam éri el a magyar felhasználókat is nap, mint nap! Szeptember végén például sajtóközleményben figyelmeztette a felhasználókat a VirusBuster: valóságos spamkitörés zúdult hazánkra. Ötezer eurós fizetés és jutalék részmunkaidős otthoni munkáért - ezt ígérte egy angol nyelvű, tömegesen terjesztett üzenet.

"Aki válaszolt egy ilyen levélre, semmit sem nyerhetett, de nagyon is sokat veszíthetett - hangsúlyozta *Stange Szilárd,* a VirusBuster technológiáért felelős termékmenedzsere. - Mert mi is a spammerek célja? Először is arról akarnak meggyőződni, léteznek-e az e-mail címek, amelyeket megszórtak. Ha válaszolunk, megerősítjük címünk helyességét, s az felkerül a számítógépes bűnözők validált címlistájára. Egy ilyen lista komoly értéket képvisel a feketepiacon, s a rajta lévő címzettek sok-sok kéretlen levélre számíthatnak."

Rejlett azonban a szeptemberi spamkitörésben még egy, az előbbinél veszedelmesebb csapda is. "Régen ismert trükkhöz folyamodtak a szerzők: ígérjünk sok pénzt kevés munkáért és kérjünk önéletrajzot a pályázóktól. Aki gyanútlanul elküldi a CV-jét, annak az adataival aztán sokféleképpen élhetnek vissza a bűnözők" - magyarázta el a szakértő.

Kemény dió volt ez a levéláradat a spamszűrőknek is. Az angol nyelvű szöveg ugyanis - bár néhány ponton nem volt igazán angolos - túlságosan hasonlított egy igazi állásajánlatra. Ha tehát egy szűrőt betanítottak arra, hogy ne engedje tovább, akkor könnyen lehet, hogy a címzetthez egy várva várt valódi munkalehetőségről szóló hír sem jutott el.

Segítséget jelenthet ilyen esetekben a fehérlista, vagyis az olyan e-mail-küldők jegyzéke, akikben garantáltan megbízhatunk. Ha egy spamszűrő fehérlistát is használhat, akkor kisebb terheléssel kell megbirkóznia, hiszen a tisztának tekintett forrásból érkező leveleket átengedheti, ugyanakkor kisebb az esély arra, hogy értékes üzeneteket tévesen kiszűrjön a rendszer. Ez utóbbi a feladónak és a címzettnek egyaránt fontos előny.

Régóta eredményesen használják világszerte a levelezés szűrésére a Spamhaus rosszindulatú e-mail szervereket tartalmazó feketelistáját. Nos, nemrég a nemzetközi nonprofit szervezet a jóindulatú, azaz megbízhatónak ítélt levelezőszerverekről is listát állított fel. A fehérlistára például bankok, ügyvédi irodák, légitársaságok, egészségügyi intézmények, kormányszervek, valamint számlázó, e-kereskedelmi, online banki tranzakció-értesítő és helyfoglaló rendszerek mail-kiszolgálói kerülhetnek fel, kizárólag meghívásos alapon.

Ugyancsak fontos a spam elleni küzdelemben a törvény szigorának alkalmazása. Reményteli ebben a tekintetben, hogy egy amerikai kerületi bíróság a közelmúltban véglegesen a Microsoft tulajdonába adott 276 internetes domaint. A szóban forgó címekről irányította a Waledac számítógépes gang a botnetjébe a világ minden táján beszervezett sok százezer spamküldő PC-t. A jogi lépéssel megnyílt az út a Microsoft előtt, hogy fellépjen azokkal az Egyesült Államokban regisztrált domainekkel szemben, amelyeket bűncselekmények elkövetésére használnak.

Virtuális támadás, fizikai célpont

Az eddigiekben olyan jelenségekről szóltunk, amelyek már hosszú évek óta folyamatosan gondot okoznak. Az elmúlt negyedév kártevői között azonban volt egy, amely - mondhatni - új fejezetet nyitott a számítógépes bűncselekmények (és hadviselés) történetében, legalábbis annak nyilvánosságra került köteteiben.

Porondra lépett ugyanis a Stuxnet, a világ első ipari folyamatirányító számítógépekre specializált kártevője. Nemigen akadt ennyire összetett, kifinomultan tervezett kórokozó a számítógépes vírusok történetében. Négy olyan sérülékenységet vett célba, amelyet csak nemrég fedeztek fel és foltoztak be. Ezt kihasználva többek között pendrive-okon és Windows állománymegosztásokon terjedt. Kutatók kimutatták: a féregnek különös képessége van a Siemens által fejlesztett ipari folyamatirányító alkalmazások megfertőzésére. Egy ilyen kártevő olyan, mint egy célra vezetett rakéta: internet nélkül is megtalálja és megsemmisíti célpontját. Egy folyamatirányító rendszerbe való beavatkozással a Stuxnet tervezői súlyos következményekkel járó szabotázsakciót követhetnek el.

Júliusban a Microsoft közzétette a Stuxnetnek áldozatul esett gépek földrajzi eloszlását. Érdekes módon úgy tűnt: Irán lett a fertőzések epicentruma. Felmerült az a feltételezés is, hogy a kártevőt egyetlen konkrét célpont: az iráni Bushehr atomerőmű megtámadására tervezték.

Elemzést tett közzé a támadássorozatról az Európai Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA). "A Stuxnet valódi paradigmaváltás, a kártevők új kategóriája, új dimenziója - és nemcsak összetettsége, a mögötte álló kifinomult mérnöki munka miatt - jelentette ki *Udo Helmbrecht* vezérigazgató. Afféle első csapásnak tekinthetjük, az egyik első jól szervezett és előkészített támadásnak, amelyet jelentős ipari célpontok ellen intéztek. Ennek komoly kihatása van arra, hogyan kell védenünk egy ország kritikus információs infrastruktúráját a jövőben. ... Most, hogy a Stuxnetben alkalmazott elvek nyilvánosságra kerültek, további hasonló támadásokra számíthatunk. Valamennyi, biztonságban érintett fél szoros együttműködésére, jobb és összehangoltabb stratégiák kidolgozására van tehát szükség."

Összefogás, gyors reagálás

Önmagában egyetlen EU-tagállam, hardver- vagy szoftvergyártó, számítástechnikai katasztrófavédelmi csapat (Computer Emergency Response Team, CERT) vagy bűnüldöző szerv sem képes egy ilyen bonyolult támadás kivédésére - hangsúlyozta közleményében az ENISA. Ennek megfelelően az ügynökség 2011-ben támogatást nyújt az ipari folyamatirányító rendszerek védelmét szolgáló elvek, eljárások kimunkálásához, s elemezni fogja, milyen mértékben függenek az egyes kritikus szektorok az információs és kommunikációs technológiáktól.

Az ENISA aktívan segíti a nagy kiterjedésű támadások elleni összehangolt védekezést, s felkérése esetén vállalja, hogy koordinálja a megfelelő ellenintézkedéseket. Bejelentették: az ügynökség vezetésével első ízben pán-európai kritikus információs infrastruktúra-védelmi gyakorlatot tartanak. A 'CYBER EUROPE 2010'-ben az EU-tagállamok mellett három EFTA-ország is részt vesz.

Ugyanakkor a Fehér Ház a webes autentikáció megerősítéséért, az online azonosítás ellenőrzésének szigorításáért szállt síkra. Amerikai kormányzati szakértők *"Megbízható azonosítás a kibertérben - Nemzeti stratégia" (National Strategy for Trusted Identities in Cyberspace, NSTIC)* címmel készítettek 39 oldalas vitaanyagot. A dokumentum egy úgynevezett "azonosítási ökorendszer" létrehozása mellett érvel. Ez olyan, együttműködésre épülő környezet lenne, amelyben a "a természetes személyek, szervezetek és gépi eszközök megbízhatnak egymásban, mert a hiteles források gondoskodnak digitális azonosításukról, illetve annak igazolásáról".

Az ökorendszer három fő rétegből állna: a környezet szabályait rögzítő felügyelő rétegből, a

szabályokat alkalmazó és érvényre juttató vezérlő rétegből, végül a szabályoknak megfelelő tranzakciók lefuttatásáért felelős végrehajtó rétegből.

Az NSTIC *Obama* elnök tavaly májusi netpolitikai elemzése nyomán készült - írta egy blogcikkben *Howard Schmidt,* az Egyesült Államok kiberbiztonsági koordinátora. Ha a tervek megvalósulnak, a polgároknak "nem kell többé egyre több és több - ráadásul esetleg nem is biztonságos - felhasználónév-jelszó kombinációt fejben tartaniuk, hogy belépjenek a különböző online szolgáltatásokba" - fogalmazott a magas rangú kormánytisztviselő, aki szerint a dokumentumot várhatóan ősszel véglegesítik.

És mit tegyenek a vállalatok? A Cisco tanulmánya szerint afféle gyors reagálású hadtestet kell felállítaniuk, mégpedig olyan szakemberekből, akiknek megfelelő rendőrségi kapcsolataik vannak, s akik tudják, hogyan kell bizonyítékot szolgáltatni a bűnüldöző szervek számára. A rendőrséggel való kapcsolatokat gondosan fel kell építeni, fenn kell tartani - nem szabad megvárni, míg egy támadás bekövetkezik.

Bővülő biztonsági piac

Mindezek hallatán érthető, hogy az IT-biztonság azon kevés ágazat közé tartozik, amely a globális gazdasági válság közepette is növelni tudta-tudja árbevételét.

"A biztonsági szegmens továbbra is a vállalati szoftverek világpiacának leggyorsabban növekvő területei közé tartozik" - állapította meg *Ruggero Contu,* a Gartner vezető elemzője. Idén a szektor több mint 16,5 milliárd dolláros volument érhet el - állítják a kutatók. Ha az előrejelzés beválik, az ágazat árbevétele 11,3 százalékkal nő a 2009-es 14,8 milliárd dollárhoz képest. A szakemberek mintegy 4 százalékkal nagyobb növekedésre számítanak tehát, mint 2008 és 2009 között, amikor is mindössze 7 százalékkal bővült a biztonsági szoftverpiac.

Csakúgy, mint eddig, az ágazat legnagyobb szeletét idén is a fogyasztói szoftverpiac adja, 4,2 milliárd dollárra prognosztizált árbevétellel. A dobogó második helyére a kutatók szerint a vállalati végpont-védelem kerül. Ez utóbbi szektorban az év végéig 3 milliárd dolláros forgalomra számítanak.

Hasonló eredményekre jutottak egy másik piackutató társaság, a Canalys elemzői. Mint mondják, a gazdaság lassan beindul, ismét van költségvetés, a cégek frissítik rendszereiket. Így a vállalati biztonsági világpiacon idénre 15 milliárd dolláros volument, s 13,8 százalékos növekedést prognosztizálnak. Utalnak arra, hogy az első negyedév forgalma 15,2 százalékkal haladta meg a tavalyi év megfelelő időszakáét.

A Canalys szakértői úgy becsülik: az idei árbevétel 33,6 százaléka - mintegy 5 milliárd dollár - realizálódik majd Európában. Az oroszlánrész - 46,4 százalék, azaz közel 7 milliárd dollár - várhatóan Észak-Amerikának jut. A 2010-es növekedés jó része az infrastruktúra biztonsági eszközök értékesítéséből származhat - ezek teszik ki a szektor végfelhasználói vásárlásainak 48,7 százalékát.

Folytatódik a szegmens növekedése 2011-ben is. Jövőre a Canalys 9,2 százalékos bővülést, 16,3 milliárd dolláros forgalmat jósol.

Folt hátán folt

Bár a korábbi időszakra vonatkozik, csak a harmadik negyedévben jelenhetett meg az adat: csaknem annyi sérülékenységet regisztráltak 2010 első felében, mint a teljes tavalyi évben együttvéve.

Mint a Secunia tanulmányában olvasható, az átlagos végfelhasználói PC-ken legelterjedtebb 50 programcsomagon összesen 380 rést találtak. Ez a végeredmény nem kevesebb, mint 89 százaléka a 2009-es esztendő egészére vonatkozó adatnak. Az egyes gyártók termékeiben regisztrált sérülékenységek számát tekintve az idei első félévben az Apple végzett az első helyen. Az almás

céget az Oracle és a Microsoft követi a dobogón.

Mind nagyobb fenyegetést jelentenek - az operációs rendszerekkel szemben - a külső cégek által szállított alkalmazások rései. Egy átlagos, 50 programot futtató PC-n 26 Microsoft-terméket és 24, más gyártótól származó szoftvert találunk. Mégis, a felmérés szerint az utóbbiakban együttvéve 3,5-szer több sérülékenységre számíthatunk, mint a redmondi óriás programjaiban. A Secunia úgy becsüli: az idei év egészét tekintve ez az arány 4,4-re nő.

Nehezíti a hibák javítását, hogy a PC-ken átlagosan 13 különböző szoftverfrissítési mechanizmus működik.

A tipikus kliensgépet fenyegető sérülékenységek száma 2007 és 2009 között 220-ról 420-ra emelkedett. A Secunia most azt jósolja: idén ez az adat 760-ra szökik, vagyis ismét csaknem megduplázódik majd.

Így hát jó okkal kaptak szép számú biztonsági frissítést a legelterjedtebb szoftverek az elmúlt hónapokban is. A következőkben röviden, időrendben a legfontosabb foltokat tekintjük át.

Július

- Július 13-i foltozó keddjén négy biztonsági frissítést bocsátott ki a Microsoft. A foltok összesen öt sérülékenységet orvosoltak. A négy foltból három "kritikus", egy pedig "fontos" minősítést kapott. A Windowshoz és az Office-hoz egyaránt két-két biztonsági frissítés szolgált.
- Negyedéves menetrendszerű biztonsági frissítésével összesen 59 biztonsági rést tömött be szoftverein az Oracle. Közel a hibák harmada - szám szerint 21 - a Solarisban volt. Mint ismeretes, a vállalati operációs rendszer a Sun felvásárlásával került az Oracle-hez. Hat sérülékenységet orvosolt a szoftverház a népszerű adatbázis-szerverben (Database Server). Számos más programot is érintett a frissítés. Ezek: a Secure Backup, a TimesTen In-Memory Database, a Fusion Middleware, az Enterprise Manager, az E-Business Suite, a Supply Chains termékcsomag és a PeopleSoft Enterprise.
- Összesen 14 - köztük nyolc kritikusnak minősített - sérülékenységet orvosolt a Firefox 3.6.7-es változatának kibocsátásával a Mozilla. Különösen veszélyes rések tátongtak a PNG képek, valamint a memória kezelésében.
- Az Apple az iTunes szoftver windowsos változatát javította. Az új, 9.2.1-es verzió egy puffer-túlcsordulási sérülékenységet szüntetett meg.

Augusztus

- Soron kívüli biztonsági frissítéssel orvosolta a hónap elején a Microsoft a Windows Shell kritikus sérülékenységét. A hackerek már támadták a rést, melyet a parancsikonok feldolgozásában fedeztek fel.
- Menetrendszerű foltozó napján, augusztus 10-én összesen 34 sérülékenység megszüntetésére 14 biztonsági frissítést bocsátott ki a Microsoft. A foltok közül nyolc "kritikus", hat pedig "fontos" minősítést kapott. A Windowshoz 12, az Office-hoz két javítócsomag látott napvilágot. Folt került a Microsoft .NET Frameworkre és a Silverlightra is.
- Frissült a windowsos QuickTime. Az Apple új verzió kibocsátásával orvosolta a videólejátszó egy kritikus sérülékenységét, amely távoli kódvégrehajtásra adott módot. Az érintett operációs rendszerek a következők voltak: Windows 7, Vista, valamint XP SP 2 és 3. A probléma Mac OS X rendszereken nem állt fenn.
- Mobil operációs rendszerét, az iOS-t ugyancsak befoltozta az almás cég. Egy olyan sérülékenységet orvosolt, amelyet elterjedten aknáztak ki a legújabb iPhone felszabadítására (azaz arra, hogy a készüléken az Apple által nem engedélyezett alkalmazásokat is futtatni lehessen). Az augusztusi operációsrendszer-verziók: iPhone-ra és iPod Touch-ra az iOS 4.0.2-es, iPadre az iOS 3.2.2.

- Expressz biztonsági frissítést bocsátott ki augusztus 19-én az Adobe. A következő szoftverek kaptak foltot: Reader 9.3.3 (Windows, Macintosh és Unix platformon), Acrobat 9.3.3 (Windows és Macintosh platformon), Reader 8.2.3 (valamennyi platformon), Acrobat 8.2.3 (valamennyi platformon), Flash Player 10.1.53.64 (valamennyi platformon).

Szeptember

- A hónap elején összesen 13 kritikus rést tömött be az iTunes windowsos kiadásán az Apple. Valamennyi hiba a program nyílt forráskódú WebKit böngészőmotor-komponensében volt, s rosszindulatú weblap megnyitásakor távoli kódvégrehajtásra adott lehetőséget. Ugyanezeket a sérülékenységeket július végén a Safari 5.0.1-ben és 4.1.1-ben már javította az Apple.
- Megjelent a Google böngészőjének új kiadása. Az első bétaváltozat megjelenésének második évfordulóján Windows, Mac OS X és Linux platformra egyaránt kibocsátott Chrome 6-ossal 17 sérülékenységet is orvosolt a keresőóriás.
- Felfrissítette böngészőjét az Apple is. Az új kiadású Safari Windows alatt három, OS X alatt két kritikus rést tömött be.
- Ugyancsak biztonsági frissítéssel rukkolt ki a Mozilla. A Firefox 3.6.9 nem kevesebb, mint 14 sebezhetőséget hárított el, köztük 10 kritikusat.
- Kilenc biztonsági frissítést bocsátott ki foltozó keddjén, szeptember 14-én a Microsoft. A foltok összesen 11 sérülékenységet orvosoltak, s közülük négy "kritikus", öt pedig "fontos" minősítést kapott. A Windowshoz nyolc, az Office-hoz két biztonsági frissítés szolgál.
- Kibocsátotta a QuickTime 7.6.8-as változatát, s ezzel két kritikus rést tömött be médialejátszóján az Apple.
- Médialejátszót javított az Adobe is: már támadták a hackerek a Flash Playernek azt a sérülékenységét, amelyet megszüntetett a cég.
- Szeptember végén soron kívüli javítócsomaggal tömte be a Microsoft az ASP.NET röviddel azelőtt nyilvánosságra került rését, amely ugyancsak ostrom alatt állt.

"Kiemelkedő" kártevők

Melyek voltak egyébként az elmúlt negyedév leggyakoribb kártevői a magyar neten? Nos, a VirusBuster folyamatosan nyilvántartást vezet az észlelt károkozókról. A cég szakemberei kiértékelik a cég házon belüli, illetve különböző helyeken működtetett levelezésvédő rendszereinek "fogását", figyelik a freemailes levelek által hordozott vírusokat. Az adatokból hónapról hónapra toplistát készítenek, s ezek a havi statisztikák a cég honlapján is megjelennek (http://www.virusbuster.hu/labor/virus-toplista). A mintaforrásokat súlyozottan összesítve a 2010. július-szeptember időszakra a jobb oldalon látható kártevő-gyakorisági lista állt elő.

	Kártevő	Részesedés
1	JS.Redirector.J	16.52%
2	Trojan.Agent.YHJN	15.51%
3	Trojan.Oficla.BNE	13.84%
4	Trojan.Oficla.BOH	8.76%
5	TrojanSpy.Zbot.AFON	6.58%
6	JS.Redirector.K	6.54%
7	Backdoor.Bredolab.DJI	5.75%
8	Trojan.Bredolab.CSQ	4.88%
9	Backdoor.Nepoe.IF	3.08%
10	Trojan.Oficla.BQR	2.50%
	Egyéb:	16.05%

"Tízes toplistánkon öt helyet két botnet, illetve az általuk terjesztett két kártevőcsalád foglalta el: a Redirector és az Oficla. Mindkettő jellemzően trójaiakat tölt le. Az előbbi általában Bredolab-, az utóbbi ZBot-variánsokkal kedveskedik a felhasználóknak" - fűzte az adatokhoz *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője.

Mindezzel korántsem állunk egyedül.

"Világszerte számtalan sebezhető gépet kerítettek hatalmukba a bűnözők. A feltört PC-kről azután bármikor indíthatnak online támadást." Ez a nyilatkozat már *Jon Ramseytől,* a SecureWorks cég technológiai vezetőjétől származik. A SecureWorks kutatói azt vizsgálták: az egyes országokban a PC-k átlagosan mekkora hányadát tették zombivá, azaz szervezték a tulajdonos tudtán kívül robothálózatba - botnetbe - a hackerek.

Nos, a nemrég közzétett tanulmány szerint a legelzombisodottabb ország az Egyesült Államok, ahol a kutatás hathónapos ideje alatt minden ezer PC-ről 1600 támadást indítottak. Nagy-Britannia - 107 támadás/1000 gép aránnyal - az előkelő ötödik helyre került. Legtisztábbnak India mutatkozott: itt ezer gépre csak 52 támadás jutott.

Egy másik biztonsági cég, az M86 Security a botnet-üzemeltetők után nyomozott. Miután a kínai kormány a közelmúltban lecsapott a számítógépes bűnözőkre, több gang más bázis után nézett, s a jelek szerint nem egy közülük Oroszországban lelt menedéket - állítják a vállalat szakemberei, akik két orosz regisztrátornál egyetlen hónap alatt ötezer új spam domaint fedeztek fel. Orosz szolgáltatóhoz költözött többek között a Zeus botnetet működtető társaság is. Az Oroszországba újonnan betelepült bandák főként spamkampányokban, online kaszinókban és gyógyszer-forgalmazásban érdekeltek.

Napjaink elterjedtebb kártevőit alkotóik weboldalakon keresztül (is) folyamatos frissítik. A kártevők felismerésének biztosítása érdekében más víruslaborokhoz hasonlóan a VirusBuster is folyamatosan nyomon követi ezeket a webhelyeket. A gyakori frissítések miatt természetesen csak generikus felismerési módszerekkel kezeljük őket, az utánkövető feldolgozás nem szolgálná a felhasználók érdekeit.

Alábbi táblázatunk július-szeptember legaktívabb kártevő-szóró domainjeit foglalja össze. Láthatóan az Egyesült Államok, Kína és Brazília megőrizte előkelő helyét a terjesztő országok között.

	Domain	**Földrajzi hely**	**Fájlok száma**	**Kártevő-család**
1.	nb.host127-0-0-1.com	Shalimar, USA	742	Swizzor
2.	nb.host192-168-1-2.com	Shalimar, USA	517	Swizzor
3.	screenblaze.com	Houston, USA	385	Trojan.DL.Delphi.BSO
4.	fileave.com	Omaha, USA	368	Worm.DR.Rebhip, JS.Redirector, JS.Wonka, JS.IFrame
5.	nguwang.com	Peking, Kína	291	Trojan.DR.StartPage
6.	hpg.com.br	Brazília	247	Banker, Banload
7.	uol.com.br	Rio de Janeiro, Brazília		
8.	110mb.com	Montreal, Kanada	182	Trojan.Gogel, Banload, Banz
9	dominiotemporario.com	Brazília		
10.	188.65.74.161	Klagenfurt, Austria		

A VirusBuster Kft.-ről

A több mint 15 éves szakmai tapasztalattal rendelkező, kizárólag magyar tulajdonú VirusBuster Kft. (www.virusbuster.hu) 1997 óta nyújt teljes körű vírusvédelmi és biztonságtechnikai megoldásokat szinte minden platformon a magyar és a külföldi piac számára. A Kft. termékei számos magyar és nemzetközi független teszten kaptak kitűnő minősítést. A cég fő terméke, a VirusBuster Professional több alkalommal szerezte meg a "Virus Bulletin 100%" díjat, a "Checkmark Anti-Virus Level One" és "CheckVir" elismerést, valamint az ICSA Labs nagy nemzetközi presztízsű "Desktop/Server Anti-Virus Detection" minősítését, majd 2007-ben és 2008-ban elnyerte az ICSA Labs "Desktop/Server Anti-Virus Cleaning" tanúsítványát. 2008-ban a cég megszerezte az OESISOK tanúsítványt, mely azt igazolja, hogy egy alkalmazás tökéletesen együttműködik a vezető piaci fejlesztők –- a Cisco, a Juniper, a NORTEL, a 3Com, az F5 –- hálózati eszközeivel, illetve a hálózatok védelmét szolgáló, a csatlakozó végpontok "egészségét" ellenőrző NAP, NAC és TNC rendszerekkel.

A VirusBuster világszerte elismert szakemberei rendszeres előadói hazai és nemzetközi konferenciáknak. Bozsó Julianna, a cég ügyvezető igazgatója az Informatikai Vállalkozások Szövetségétől (az IVSZ-től) 2008-ban elnyerte az "Év Informatikai Cégvezetője" díjat.

A Kft. 2003-ban "Év innovatív üzleti megoldása", 2004-ben pedig "IT Reménység" díjban részesült. Két ízben is megkapta a cég az IVSZ-től a "Minősített Szoftver Exportőr" címet és 2005-ben megszerezte az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási tanúsítványt. A VirusBuster webáruháza 2009-ben kiérdemelte a "Fair Business" minősítést, s ugyanebben az évben a cég Üzleti Etikai Díjat kapott.

Elérhetőségeink

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

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937