Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2010. I. negyedéves jelentés

Tartalomjegyzék

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2010. évi I. negyedéves jelentését.

Ez az éves jelentés 2010. legfontosabb IT- és hálózatbiztonsági momentumait gyűjtötte egybe a leggyakoribb szoftversérülékenységektől kezdve a web sérülékenység keresőkről szóló tanulmányon át a VirusBuster Kft. összefoglalójáig a 2010. I. negyedévének informatikai biztonsági trendjeiről.

Az elmúlt év jelentős eseményeihez tartoznak még sajnos – a szoftversérülékenységeken kívül – a tavalyi év internetbiztonsági incidensei és a káros szoftverek. A Nemzeti Hálózatbiztonsági Központ jelentése külön fejezetet szentelt a világ második legnagyobb botnetévé vált Pushdo szoftver analízisének és a terjedéséről szóló tanulmánynak.

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 felkészülésükben.

Budapest, 2010. április

A Nemzeti Hálózatbiztonsági Központ (PTA 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

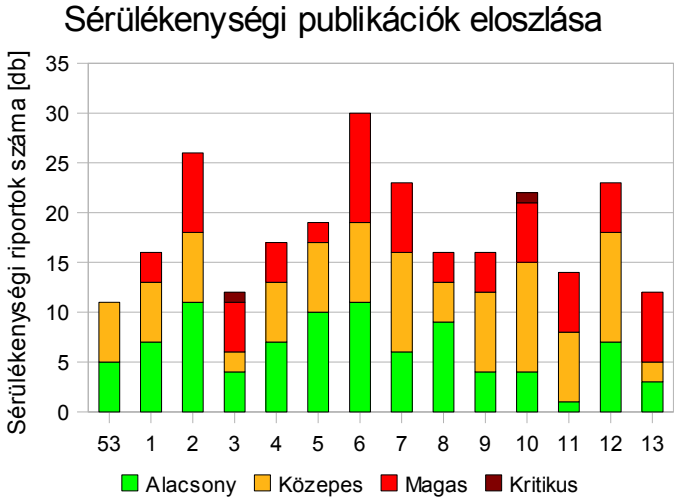
ügyvezető igazgató

Szoftver sérülékenységek

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

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ** a 2010. 1. negyedéve során 257 **db szoftver-sérülékenységi információ**t publikált, amelyekből 89 db alacsony, 95 db közepes, 71 db magas és 2 db kritikus kockázati besorolású.

A negyedév során riportolt sérülékenységi információk havi eloszlása, az egyes hónapok összesített értékei kismértékben ingadozóak, de összességében mérvadó eltérést nem mutatnak.



A negyedév során kiadott sérülékenységi publikációk közel 30%-a magas és/vagy kritikus kockázati besorolású. A legnagyobb veszélyt ezek jelentik, mivel ezek mind széles körben elterjedt és használt alkalmazásokat érintenek, továbbá távoli hozzáféréssel kihasználhatóak.

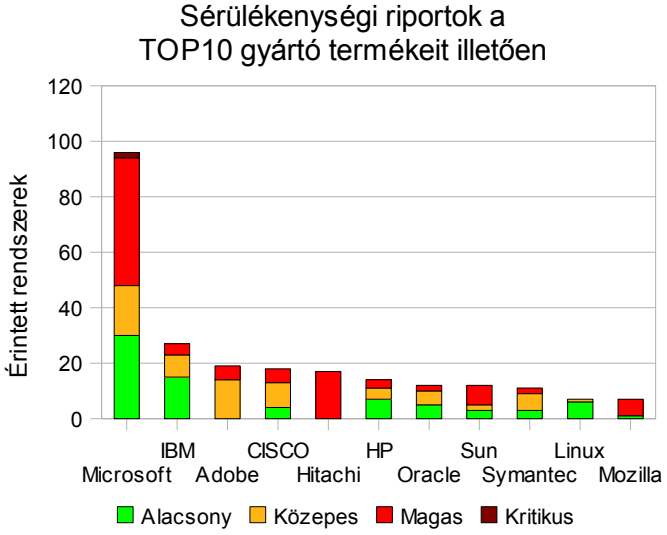
Ezen belül is a legnagyobb károk okozására a kritikus sérülékenységek alkalmasak, melyek kapcsán Központunk ebben a negyedévben összesen 2 ízben adott ki sérülékenységi tájékoztatót támogatott szervezetei részére, továbbá tett közzé publikációt weboldalán:

- Microsoft Internet Explorer sérülékenységek – 2010. január 22.
- Internet Explorer nem részletezett kód futtatási sérülékenység – 2010. március 10.

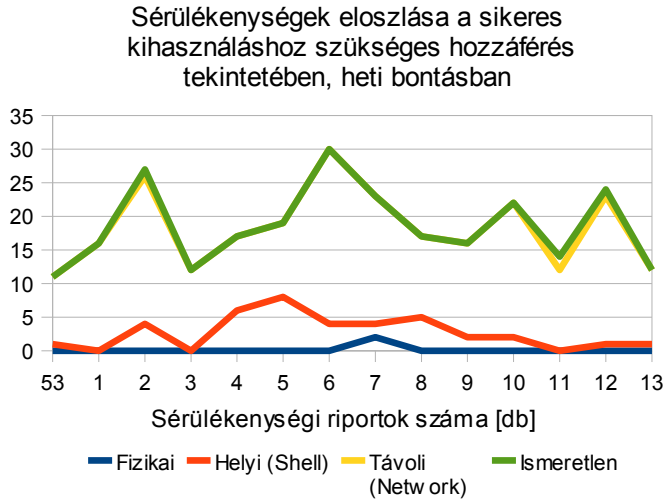
Az előző negyedévekhez hasonlóan az egyes gyártók termékei kapcsán készült kimutatást még mindig a Microsoft (MS) vezeti.

Nagyszámú érintettségük mellett érdemes még más szempontból is megvizsgálnunk a Microsoft termékeinek sérülékenységeit, hiszen az ezek által érintett szoftverek 50%-a kritikus vagy magas kockázati besorolású sérülékenységek kapcsán került regisztrálásra.

Kritikus és magas kockázati besorolású sérülékenységek terén a Hitachi, Sun és Adobe termékek is kimagaslóan nagy százalékos értéket mutatnak, bár ezek gyakorisága jóval alacsonyabb.



Mindezektől függetlenül, fontos, hogy az esetleges sérülékenységek kihasználásával bekövetkező incidensek száma és az általuk okozott károk mértéke jelentősen csökkenthető, ha a használt szoftvereket rendszeresen a kiadott aktuális frissítésekkel telepítve használjuk.

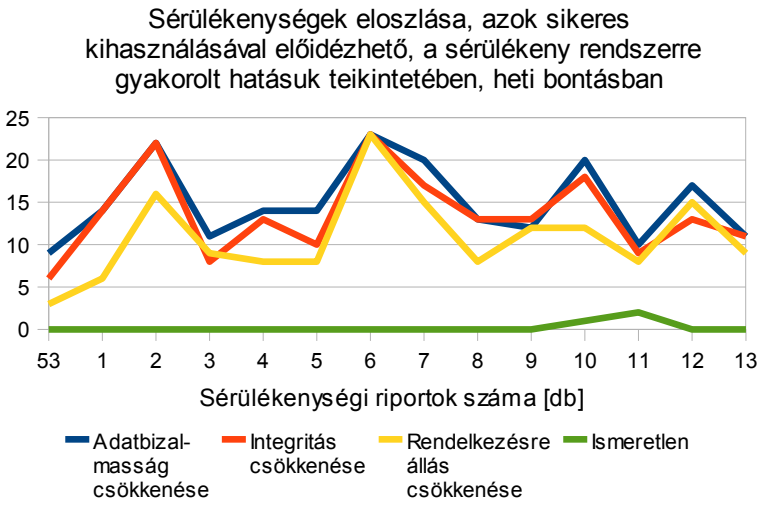


Sérülékenységeket kihasználva támadást intézni adott rendszer ellen legkönnyebben távoli kapcsolat használatával lehet, és a grafikonon is jól látszik, hogy a távoli kapcsolaton keresztül kihasználható sérülékenységek vannak jelen a legnagyobb számban.

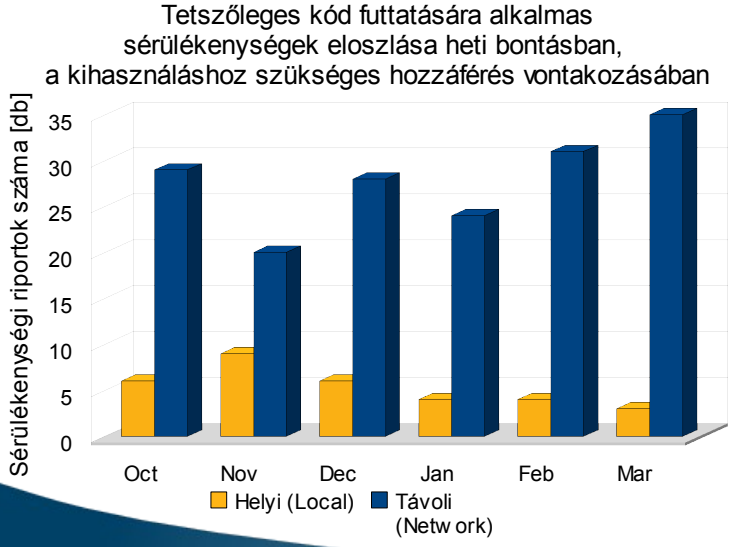
Viszont, ha rendszereinket rendszeresen frissítve használjuk, elkerülhetjük – de mindenképp csökkenthetjük – az infrastruktúrán és az azon tárolt adatok nem kívánt kompromittálódását vagy annak esélyét.

Egy sikeresen lefolytatható támadás esélyét tovább növelik a kihasználáshoz szükséges - az interneten publikusan elérhető - előre elkészített kódok, kód-részletek..

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



A sérülékenységek eloszlását a rendszerre gyakorolt hatásukkal együtt ábrázoló grafikonon jól látszik, hogy a görbék megközelítőleg ugyanazt a tendenciát követik. Ennek oka az, hogy az egyes sérülékenységek kihasználásával sikeresen lefolytatott támadás által, az adott rendszer több szempontból is kompromittálható.



A tetszőleges kód futtatására alkalmas sérülékenységek kihasználása által képesek a támadók a legnagyobb károk okozására.

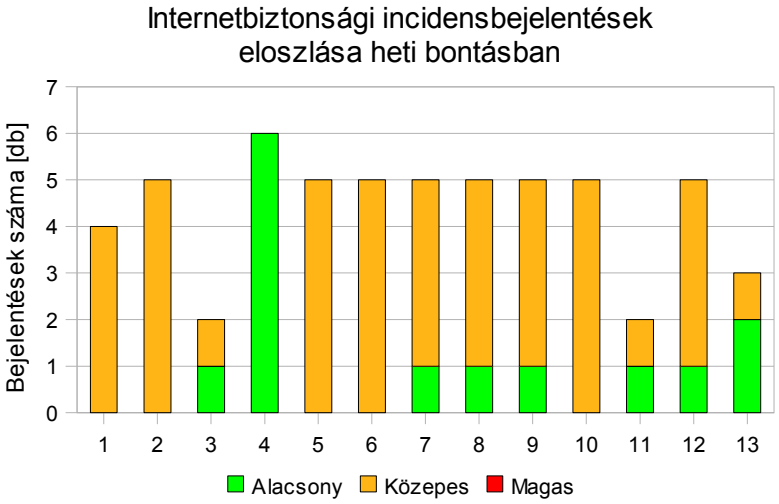
Az ilyen jellegű sérülékenységek száma 2010. 1. negyedévében 101 volt, amely közel 40%-a a periódusban regisztrált sérülékenységeknek.

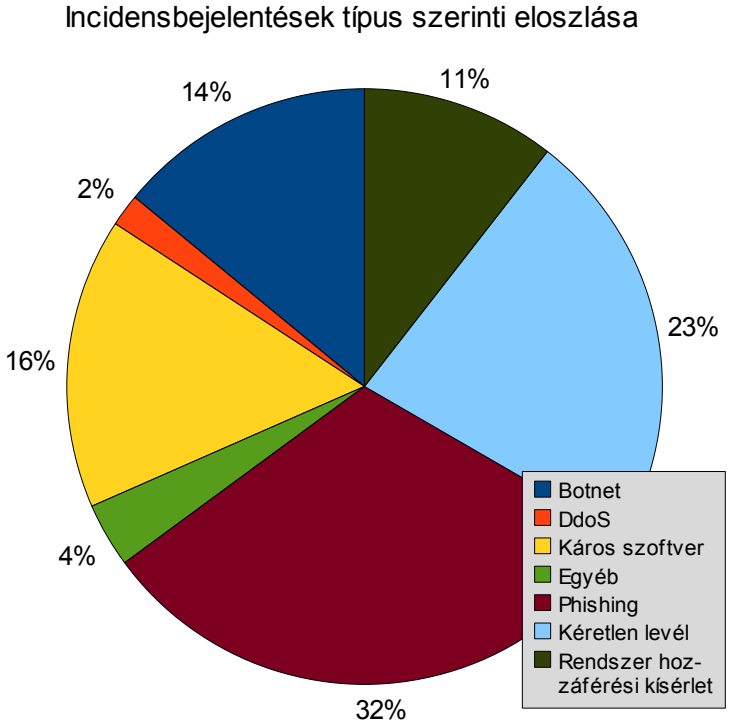
Internetbiztonsági incidensek

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 során összesen **57 db incidens bejelentést** regisztrált és kezelt, ebből 14 db alacsony és 43 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 első negyedévében legnagyobb számban adathalász tevékenység (32%), spam tevékenység (23%) és káros szoftverek terjesztése (16%) kapcsán érkeztek bejelentések, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatok bejelentéseit.

A bejelentések több mint 90%-a hazai forrású káros tevékenységgel vagy tartalommal volt összefüggésben, és túlnyomó részt külföldi partnerszervezetektől érkezett.

Web sérülékenység keresők: segédeszközök vagy játékszerek?

Egy web alkalmazás sérülékenység vizsgálatának manuális végrehajtása igen bonyolult és kimerítő folyamat. Tesztelési szempontból a folyamat automatizálását örömmel fogadták, ezért manapság sok kereskedelmi és nyílt forrású eszköz érhető már el. A nyílt forrású eszközök gyakran kifejezetten a manuális tesztelés támogatására készülnek. Ezt az egyetlen feladatot igen jól végre is hajtják, vagy a grafikus felhasználói felület (GUI) és a riporting funkciók (pl. W3AF) számos egyéb feladataival kombinálva. Ezzel szemben a kereskedelmi web sérülékenység keresők, mint amilyenek például az IBM Rational Appscan, HP Webinspect, Cenzic Hailstorm és az Acunetix Web Vulnerability Scanner, a „minden egy helyen" elv szerint tervezett automatizált tesztelő eszközök, melyekkel időt lehet megtakarítani és az egyes vizsgálatok kiterjeszthetőek. A web alkalmazás sérülékenység keresők alapvetően egy kereső motorból állnak, mely a web alkalmazást feltérképezi, a kommunikációs protokollokat vizsgálja, a felhasználói beviteli mezőket ellenőrzi, valamint az adatbázis támadás vektorait és a véletlenszerű reakciókat vizsgálja. Ehhez tartozik egy profi grafikus felhasználói felület és egy fejlett riporting funkció is. A kereskedelmi forgalmazók folyamatosan frissítik a kereső motorokat és a támadási vektor adatbázisokat is.

A web sérülékenység keresők kiértékelése

Az elmúlt években számos sérülékenység vizsgáló[1] összehasonlítását végezték el, és semmilyen általános következtetést nem sikerült levonni az eredményekből. Az eltérő eredmények nagy része a közös tesztelési kritériumok hiányával magyarázható. A sérülékenység keresőket jellemzően a tesztelők használják – működés-, hálózat biztonsági tesztelők, írás-tesztelők, fejlesztők - eltérő feladatokra, de mindegyikük másként tekint ezekre az eszközökre, ami eltérő értelmezési eredményekhez vezet. Néha a web sérülékenység keresőket más biztonsággal kapcsolatos termékekkel is összehasonlítják. Ugye az almát sem hasonlítjuk össze a naranccsal (Lásd 1. lábjegyzet)? Másik magyarázat az eltérésre a teszt alapjaiban kereshető. Óriási mennyiségű technológia és módszer áll rendelkezésre egy web alkalmazás létrehozására, így igen nehéz egy közös tesztelési stratégia meghatározása. Minden egyes alkalmazás más megközelítést igényel, amit nem mindig könnyű elérni, ezért is olyan nehéz az eredményeket összehasonlítani. Végül, mind a tesztelők, mind a forgalmazók más szempontokat tartanak szem előtt céljaik elérésére. Habár a sérülékenység vizsgálók kívülről nézve egyformának tűnhetnek, de az eltérő technológiai alapok miatt, az értelmezés és az eredmények összehasonlítása bonyolultabb lehet, mint azt gondolnák. A web alkalmazás biztonsági konzorcium (Web Application Security Consortium – WASC) 2007-ben elindított egy projektet, hogy meghatározza a web alkalmazás biztonsági vizsgálatok kiértékelésének alapelveit a sérülékenységek azonosítására[2]. Sajnos ez a projekt még nem fejeződött be, de már egy előzetes verziója az eredménynek megjelent [3].

1 http://www.networkcomputing.com/rollingreviews/Web-Applications-Scanners/, http://ha.ckers.org/blog/20071014/web-application-scanning-depthstatistics/, http://anantasec.blogspot.com/2009/01/web-vulnerability-scannerscomparison.html
2 http://www.webappsec.org/projects/wassec/
3 http://sites.google.com/site/wassec/final-draft

Ez a cikk a különböző vizsgálatokra és a sérülékenység keresők használatára fókuszál. Nem ad választ arra, hogy melyik az elérhető legjobb sérülékenység kereső, de rávilágít néhány eszköz erősségére és gyengeségére, betekintést nyújt abba, hogy hogyan használjuk ezeket fel sérülékenység elemzésre.

A web sérülékenység vizsgáló használata

A sérülékenység kereső olyan, mint egy fúró. Habár az elsőket arra tervezték, hogy megkeressék a réseket, a későbbiek létre is tudják hozni azokat, de a használatuk hasonló. Amennyiben egy dobozba belefúrunk valahol, akkor lehet, hogy eltalálunk valamit, de a legtöbb esetben nincs eredmény. Anélkül, hogy számos gépezet konfigurációját megvizsgálnánk, a lehetséges fúrófejekkel belefúrunk az anyagokba, így több mint valószínű, hogy nem a jó lyukba fúrunk és valami váratlan dolog történik. Hasonló ehhez a sérülékenység vizsgáló futtatása a dobozon kívülről, ami talán hoz valami eredményt, de anélkül, hogy megvizsgálnánk a sok konfigurációs beállítási lehetőséget és a teszt objektum szerkezetét az eredmény nem lehet optimális. Minden egyes helyzetben más lehet az 'optimális konfiguráció'. Amennyiben hatékonyan akarjuk használni a sérülékenység vizsgálót, akkor előbb meg kell értenünk, hogyan működnek ezek és mit tudnak vizsgálni.

Alapvetően a keresők a következő három lépésben működnek:

1. azonosítani a lehetséges sérülékenységet
2. megpróbálni kihasználni azt
3. bizonyítékot keresni a sikeres kihasználásra

Ahhoz, hogy minden egyes lépés hatékonyan fusson, a keresőt az adott szituáció szerint kell konfigurálni. Ezen lépések bármelyikében a hibás konfiguráció hiányos jelentéshez és megbízhatatlan eredményekhez vezethet, tekintet nélkül a másik két lépés eredményességére.

Ismerni kell, hogy mit tesztelünk

Mielőtt a sérülékenység vizsgálót elindítanánk a lehetséges problémák megkeresésére, először is tudnunk kell, hogy mit akarunk tesztelni. A weboldal feltérképezése alapvetően fontos a sérülékenységek hatékony vizsgálatához. A keresőnek be kell jelentkeznie az alkalmazásba, hitelesítettnek kell maradnia, fel kell fedeznie a használt technológiát, meg kell találnia az összes oldalt, script-et és az egyéb működéshez vagy az alkalmazás biztonsága szempontjából szükséges elemet. A legtöbb sérülékenység vizsgáló számos lehetőséget biztosít a bejelentkezésre és a weboldal feltérképezésére a web alkalmazások 'ellen', de ha a „szokványos” technológiákat kombinálva használják, akkor kiegészítő paraméterezésre van szükség.

Egy másik paraméter például képes a kereső által használt felhasználó agent megválasztására vagy módosítására. Amennyiben a web alkalmazás a különböző böngészőkhöz eltérő funkciókat biztosít vagy mobil verziót is tartalmaz, akkor a keresőnek ezt fel kell tudnia deríteni, valamint azt is fel kell ismernie, ha az adott weboldal csak egy bizonyos böngészővel működik helyesen. A sikeres bejelentkezés után a keresőnek azonosítottnak (hitelesítettnek) kell maradnia és nyomon kell követnie a weboldal állapotát. Addig ez nem okoz problémát, amíg a szabványos eljárásokat használják (pl. cookie-k), de az URI-ban használt egyedi eljárások könnyen vezethetnek problémákhoz. Habár a keresők képesek azonosítani ezeknek a problémás technológiáknak a

meglétét, automatikus megoldást csak ritkán biztosítanak. Ha a tesztelő nem ismeri vagy nem érti az alkalmazást, a használt technikákat és a lehetséges problémákat, akkor a teszt hatékonysága egészen korlátozott lehet.

A jók

A sérülékenység vizsgálók képesek a sérülékenységek széles körének azonosítására, melyek mindegyike más megközelítést igényel. Ezek a sérülékenységek nagyjából négy területre oszthatóak fel:

- információ közzététel
- felhasználói bemenettől független
- felhasználói bemenettől függő
- logikai hibák

Az információ közzététel az összes olyan hibával foglalkozik, amely érzékeny információkat biztosít a tesztelt rendszerről vagy az alkalmazás tulajdonosáról esetleg annak felhasználóiról. A hiba oldalak túl sok információt mutathatnak meg, ami az alkalmazott technológia azonosítását és a nem megfelelő konfigurációs beállítások felfedését eredményezheti. A szabványos telepítő oldalak (install pages) segítik a támadót, hogy sikeresen támadja meg a web alkalmazást, ahol e-mail címek, felhasználó nevek, telefonszámok segítik a social engineering típusú támadások kivitelezésében. Néhány kereskedelmi forgalmazó ellenőrzi a Google Hacking Database[4] bejegyzéseit is. Ezt a lehetőséget a tesztelési fázisok elfogadása után, korlátozottan használják. A felhasználó-független sérülékenységek a nem biztonságos kommunikációt fedik le, például jelszavak küldése egyszerű szövegként, illetve tárolásuk egy titkosítatlan vagy gyengén titkosított cookie-ban, továbbá kitalálható rész azonosítók, rejtett mezők, a web szerveren engedélyezett nyomkövető beállítások. Mind az információ felfedés, mind a felhasználó független sérülékenységek kézi ellenőrzése időigényes és fárasztó. A sérülékenység keresőknél ezeknek a problémáknak hatékony azonosítása szinte alapértelmezett.

A rosszak

Nagyobb problémák merülnek fel a felhasználó függő sérülékenységek tesztelésekor. Ezeket a problémákat a felhasználói bemenetek nem megbízható feldolgozása okozza. Az ilyen fajta legismertebb sérülékenységek a Cross-site scripting (XSS)[5] [6], az ehhez közelálló Cross-site request forgery (CSFR)[7] [8] és az SQL befecskendezés[9] [10]. Az automatikus vizsgáló eszközök feladata ezeknek a sérülékenységeknek a tesztelésekor a lehetséges sérülékenység helyének felderítése, majd kihasználása, és a sérülékenység sikeres kiaknázásakor fellépő hatások feltárása.

4 http://johnny.ihackstuff.com/ghdb
5 http://en.wikipedia.org/wiki/Cross-site_scripting
6 http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
7 http://en.wikipedia.org/wiki/Csrf
8 http://www.owasp.org/index.php/Cross-Site_Request_Forgery
9 http://en.wikipedia.org/wiki/SQL_injection
10 http://www.owasp.org/index.php/SQL_injection

SQL befecskendezés

Jelenleg az SQL befecskendezés a legismertebb sérülékenység. Ilyen támadások hatása lehet a weboldalak rosszindulatú megváltoztatása (deface) vagy a feltört adatbázisok. Habár a legegyszerűbb támadási vektorok már nem jelentenek problémát a legtöbb web alkalmazásnak, a kifinomultabb változatok fenyegetést jelentenek. Amennyiben az alkalmazás a támadásról nem jelenít meg semmilyen hiba üzenetet vagy visszajelzést, még akkor is sérülékeny lehet az úgynevezett vak SQL befecskendezésekre. Habár néhány vak SQL befecskendezést a sérülékenység keresők felderíthetnek, de az összeset nem képesek lefedni, legfőképpen végrehajtási okok miatt. A vak SQL befecskendezésekre jellemző, hogy sokáig tart elvégezni a tesztet, különösen ha az alkalmazás minden mezőjét tesztelik ezekre a sérülékenységekre. A legtöbb forgalmazó felhívja a figyelmet erre a korlátozásra és egy önálló vak SQL befecskendezés eszközt biztosít az alkalmazás meghatározott helyein a tesztelésre.

XSS és CSRF támadások

A Cross-site scripting (és a Cross-site request forgery) támadások talán a leginkább alábecsült sérülékenységek manapság. Ezeknek a hibáknak a következményei viszonylag ártalmatlannak és elszigeteltnek tűnnek, de a kifinomultabb változataik mindennaposak a VPN csatlakozások eltérítésekor, a tűzfalak megkerülésekor és az áldozat gépe feletti teljes ellenőrzés megszerzésekor. Az XSS-sel az a fő probléma, hogy a lehetséges támadási vektor futása milliókra rúghat (ha nem több). Például egy XSS szál 2007. szeptemberétől fut a sla.cker.org[11]-on, ami közel 22 000 postafiókot tartalmaz idáig, és csaknem naponta kerülnek újabb vektorok kézbesítésre.

Számos ok játszik még szerepet a lehetséges támadási vektorok óriási számában:

- Mindegyik böngésző megpróbál mindent értelmezni, nem csak a hagyományos SCRIPT és HTML tag-eket, hanem a CSS template-eket, iframe-eket és a beágyazott objektumokat is, stb.
- Lehetséges a *tag*-ek rekurzív használata is (pl. <SCR<SCRIPT>IPT>)
- A támadási vektorokban többfajta kódolás használható (pl. unicode[12]).
- Ezekből a vektorokból többet is össze lehet kombinálni, ezzel létrejön egy új vektor, amelyet az alkalmazások vagy szűrési eljárások nem tudnak megfelelően kezelni.

AJAX használatával a lehetőségek száma exponenciálisan emelkedik. Nyilvánvaló, hogy lehetetlen az összes ilyen variációt egyidejűleg kezelni. A sérülékenység keresők a legelterjedtebb támadási vektoroknak csak egy részhalmazát biztosítják, néha ezeket véletlenszerűen kombinálják. Amennyiben ez a lista a gyakorlatban nem hatékony, akkor további támadási vektorokat kell hozzáadni vagy manuálisan kell tesztelni. A másik probléma az XSS támadások különbözősége, a két legismertebb típus a visszaható és a tárolt támadások. A visszaható támadások hatása az, hogy azonnal visszahelyeződnek a klienshez, miután elkészül egy viszonylag egyszerű elemzés. Míg a tárolt vagy ismétlődő támadások ezzel szemben több helyen kerülnek tárolásra és nem láthatóak azonnal. Még a bejelentkezett felhasználó sem biztos hogy látja az eredményt, így egy másik felhasználó bejelentkezése is szükséges lehet, az alkalmazás logikájának megértéséhez.

11 http://sla.ckers.org/forum/read.php?2,15812
12 http://en.wikipedia.org/wiki/Unicode_and_HTML

A tárolt és ismétlődő felhasználói beviteli sérülékenységet alapvetően két módon lehet ellenőrizni:

- A web alkalmazás minden felhasználói beviteli mezőjének kihasználása és az alkalmazás vizsgálat teljes megismétlése a sikeres kiaknázásra utaló jelek megjelenése után.
- Ellenőrizni, hogy mi került a szerveren tárolásra szűrés és tisztítás után.

A legtöbb kereső az első eljárás végrehajtását választja, de az összes sikeres kiaknázás felderítése bonyolult feladat. Különösen, ha az alkalmazásban különböző felhasználói szerepkörök vannak, vagy kiterjedt az adatáramlás, a sikeres kiaknázások felderítése az alkalmazás megértése és logikájának elsajátítása nélkül bonyolult feladat. Az Acunetix a második eljárás megvalósítását használja, ezt a technológiát AcuSensor[13]-nak nevezik. Habár ez a technológia jó eredményeket mutat például a tárolt XSS támadások és a vak SQL befecskendezéses támadások felderítésben, legnagyobb hátránya, hogy a web szerverre telepíteni kell, ahhoz hogy használni lehessen. Ez nem jelent nagy problémát egy fejlesztői, sőt még egy elfogadott környezetben sem, de például egy termelési környezetben ez nem lehetséges vagy nem engedélyezett.

A gonoszok

A legbonyolultabb feladat, amikor egy web alkalmazásban meg kell találni az alkalmazási és üzleti logikai hibákat. Általában ezek a hibák más sérülékenységek kombinációi, sőt még működési elemek is társulnak a problémához. Például egy logikai hiba - az alapértelmezett jelszó megfelelő hitelesítés nélkül, vagy a webshopból a rendelés után a jelszó átadása a fizető lapnak. Amennyiben a logikai hibához még biztonsági problémák is társulnak, az alkalmazás működésében vannak tervezési hiányosságok, akkor ennek felderítése az összes sérülékenység keresőnek problémát okoz. A kereskedelmi forgalmazók, mint például az IBM és a Cenzic, rendelkeznek az alkalmazás ellen irányuló logikai támadásokat meghatározó modullal is, melyek még igen kezdetleges modulok és alapos paraméterezést igényelnek. A logikai hibák tesztelésekor szükség van a manuális tesztelésre is annak ellenére, hogy a sérülékenység keresők ismétlődő és részletes tesztelésre is használhatóak. Gyakorlatilag minden kereskedelmi forgalmazónak, még például a Burp Suite Pro-nak is, van választható lehetősége a sérülékenység vizsgáló böngészőként való használatára. Ezáltal a tesztelő kiválaszthatja az alkalmazás tesztelésének módját, miközben a kereső automatikus ellenőrzéseket végez a háttérben.

Következtetések

A sérülékenység keresők nagyon hasznos eszközök, melyek fejlesztik az alkalmazás biztonságát és minőségét. Minden tesztelési eszköznek, figyelembe kell venni a korlátait és alapvető fontosságú ezen eszközök helyes használata. A webes alkalmazások korai fejlesztési szakaszában lehetőség van a minőség és biztonság növelésére, a kommunikációs problémák és a rossz gyakorlat hatékony vizsgálata mellett. Ha a felhasználói bevitel szűrésére és megtisztítására használják a tesztelést, akkor időt lehet nyerni a gyors befecskendezéses támadásokkal. Az eredmények manuális felülvizsgálata alapvetően lényeges, de a korlátozott mennyiségű támadási vektor miatt a kézi tesztre is szükség van. A teljesen automatizált üzleti és alkalmazás logikai tesztelés nem lehetséges a sérülékenység keresőkkel. A sérülékenység vizsgálóknak ugyanolyan korlátaik vannak, mint minden más tesztelési eljárásnak. A tapasztalt biztonsági tesztelők az eszköz használatával időt takaríthatnak meg és növelhetik a teszt hatósugarát a biztonsági tesztelési folyamatok legkimerítőbb részeinek az automatizálásával.

13 http://www.acunetix.com/websitesecurity/rightwvs.htm

A Pushdo botnet

A Pushdo botnet, más néven Pandex vagy Cutwail 2007. január[14] óta fellelhető. Míg a háttérben volt és jóval kevesebb figyelmet kapott mint a hírhedt Strom vagy a Conficker, a világ második legnagyobb botnetévé nőtte ki magát[15]. A napi 7.7 billió email küldésével minden huszonötödik levelet működéséhez köthetünk.

A káros szoftver fejlesztői minden technikát bevetettek, hogy a kártékony aktivitás nehezen érzékelhető legyen:

- A Pushdo mellett más kártékony szoftverek is felelősek a nagy számú kéretlen levelek küldéséért, mivel ez a kártékony szoftverek terjesztésének egy elterjedt módja. Ennek eredményeképpen számos eltérő érzékelések léteznek ezen veszély variánsainak észlelésére. Az ilyen fenyegetettségek detektálását legtöbb esetben „általános észlelésnek" jelölik meg, mely elősegíti a botnet rejtőzködését – nehezebbé téve a hírhedtebb társaitól való megkülönböztetést.
- A Pushdo komponenseinek túlnyomó többsége memória rezidens és csak kis számú lemezírási műveletet hajt végre, így nehezítve a detektálást.
- A jól ismert Conficker és a Storm valamilyen sérülékenység kihasználásával és tömeges levelek küldésével terjed. Ugyanakkor a Pushdo nem rendelkezik önmagát sokszorosító mechanizmussal, illetve féreg viselkedési formával.
- Megtévesztő az is, hogy a botnet tulajdonosok gyakran változtatják a Pushdo funkcióit és kódját.

A következőkben a fenyegetés eltérő komponenseire a következőképpen hivatkozunk:

- Pushdo: A kártékony szoftver fő binárisát illetjük ezzel a névvel. A Pushdo valójában egy fejlett letöltő program. Működése során először megfertőzi a rendszert, majd letölti a Cutwail spam modult. Általában a Cutwail mellett telepítésre kerül egy külső bűnözői csoporttól származó kampány modul is.
- Cutwail: a Pushdo botnet kéretlen levelek küldését végző modulja.

Pushdo Analízis

Mint a legtöbb káros szoftver, a Pushdo is bináris fájlként kerül terjesztésre. Az analízis során a káros kód vizsgálatának eredményei, majd a teszt környezetben futtatott malwarezen aktivitása kerül ismertetésre.

14 http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PANDEX.A&VSect=Sn
15 http://www.messagelabs.com/mlireport/MLIReport_2009.01_Jan_Final.pdf

Telepítő

Általában a malware telepítő binárisa nem csomagolt. Végrehajtása után a káros szoftver ellenőrzi, hogy már fut-e „rs32net.exe” néven, mely alapértelmezés szerint a C:\Windows\System32 mappában található. Amennyiben még nem fut, készít magáról egy rs32net.exe nevű másolatot a rendszer mappában, és végrehajtja. Számos variáns esetén ez a név nincs „bedrótozva” a binárisba, inkább az aktuálisan belépett felhasználó nevét használják a fájl elnevezésére.

A futtatás után a telepítő eltávolítása a következő parancssorral történik:

cmd /c del [ORIGINAL_INSTALLER_LOCATION]>> NUL

Miután a káros szoftver megfelelő néven, és a megfelelő mappában fut, a telepítő elindítja a fő rutinját. Az eljárás először egy új szálat hoz létre.

Ez a szál a felelős a következő két rendszer betöltési pont létrehozásáért és 10 másodpercenkénti újragenerálásáért:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Rs32net
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Rs32net

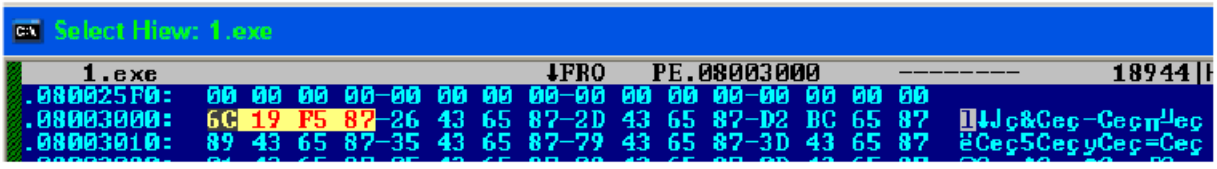
Mindkét kulcs a káros szoftverre mutat, és biztosítja annak automatikus végrehajtását a gép újraindításakor.

Ezután a kód végrehajtja az svchost.exe egy másolatát (a továbbiakban svchost[1] megnevezéssel hivatkozunk rá), elindítva a folyamatot felfüggesztett módban. Majd végrehajtható kódot fecskendez az svchost-ba a *WriteProcessMemory* windows API ismételt hívásával. A befecskendezett PE kód minden egyes szekcióját sorjában az svchost[1] memória területére írja a 0x90000000 memória offset-től kezdve, mielőtt az svchost[1] belépési pontja a befecskendezett kód belépési pontjára mutatna. Majd az svchost[1] főszála visszaállításra kerül, melynek eredményeként a befecskendezett kód végrehajtódik. Korábban a malware írói ugyanezen feladatok ellátására az Internet Explorer-t használták az svchost helyett[16].

A befecskendezett kód titkosítva helyezkedik el az Rs32net.exe adat szekciójának 0x3000 és 0x5C00 offset-jei között. A kód befecskendezése előtt a titkosítás feloldása 4 byte-os (1 dword) darabokban történik, a következő algoritmus használatával:

Decrypted_Dword = Encrypted_Dword XOR (0x87654321 XOR Dword_Offset)

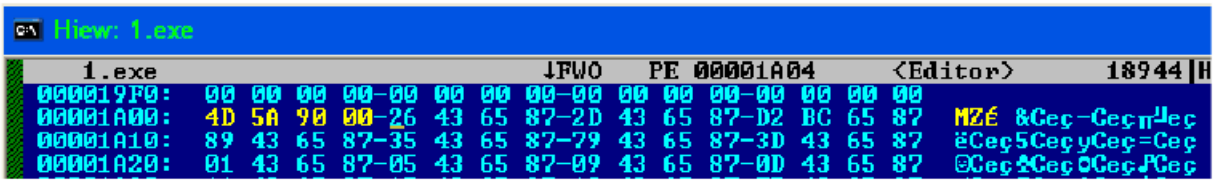
Első titkosított DWORD [6C19F587]



1. ábra

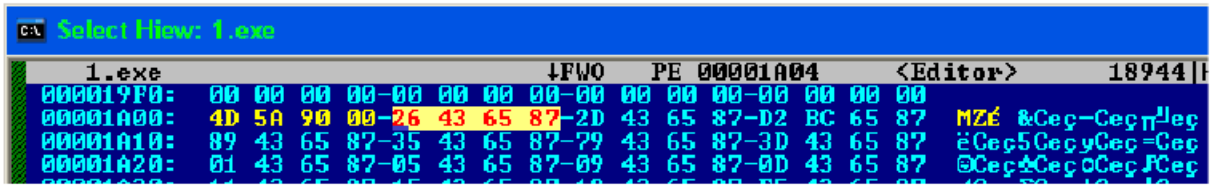
16 http://www.virusbtn.com/virusbulletin/archive/2008/03/vb200803-pandex

Titkosítás feloldása – 6C19F587 XOR (87654321 XOR 0)



2. ábra

Második titkosított DWORD. Decrypted_DWORD = 26436587 XOR (87654321 XOR 4)



3. ábra

Az adat egy kis részének dekriptálását egy kisebb „simítási” művelet követi a befecskendezést megelőzően. Ez a „simítás” az Rs32net.exe /n paraméterétől függően kis mértékben változhat. A módosított adat a HTTP GET kéréseknél használt paraméterekből áll, mely a következő fejezetben kerül kifejtésre.

Végül az Rs32net.exe egy második másolatot is készít magáról a memóriában. Ekkor /n paraméterrel fut, melynek eredményeként létrehoz egy másik svchost folyamatot (svchost[2]), amely némileg eltér az előbbitől. A rutin véghezvitele után, az Rs32net.exe továbbra is a memóriában fut és folyamatosan újragenerálja a fent említett registry kulcsokat.

Az alkalmazott technikával szinte soha nem történik meg a malware összetevők írása a merevlemezre. Ezzel jelentősen megnehezíti az anti-vírus szoftverek detektálását. Ezt a technikát a legtöbb Pushdo komponens alkalmazza.

Letöltő modul

Miután a telepítő befecskendezte a kódokat az svchost[1].exe illetve az svchost[2].exe folyamatokba, azok működése szinte azonos módon történik. Mindkettő downloader-ként funkcionál és további külső Pushdo komponenseket tölt le.

Mindkettő a saját MZ fejlécek ellenőrzésével indul, majd végrehajtják a fő rutinokat. Először lekérdezik a következő registry kulcsokat a fertőzött gépről, hogy kinyerjék a rendszer bios időt, a video bios dátumot és a processzor típust:

HKLM\Hardware\Description\System\SystemBiosDate
HKLM\Hardware\Description\System\VideoBiosDate
HKLM\Hardware\Description\System\CentralProcessor\0

A merevlemezzel kapcsolatos információk megszerzése a *GetVolumeInformation* API segítségével történik. Ezzel a technikával egyszerűen megállapítható lehetne, hogy a Pushdo futása virtuális

környezetben történik-e vagy sem. Ugyanakkor úgy tűnik, hogy a Pushdo nem használja fel ezt az információt és ugyanolyan módon működik virtuális és normális környezetben is.

Ezek után feloldja a titkosítást az adat szekció egy területéről, mely három paraméter értéket, és egy hat IP címből álló listát szolgáltat. A titkosítás feloldása egyszerű XOR művelettel történik, mely során a 0x78d616b2 érték használatos. Az IP címek mind az svchost[1], mind az svchost[2] számára azonosak, ugyanakkor a paraméterek kis mértékben eltérnek. Míg az IP címek az eltérő variánsok esetén is megegyeznek és „bedrótozottak", a tapasztalat azt mutatja, hogy igen sűrűn frissülnek.

Command & Control IP címek

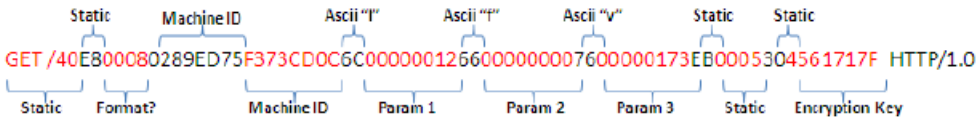
Dropsite IP Addresses	
70.38.68.137	69.64.67.194
91.211.64.117	74.54.77.82
94.247.3.46	74.54.135.202
192.8.75.216	216.55.176.45
216.195.63.22	72.167.49.117
66.45.246.146	92.62.101.118

4. ábra

A kártékony szoftver minden egyes drop-site IP címhez megpróbál kapcsolódni. A tesztelés során a legtöbb drop-site vagy C&C szerver Észak-Amerikához volt köthető. Az IP címek más-más szolgáltató hálózatában és más ASN[17] alatt voltak. Mindez jelentős redundanciát biztosított a Pushdo botnet számára. Hat különböző szolgáltatóval szükséges tárgyalni a káros szoftver bármelyik variánsának leállításához.

A kapcsolat sikeres kiépítése után speciális HTTP GET kéréseket küld a malware. A GET kérések eltérnek az svchost[1] és svchost[2] esetében, de a formájuk azonos.

HTTP GET kérés



5. ábra

A kérés egyes részei statikusak és a végrehajtható fájl tartalmazza, mások eltérő jelentéssel bírnak:

- **GET /40E8**: Tapasztalat szerint úgy tűnik, hogy egy vagy több végrehajtható kód lekérését jelenti a szerverről, mely később az áldozat gépén kerül futtatásra.
- **Format**: Amennyiben ez az érték kisebb mint 0015, a letöltött kód titkosítási folyamaton esik át, mely során a GET kérés utolsó 8 karaktere szolgál kulcsként. Abban az esetben, ha az érték 0015 vagy annál nagyobb, akkor a kódot titkosítás nélkül szolgáltatja a szerver. Ebben az esetben ez előzőekben már említett „simításra", kiigazításra van szükség a futtatást megelőzően.

17 ASN (Autonomous System Number) - Autonóm rendszer száma

- **Machine ID**: A két azonosító, a fertőzött számítógép azonosítására szolgál. Az azonosító generálása a rendszer bios dátumot, a video bios dátumot, a processzor típusát és a rendszer kötet információt veszi alapul.
- **Parameters**: A paraméter 3 határozza meg, hogy melyik fájlt szolgáltassa a szerver.
- **Encryption Key**: A titkosításhoz és annak feloldásához használatos kulcs.

A GET kérések formázása a Pushdo botnet egyik olyan jellemvonása, amely folyamatosan fejlődik. Létezik bizonyíték arra, hogy a formázás módját az IDS rendszerek megkerülése érdekében módosították[18].

A szerver a kérésre egy vagy több futtatható fájlt küld. Ezek a fájlok titkosítva, illetve titkosítás nélkül is érkezhetnek a fenti leírás szerint.

A káros szoftver ellenőrzi a letöltött fájlok MZ fejlécét. Megbizonyosodik arról, hogy a „This Program cannot be run in DOS Mode" kifejezésből a „This" karakterlánc megtalálható-e. Amennyiben megtalálható, a malware létrehoz egy ideiglenes fájlt a „Local Setting\Temp" mappában. A könyvtárba bemásolja a letöltött fájlokat, majd végrehajtja azokat. A továbbiakban ezekre a fájlokra TempFile néven hivatkozunk.

Abban az esetben, ha a „This" helyett „Thus" (gyakorlatilag a mondat harmadik karakterét ellenőrzi a malware) karakterláncot olvas a kártékony szoftver, akkor az svchost egy új példánya készül el. Majd az előzőekben ismertetett módon a *WriteProcessMemory* segítségével befecskendezésre kerül a kód.

A letöltő modul nyomon követi mindezeket a folyamatokat és a hozzájuk tartozó információt struktúrában tárolja a memóriában, mely tartalmazza az érintett folyamat azonosítót is (PID). Amennyiben egy bizonyos karakter a végrehajtható kód fejlécében „z" (például: Thuz), a struktúrában kritikusként kerül megjelölésre a befecskendezett modul. A letöltő modul folyamatosan ellenőrzi a futó folyamatokat és összehasonlítja a memória struktúrában tárolttal. Kritikus modul törlésekor újra előállítja az svchost.exe folyamatot és befecskendezi a modul kódját.

Letöltött modulok – TempFile

A TempFile-t a letöltő modul tölti le és az aktuális felhasználó Local Settings\Temp könyvtárába kerül. A név minden egyes alkalommal eltérő lehet, viszont a *GetTempFileName* API funkciótól függ és „.tmp" kiterjesztéssel rendelkezik.

A TempFile először a kernel fájl nevét generálja, amely a következő formátumot követi:

[SYSFILENAME] = ati + [3 Véletlenszerűen generált karakter] + xx.sys

(Például: ati0bsxx.sys.)

Ezt követően beállítja a kernel drivert úgy, hogy abban az esetben is betöltődjön, ha a gép biztonságos üzemmódban indul. Ezt a következő két registry kulcs létrehozásával teszi:

HKLM\SYSTEM\CurrentControlSet\Safeboot\Minimal\[SYSFILENAME]
HKLM\SYSTEM\CurrentControlSet\Safeboot\Network\[SYSFILENAME]

18 http://www.virusbtn.com/virusbulletin/archive/2008/03/vb200803-pandex

Amint a registry kulcsok létrehozása megtörtént, a végrehajtható kernel a Windows rendszer mappába kerül és létrehoz egy kernel driver szolgáltatást standard API-k használatával.

A telepítés befejezéséhez a TempFile létrehozza a következő registry bejegyzéseket minden egyes ControlSet esetében, mely szükséges a kernel driver szolgáltatás végrehajtásához a rendszer indulásakor:

HKLM\SYSTEM\ControlSet001\Services\[SYSFILENAME]

Group: **SCSI Class**

ImagePath: **System32\Drivers\[SYSFILENAME]**

Start: **0x00000000** (Boot – Loaded by Boot Loader)

Type: **0x00000001** (Kernel Device Driver)

A kernel driver a bootolási folyamat korai szakaszán kerül betöltésre a Start és Group értékek eredményeképpen. Így korábban kerülnek betöltésre mielőtt egyes biztonsági termékek felfedezhetnék.

Végül a TempFile letörli önmagát, hasonlóképpen mint a telepítő modul:

cmd /c del [TEMPFILE]>> NUL

Letöltött modulok – Cutwail spam motor

A Cutwail Spam motor a Pushdo család egyik legfontosabb összetevője. Egy hatékonyan kódolt, optimalizált spam motor, mely könnyen frissíthető az új spam kampányok igényeihez igazítva.

Mindenek előtt a Cutwail létrehoz hét mutex-et, melyet a thread fog használni koordinációs célokra a többszálúsított kommunikációja folyamán.

A modul ellenőrzi a host fájl tartalmát (%SYSTEM\etc\driver\hosts) mielőtt elindítaná a fő szubrutinját – a szál létrehozást.

A Cutwail 60 új szálat állít be, mindegyiket függő állapotba, majd megkezdi a kommunikációt a C&C szerverrel.

A fő szál az előbbiekben tárgyalt C&C szerverek IP címeihez próbál csatlakozni. A kapcsolat kiépülésekor használt csatornát titkosított párbeszédhez használja, mely lehetőséget biztosít a spam futásához szükséges beállítások lekérdezéséhez.

A C&C szervernek küldött adat 32 byte-ból áll, mely kilenc mezőt tartalmaz, amelyek közül számosnak ismert a tartalma illetve a funkciója:

```
Field #1 dd OSVer
Field #2 dd Internal_IP_Address
Field #3 dd Req
Field #4 dd Control
Field #5 dd ??
Field #6 dd Windows version
Field #7 dw DNSQuery
Field #8 dw ??
Field #9 dd ??
```

A szerver ugyancsak struktúrában válaszol:

```
Response_Type dd
Data_Size dd
...
[Encrypted_Data]
```

A két dword után következő tartalom titkosított. A Cutwail titkosítása viszonylag egyszerű. Egy statikus kulcsot használ, melyet a Cutwail kódja tartalmaz. A kulcs egy karakterlánc, mely egy orosz kifejezésből ered. Könnyen megérthetjük visszafelé olvasva, amennyiben orosz nyelvtudással rendelkezünk:

„reva gurd iuh an it ak-lehsoP”

A visszafelé olvasott „aver”, valószínűleg a moszkvai kirendeltséggel is rendelkező Avermedia vállalkozásra utal (http://www.avermedia.com). A támadók egyszerűen nem kedvelik a vállalkozás hardvereit, esetleg elégtelen korábbi alkalmazottakról lehet szó.

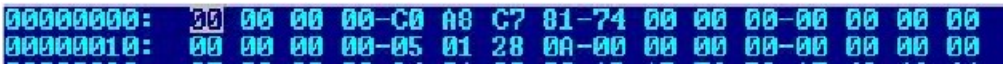
A titkosítás feloldása több szinten történik:

- Elsőként a Cutwail a titkosított karakterláncot blokkokra osztja, melynek hossza megegyezik az aktuális kulcs hosszával (jelen esetben 29 byte).
- Majd minden egyes blokkon XOR művelet végrehajtása történik a megadott kulcs használatával.
- Az eredményt megfordítja (az első byte a huszonkilencedikkel, a második a huszonnyolcadikkal stb. helyet cserél)
- A páros blokkokon (második, negyedik stb.) negálási művelet végrehajtása történik meg.
- Végül, a megmaradt byte-okon, melyek nem alkotnak egy teljes blokkot egy egyszerű negálási művelet végrehajtása tapasztalható.

Cutwail inicializáció

A Cutwail kliensek kezdő kérései a következő formát követik: Az első mező 0x00000000 értékre van beállítva, hacsak az OSVersion registry bejegyzést már a Pushdo korábban létre nem hozta. A második mező a külső IP címet tartalmazza és további kapcsolat során változatlan marad. A Req mező inicializálása 74h értéknél történik meg és ugyancsak változatlan marad a továbbiakban. A Windows verziót a *GetVersion* API határozza meg. Windows XP SP2 esetén (5.1.2600) ez az érték 05 01 280A (280A a 2600 hexadecimális jelölése). A kérés fennmaradó része nullákból áll.

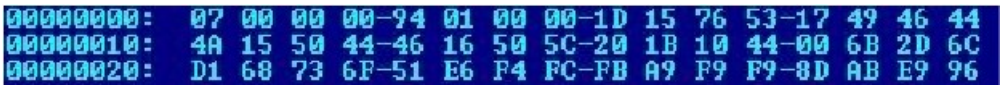
Cutwail kliens kezdő kérése



6. ábra

A szerver válaszát a 7. ábra szemlélteti. A kezdő válasz típus mindig 7. Megfigyelendő a mezők little-endian természete (a 0x00000007 érték az Intel processzorok esetén 0x07000000 értékkel kerülnek tárolásra). A második mező a következő adatok méretét tartalmazza. Az inicializáló kérések esetén ez általában 194h byte.

Cutwail inicializáló válasz

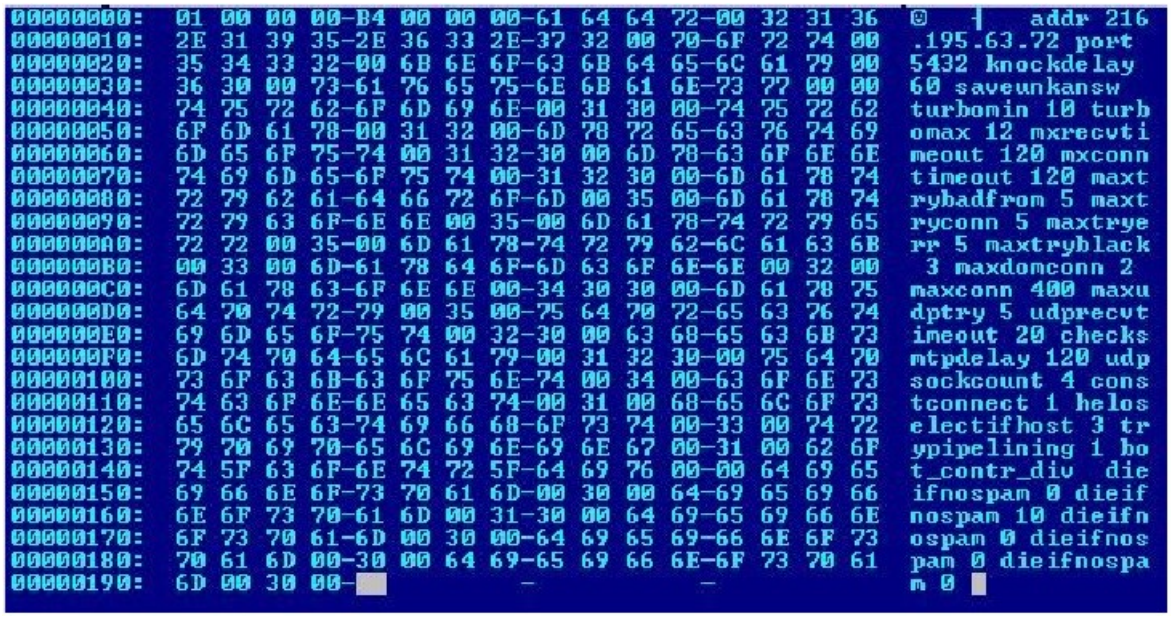


7. ábra

Az információ további része titkosított. A titkosítás feloldása után a Cutwail modul konfigurációs beállításai nyerhetők ki. A konfiguráció tartalmaz egy új IP címet valamint egy portot és egyéb hálózati beállításokat, mint időtúllépést, próbálkozások maximális számát stb. Ezek a beállítások az alapértelmezett, „bedrótozott” értékek a következők:

Addr: Varies (216.195.63.72 in our samples)
Port: Varies (5432 in our samples)
Checksmtpdelay: 120
Maxconn: 512
Constconnect: 1
Udpsockcount: 16
Maxudptry: 5
Udpprecvtimeout: 20
Knockdelay: 20

Cutwail inicializáló beállítások

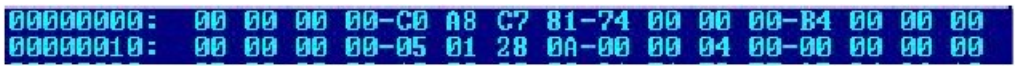


8. ábra

A válasz első mezője általában 1 értékkel rendelkezik. A második egy folytatólagos kód, mely a további üzeneteknél használatos. Jelen esetben a C&C szerver kéri a klienst, hogy kövesse a 0x000000B4 kontroll kódot.

A második kérés nagyon hasonló az elsőhöz, viszont a Cutwail kliens már használja az előzőekben fogadott kontroll kódot. További eltérést jelent a nyolcadik mező 00 04 értéke.

Cutwail második kérés



9. ábra

Első ránézésre a szerver válasz is nagyon hasonlít az inicializáló válaszra. Ebben az esetben a Response_Type kód 5 és a titkosított adat mérete 16 byte (0x00000010h).

Cutwail második válasz

10. ábra

A dekriptált üzenet 4 byte-tal indul, mely a bot azonosítót takarja. Az azonosító a következő registry kulcsként kerül tárolásra, mint egy fertőzés jelölő.

HKCU\SOFTWARE\Microsoft\OSVersion

A példában ez az érték s 0x000D8E6E. A következő a kliens külső IP címe a szerver perspektívájából. A harmadik mező ugyancsak egy azonosító a bot számára.

Cutwail azonosító beállítások

11. ábra

Az üzenet fogadása után, a Cutwail kliens egy reverse DNS lekérdezéssel ellenőrzi, hogy a külső IP címéhez tartozik-e valamilyen domain név.

A harmadik lekérdező csomag után a kliens már rendelkezik egy bot azonosítóval, egy fertőzés jelölővel, mindössze a kéretlen levelek küldéséhez szükséges információra van szüksége.

Az első mezőben az új fertőzés jelölő használatos, illetve a reverse DNS válasz a hetedik mezőben. A példa során az IP címhez DNS bejegyzés nem volt köthető, így ez az érték kettőre volt állítva. Az üzenet további része ugyanaz maradt mint az utolsó üzenetnél.

Cutwail harmadik kérés

12. ábra

A C&C szerver a standard két mezőből álló üzenettel válaszol, illetve az azt követő titkosított adattal. Jelen esetben a Response_Type értéke 8.

Cutwail harmadik válasz

13. ábra

A titkosított információ viszonylag nagy méretű (pár száz Kb) és az aktuális kampány célzott email címeit tartalmazza. Az email címek listája halmazokba vannak szervezve és a botnet vásárlójának választásától függ. Célzott halmaz lehet a moszkvai személyek, esetleg a szentpétervári üzleti email címek halmaza.

Cutwail címlista

14. ábra

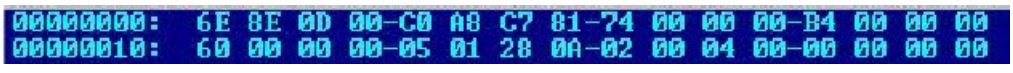
Az első mező 60h (96), melyet a spam levelek céljai követnek a következő struktúrában:

Email_address string
Email_server string
Server_IP_Address dd

A fenti példa szerint az első email cím jagja@ostrov.sakhalin.ru, a hozzákapcsolódó email szerver az mx1.sakhalin.ru és a szerver IP címe pedig 0xC348FA1B, azaz 195.72.250.27. Az előre meghatározott email címek, MX szerverek és a levelező szerverek IP címei megkímélik a fertőzött klienst számos feladat elvégzésétől. A továbbiakban nincs szükség DNS lekérésekre a kéretlen levelek küldése során.

Az információ lekérésének következő lépésében az egyedüli eltérés az ötödik mező értéke.

Cutwail negyedik kérés



15. ábra

Az ötödik mező 60h értéke arra készteti a szervert, hogy további információt szolgáltasson. A válaszban Response_Type értéke 6 és a titkosított adat mérete ismét nagy.

Cutwail negyedik válasz

```
00000000:  06 00 00 00-2C 18 03 00-13 13 17 0D-73 14 14 3F
00000010:  1F 20 69 75-6A 20 61 6F-0B 69 74 20-74 6B 2D 6C
00000020:  65 68 73 7C-9F B1 BA A9-E3 EE F1 E6-E4 F6 BE F0
```

16. ábra

A titkosított adat számos, könnyen testre szabható sablont tartalmaz. Könnyedén megadható a levelek tárgya, tartalma, csatolmányai stb.

A Cutwail spam levelek céljai gyakran az orosz piachoz köthetők, így nagy számú cirill karakterekkel találkozhatunk ezekben a mintákban.

Cutwail spam sablon

```
ID       □    +□  □    {MasSlaves} {rusname1} {rusfamili1}  <{generic_ru_mail}> {HTML_DECODE}{_BODY_HTML}{/HTML_DECODE}
 <table width="737" border="2" cellpadding="15" cellspacing="6" bordercolor="#000000">
  <tr>
 <td width="707" bordercolor="#000000"><table width="711" border="0" cellspacing="0" cellpadding="10">
  <tr>
   <td width="128"><div align="center"><img src="http://img-fotki.yandex.ru/get/3211/dogma59.7/0_20a03_a6e371d3_L.jpg
   <td width="543" valign="top"><p><font size="+2"><strong><font color="#FE960A"><font color="#CC3300" face="Georgia,
  <p><font color="#CC3300" size="+2"><strong><font face="Georgia, Times New Roman, Times, serif">Xîòèòå ñîöèàëíûé Àâs
  <p><font color="#CC3300" size="+2"><strong><font face="Georgia, Times New Roman, Times, serif">Xîòèòå èìåòü ïëîùàäè
  </tr>

 </table>
  <p align="center"><strong><font color="#0099FF" size="+3" face="Georgia, Times New Roman, Times, serif">Òîëüêî - ýòî
  <p align="center"><strong><font color="#666666" face="Georgia, Times New Roman, Times, serif">Ñòî÷íû, <font color=
  <div align="center">
  <table width="721" border="0" cellspacing="0" cellpadding="0">
  <tr>
   <td width="541" valign="top"><p align="center"><font size="+1"><strong><font color="#666666" face="Georgia, Times
 ïîìîùü Âàì íàéòè êîìïàíèþ è âûáðàòü ïëîùàäü!</font></strong></font></p>
   <p align="center"><font size="+3"><strong><font color="#CC3300" face="Georgia, Times New Roman, Times, serif">ÂÎÂÊ
   <td width="170"><div align="center"><img src="http://img-fotki.yandex.ru/get/3211/dogma59.7/0_20a02_8b7d5160_L.jpg
  </tr>
   </table>
  </div>
  <p align="right"><font size="+2"><strong><font color="#CC3300" face="Georgia, Times New Roman, Times, serif">Ðàçìå
 <p><strong><font size="+1" face="Georgia, Times New Roman, Times, serif">òåë:</font><font size="+3"> </font>{tel5423
  </tr>
 </table>
</div>
 Date: {DATE}
From: {TAGMAILFROM}
Return-Path: <{_generic_ru_mail}>
X-Priority: 3 (Normal)
Message-Id: <{DIGIT[10]}.{DIGIT[14]}@{MAILFROM_DOMAIN}>
To: {MAIL_TO}
In-Reply-To: <{nHEX[44]}@{MAILTO_DOMAIN}>
References: <{nHEX[44]}@{MAILTO_DOMAIN}> <{nHEX[32-44]}@{MAILFROM_DOMAIN}>
```

17. ábra

Az ötödik kérésnél a kilencedik mező értéke 14h (20).

Cutwail ötödik kérés

```
00000000:  6E 8E 0D 00-C0 A8 C7 81-74 00 00 00-B4 00 00 00
00000010:  60 00 00 00-05 01 28 0A-02 00 04 00-14 00 00 00
```

18. ábra

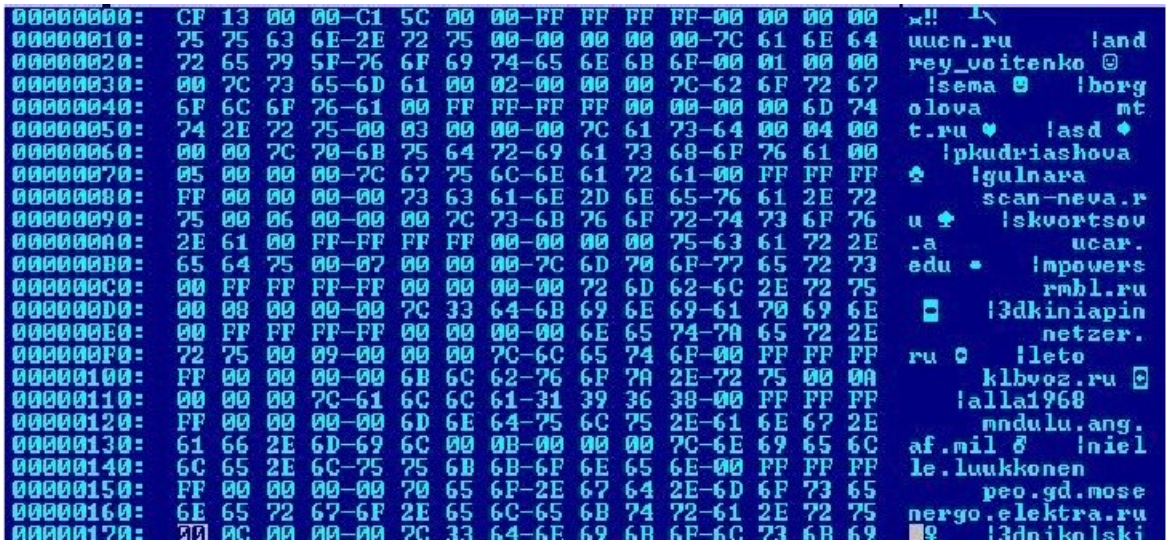
Az utolsó válasz formája megegyezik az előbbiekkel, a Response_Type értéke 1, és méret 5cc9 azaz 23,753 byte.

Cutwail ötödik válasz

19. ábra

Az információ utolsó szelete vezeték- és keresztneveket, valamint domain neveket tartalmaz, melyek a hamis email címek „From” mezőjében szerepelnek a későbbiekben.

Cutwail hamis email adatok



20. ábra

Az összes információ begyűjtése után a Cutwail beállítja az összes spam szálat.

- A thread-ek egy részének az a feladata, hogy DNS kéréseket hajtson végre, melyek megkerülik a helyi DNS szervereket, mivel közvetlenül a root DNS szervereket próbálják elérni.
- Egy szál feladata az „OSVersion” registry bejegyzés beállítása, mely fertőzés jelölőként használatos.
- Egy másik szál felelős a „bedrótozott” MX szerverekhez – mint például mx.google.com, msx.mail.ru és mx2.messagingengine.com – való kapcsolódásokért. Ezzel a módszerrel ellenőrizhető, hogy az eszköz online-e illetve az, hogy a tűzfal szűri-e az ilyen jellegű kéréseket.
- A többi thread a kéretlen levelek küldéséért felelős. Működésük feltétele az előbbi ellenőrzés sikeres kimenetele.

A szálak folyamatosan futnak mindaddig, amíg az összes spam küldése meg nem történik. Majd a Cutwail modul átlép egy másik üzemmódba, ahol meghatározott időközönként a következő spam feladatot próbálja lekérni a C&C szervertől.

Letöltött modulok – Pushdo kernel modul

A Pushdo kernel modul indítása a boot folyamat korai stádiumában történik. A kernel modul biztosítja, hogy a Pushdo a továbbiakban is működőképes legyen a fertőzött eszközön. Továbbá felelős azért, hogy megtörténjen a végrehajtása a memóriában.

A kernel modul egy dropper, végrehajtásakor ellenőrzi az aktuális Windows verziót. Majd kicsomagolja a kódja egy részét és befecskendezi a services.exe folyamatba. Ez a kód – melyre a későbbiekben „inner kernel driver" névvel hivatkozunk – felelős a Pushdo kernel műveleteiért.

Az inner kernel driver ellenőrzi az összes registry kulcsot, mely kapcsolatban áll a kernel modullal, így bizonyosodik meg arról, hogy nem távolították el a rendszerről.

Három visszahívó eljárás beállításával információt gyűjt a rendszer módosításairól és a lényeges eseményekről. Mindezt három kernel API hívással teszi:

- **IoRegisterFsRegistrationChange** – Ez a rutin egy fájlrendszer filter driver-t regisztrál, mely jelzést kap minden egyes fájlrendszer regisztrálásáról. Gyakorlatilag ilyen esemény a Windows betöltési folyamat, illetve az USB tárak felcsatolása, illetve eltávolítása. Ezen események eredményeként az inner kernel modul dekódolja a letöltő modult és befecskendezi azt a services.exe-be.
- **CmRegisterCallback** – A rutin egy registry visszahívó modult regisztrál, mely lehetővé teszi a registry műveletek megfigyelését, blokkolását valamint a módosítását. A driver elfogja a registry módosítást célzó kísérleteket és blokkolja mindazokat, melyek a Pushdo működését érintik.
- **PsSetCreateProcessNotifyRoutine** – A rutin a folyamatok létrehozását és törlését figyeli. Abban az esetben, ha új services.exe folyamat létrehozása történt meg, dekódolja a letöltő modult és befecskendezi a services.exe folyamatba.

A visszahívó hurkok telepítése után a kernel modul újból ellenőrzi a registry bejegyzéseket.

Letöltött modulok – Pushdo sniffer modul

A Pushdo sniffer modul elősegíti a spam statisztikák készítését, valamint az új email címek gyűjtését a fertőzött gépekről.

A letöltő modul a sniffer modult a következő helyre menti:

%WINDOWS%\systems\drivers\tcpsr.sys

A mentés után a letöltő modul elindítja a sniffer-t mint egy kernel eszköz vezérlőt. Ez lehetővé teszi a sniffer modul számára, hogy hurkolja az ndis.sys hálózati funkcióit. A modul lehallgatja a kimenő SMTP forgalmat a 25-ös porton. A lehallgatott adatokból kinyeri, majd tárolja az email címeket.

A sniffer végrehajtása után a letöltő modul eltávolítja a tcpsr.sys fájlt a merevlemezről, így rejtve el a Pushdo működését.

A letöltő modul aktívan kommunikál a sniffer vezérlővel, hogy kinyerje a címzettek adatait. Az adatok egy bizonyos méretének elérésekor HTTP POST kapcsolaton keresztül továbbításra kerül a begyűjtött információ egy megadott IP címre.

A metódus részletes információt szolgáltat nem csak a kiküldött kéretlen levelekről, hanem az összes észlelt címzettről is. Mindez lehetővé teszi, hogy a Pushdo megbizonyosodjon arról, hogy az előre meghatározott spam mennyiséget kézbesítette az ügyfelei részére.

A metódus egyik érdekes mellékhatása az, hogy a sniffer nem tesz különbséget a kéretlen és a legitim levelek között. Mindemellett a legitim címeket a bűnözői csoportok begyűjthetik és adatbázisukban tárolhatják.

Kampány modulok

A Pushdo egyik különleges jellemvonása az, hogy harmadik félhez tartozó káros szoftvereket képes kiszolgálni. A kutatás során a külső kártékony szoftverek számos példáját sikerült megfigyelni. A vizsgált szoftverek eltérő viselkedéssel bírtak. Minden jelentősebb frissítés esetén a Pushdo újrafertőzte a számítógépet a külső szoftverek újabb verzióival. Számos esetben az előbbi verziók eltávolítását követően.

A káros szoftver mögött – Botnet tulajdonosok

A botnet mögött álló motivációk kutatásának része volt a közvetlen kapcsolat a botnet tulajdonosokkal. A kapcsolathoz szükséges információk könnyen megszerezhetőek voltak a kéretlen levelekből. Jelen esetben ICQ számot és közvetlen vezetékes vonalat tartalmaztak a levelek.

Elsőként, biztonsági megfontolásból az ICQ csatornán történt a megkeresés. Az orosz üzenetek ICQ csatornán történő továbbításának árait többszöri próbálkozással sem sikerült kideríteni. Minden esetben az eredeti kéretlen levél érkezett válaszként. Úgy tűnik, hogy a botnet tulajdonosok egy automata botot alkalmaztak, mely az ICQ listára küldött üzenetekre a legfrissebb árlistát küldik válaszul. Mivel a kapcsolatfelvétel ezen módja nem hozott gyümölcsöző eredményt, ezért közvetlen hívással folytatódott a botnet tulajdonosok megkeresése.

Először egy orosz mobil telefon beszerzése történt meg, melynek segítségével a hívások bonyolítása történt. A hívott telefonszám egy moszkvai vezetékes szám volt. Két független hívás során – első alkalommal magánszemélyként egy erotikus website reklámozásával kapcsolatban, másodjára fuvarozási szolgáltatás hirdetésével kapcsolatban – sikerült érdekes információkat szerezni.

A hívások során a választ adó személy segítőkészen rámutatott a http://advert1.ru weboldalra, ahol a kéretlen leveleknél jóval részletesebb információ található az árakkal kapcsolatosan.

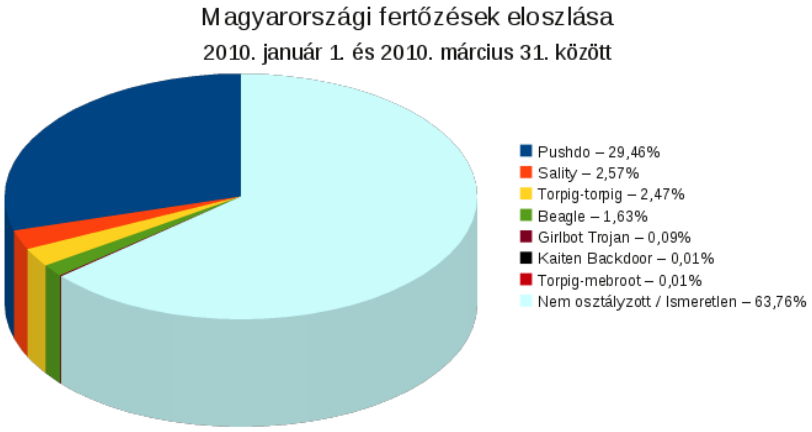
Két alternatív fizetési mód volt választható. Az első szerint egy futár gyűjtené be a szolgáltatás ellenértékét. Ez az opció csak Moszkva körzetében élő lakosok számára érhető el. A másik lehetőség a banki átutalás. A fizetés módjától függetlenül, legális számlát biztosítanak, a befizetett összegről hirdetési címén.

A szállítmányozással foglalkozó vállalkozás számára a botnet tulajdonosok egy egyszerű weboldal készítését is felajánlották. Mivel így jelentős mértékben növelhető a spam kampány sikerességi rátája. Mindkét esetben felajánlották a levelek optimalizálását, hogy megkerüljék a legtöbb anti-spam szolgáltatást.

A felvetett jogi aggodalmakra reagálva, biztosítottak arról, hogy a kéretlen levelek küldésének gyakorlata nem illegális Oroszországban.

A Pushdo terjedése

A Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary) együttműködik a Shadowserver Foundation szervezettel, melynek célja, hogy felderítse és felszámolja az interneten található botnet hálózatokat, azok klienseit, valamint az irányításukhoz szükséges C&C szervereket. A Nemzeti Hálózatbiztonsági Központ − mint Nemzeti Kapcsolati Pont − 2008. II. negyedévétől, napi szinten jelentést kap a Shadowserver Foundation-tól a magyarországi botnet kliensekről és a C&C szerverekről.



21. ábra

A riportokban szereplő bot fertőzések elemzését szemlélhetjük a 21. ábrán. Jól kivehető, hogy az adott időszakban a leggyakrabban észlelt ismert fertőzés a Pushdo volt, mely az összes érzékelés 29,46%-át tette ki.

A Pushdo egy különleges botnet abban az értelemben, hogy nem önreprodukáló. Más botnetek féreg viselkedési formával rendelkeznek és gépről gépre terjednek a hálózaton. Esetleg spam motorjukat használva linkek és csatolmányok segítségével fertőznek. Ugyanakkor a Pushdo egyik technikát sem alkalmazza.

A terjedés egyedül a weben történhet. Számos tanulmány[19] rámutat arra, hogy a telepítő fájlt más, jól ismert malware család – mint a PE_VIRUT, a TROJ_EXCHANGER és a TROJ_BREDOLAB – közvetítette.

Úgy tűnik, hogy a Pushdo más malware csoportokkal megállapodott a csoportok szoftvereinek telepítéséről. Mindez elősegíti a Pushdo rejtőzködő gyakorlatát.

19 http://blog.fireeye.com/research/2009/04/botnetweb.html#

Referenciák

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PANDEX.A&VSect=Sn

http://www.messagelabs.com/mlireport/MLIReport_2009.01_Jan_Final.pdf

http://royal.pingdom.com/2009/01/22/internet-2008-in-numbers/

http://www.virusbtn.com/virusbulletin/archive/2008/03/vb200803-pandex

http://www.secureworks.com/research/threats/topbotnets/?threat=topbotnets

http://blog.fireeye.com/research/2009/04/botnetweb.html

http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

http://Shadowserver.org

A VirusBuster Kft. összefoglalója 2010 első negyedévének IT biztonsági trendjeiről

Melyek voltak az új évtized első negyedévének legfontosabb, trend értékű jelenségei, hírei az informatikai biztonság területén? Beszámolónkban előbb erre a kérdésre keressük a választ, majd a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk a 2010. január-március időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól.

Negyedéves összefoglalónk főbb témái:

1. Halászat - az adatok tengerén
2. Vadászat - site-ra, szellemi tulajdonra
3. Halőrök, vadőrök - biztonságpolitika
4. Mobil veszedelem
5. Áradó levélszemét
6. Folt hátán folt
7. "Kiemelkedő" kártevők

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

Halászat - az adatok tengerén

Januárban történelmi csúcsra hágott az adathalász támadások száma. Az idei év első hónapjában 21 százalékkal több próbálkozást regisztráltak, mint tavaly decemberben - mutatott rá az RSA Security biztonsági cég elemzése. Az online csalásokról szóló jelentés (Online Fraud Report) szerint 2010 első hónapjában 18.820 támadást észleltek, több mint kétszer annyit, mint egy esztendővel korábban.

Valamennyi derűlátásra ad okot, hogy a célba vett márkák száma 2009 decemberéhez képest csak 2 százalékkal emelkedett. Ugyanakkor 35 szervezet most januárban szenvedte el élete első támadását - ez az adat több mint háromszorosa a decemberinek.

Mint a jelentésből kiderül, mind gyakrabban kerülnek a bűnözők célkeresztjébe az amerikai egyetemek. Egyre több esetben találkozni a felsőoktatási intézmények portálját vagy webmail szolgáltatását leutánzó csalárd lapokkal.

Továbbra is az Egyesült Államokból indult ki a legtöbb támadás: Amerika részesedése decemberhez képest januárra 12 százalékkal, 57 százalékra nőtt. Ugyan Kína maradt a második helyen, de az itt hosztolt adathalász lapok aránya 17-ről 9 százalékra zsugorodott. A harmadik helyet Dél-Korea, a negyediket Németország foglalta el, 8, illetve 6 százalékkal. És melyek voltak a legnépszerűbb

célországok? Egyesült Államok (48 százalék), Nagy-Britannia (34 százalék), Olaszország (5 százalék).

Persze az adathalászok magyar vizeken is kivetették hálójukat. Januárban egy hét leforgása alatt kétszer kényszerült arra a CIB Bank, hogy ügyfeleit ilyen támadásra figyelmeztesse.

Még szerencse, hogy - bár a CIB honlapját igazán élethűen sikerült leutánozniuk -, magyarul nem tudtak a bűnözők. Így csalinak szánt, hibáktól hemzsegő, nyilvánvalóan gépi fordítással készült e-mailjüknek - melyből a VirusBuster munkatársaihoz is jutott - remélhetőleg senki nem ült fel.

Tájékoztatóiban a CIB hangsúlyozta: "az e-maileket véletlenszerűen küldik el nagy mennyiségben interneten megtalálható e-mail címekre, tehát nem a CIB Bank ügyfél-adatbázisában található e-mail címekhez fértek hozzá". Hozzátették: a bank semmilyen esetben nem kéri sem e-mailben, sem SMS-ben az ügyfelei azonosítóit és nem is szólítja fel őket ezek megadására vagy megváltoztatására.

Ha nyelvünk ritkasága egyelőre véd is valamennyire, azért nem árt az óvatosság. Kis körültekintéssel - például jelszavaink gondos megválasztásával - nagy bajt előzhetünk meg.

Mondjuk ezt azért, mert mint a Trusteer online biztonsági cég nemrég közzétett adataiból kiderül, a webbankoló polgárok 73 százaléka használja a számlájához megadott jelszót más, kevésbé érzékeny site-on is. Mi több, a pénzintézeti ügyfelek csaknem fele (47 százaléka) nemcsak a banki jelszót, hanem egyenesen a felhasználónév-jelszó párost alkalmazza más webhelyekre való belépésre.

A kutatók azt találták: ha a bank megengedi, hogy az ügyfél maga válasszon felhasználónevet, akkor a "felhasználónév-újrahasznosítás" aránya eléri a 65 százalékot. Ha a nevet a bank osztja ki, akkor valamivel kedvezőbb a helyzet: "csak" az ügyfelek 45 százaléka él ugyanazzal az azonosítóval más site-on.

Mi a következmény? Ha valaki véletlenül bedől egy számítógépes bűnöző trükkjének, s kiadja - mondjuk - egy közösségi portálhoz használt belépési azonosítóit, akkor a hackernek nagy esélye van rá, hogy ugyanazzal a felhasználónév-jelszó párossal az illető bankszámlájához is hozzáférjen.

Legyen legalább három online azonosító-készletünk! - ajánlja a Trusteer. Egyet csak pénzügyi site-okon használjunk, egyet tartsunk fönn az olyan webhelyekre, ahol nyilvántartják a személyazonosságunkat, végül a harmadikkal a kevésbé érzékeny tájakon szörföljünk! Ez persze még csak az első lépés, hiszen az is nagyon fontos, hogy kellően erős jelszót válasszunk - olyat, amelyet automatikus módszerekkel (szótárral, próbálkozással) nem lehet feltörni

Vadászat - site-ra, szellemi tulajdonra

Szegény embert az ág is húzza. Botrányok, hideg és hó miatti leállások közepette januárban a BKV-ról ráadásul még az is kiderült, hogy site-ja fertőző lapot tartalmaz. A bkv.hu galériáján található "rendesen összekuszált JavaScript kódról elsőként a Buhera blog számolt be. A kártékony program egy orosz domainen keresett további futtatható kódokat. *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője elmondta: a bkv.hu-n talált kód a karácsonyi ünnepek után árasztotta el a világhálót. Meglehetősen kevés biztonsági cég szoftverje ismerte fel - a VirusBuster közéjük tartozott.

Míg kis hazánkban a BKV körül kavargott a por, a világ szeme Amerikán és Kínán volt. Öt kontinensen került a lapok címoldalára: feltehetően Kínából kiinduló "rendkívül kifinomult és jól célzott" hackertámadást intéztek összesen 34 nagy amerikai cég ellen. Először a Google számolt be a szellemi tulajdona elleni akcióról, ám lapértesülések szerint a célpontok között volt a Yahoo, a Symantec, a Northrop Grumman és a Dow Chemical is.

A Microsoft tájékoztatóval reagált, melyben megerősítette: a hackerek az Internet Explorer régebbi, 6-os változatának egy újonnan felfedezett sérülékenységét aknázták ki. A szoftveróriás soron kívüli folt kibocsátásával sietett betömni a rést.

Ugyanakkor az Egyesült Államok diplomáciai jegyzéket intézett a kínai kormányhoz az eset miatt. *Philip Crowley* külügyminisztériumi szóvivő közölte: "aggodalmunkat fejezzük ki az incidens miatt, s kérni fogjuk Kínától: magyarázzák meg, hogyan történt, s mit szándékoznak tenni az ügyben". Maga az első számú célpont, a Google március végén bezárta addigi kínai portálját, s az ázsiai ország keresőit hongkongi honlapjára irányítja át.

Akár válaszgesztusnak is tekinthető, hogy a kínai hatóságok az incidenst követően, februárban nyilvánosságra hozták: még novemberben bezártak egy céget, amely a vád szerint kémprogram-fejlesztésre és online támadásokra tanított be hackereket. Három személyt letartóztattak, a Black Hawk Safety Net elnevezésű vállalkozást pedig bezárták a rendőrök a Kína középső területén fekvő Hubei tartományban. A Xinhua hírügynökség szerint a cég az ország legnagyobb hacker-kiképző site-ját üzemeltette. Tizenkétezer fizető tagjának hacker eszközöket és trójai programokat kínált, további 170 ezer ingyenes, regisztrált felhasználójának pedig egy szűkített eszközkészletet. A céget kiberbetörő tanfolyamok szervezésével is vádolják.

Jóllehet a Google-incidens lezárult, nem árt, ha a cégek körülnéznek a házuk táján. Bárkit érhet baj: nem kevesebb, mint a programok 58 százaléka ad módot potenciálisan a Google-t ért támadáshoz hasonló hacker-akcióra - figyelmeztetett egy alkalmazásbiztonságra specializálódott cég, a Veracode.

Halőrök, vadőrök - biztonságpolitika

A támadások közepette világszerte szerveződik a védelem is. Március végén tartotta például ötödik éves tanácskozását a számítógépes bűnözésről az Európa Tanács. A strasbourgi konferencia résztvevői a nemzetközi együttműködés javítását szorgalmazták, hogy jobban ki lehessen aknázni a rendelkezésre álló eszközöket, s az országok átvehessék a másutt jól bevált módszereket, kezdeményezéseket. Ugyanilyen fontos a bűnüldözés és az ipar együttműködésének bővítése - hangsúlyozták.

Támogatásukról biztosították a delegátusok az ICANN javaslatát, miszerint szigorítani kellene a domainregisztrációs szabályokat. Mint elhangzott, a rendőrségnek a számítógépes bűnözés elleni küzdelemben fel kellene tudnia használni a WHOIS adatbázist - persze úgy, hogy ne sértse a regisztrálók személyiségi jogait. Több ajánlást tett a konferencia a felhő alapú technológia elterjedésével összefüggő biztonsági és adatvédelmi problémákkal kapcsolatban is.

Az európaiak felszólították a brazíliai Salvadorban áprilisban megrendezendő 12. ENSZ Bűnmegelőzési és Igazságszolgáltatási Konferencia résztvevőit: fogadják el a kiberbűnözés, az elektronikus kémkedés és a kapcsolódó fenyegetések elleni globális akciótervként az Európa Tanács

Budapesten 2001-ben lefektetett Számítástechnikai Bűnözésről Szóló Egyezményét. A szerződést eddig 29 - jórészt európai - ország ratifikálta, de csatlakozott hozzá az Egyesült Államok is. Portugália és Montenegró a mostani konferencia alatt lépett be a táborba, s Argentína ugyancsak jelezte: elfogadná az egyezményt. Nagy-Britannia, Spanyolország és 17 további állam aláírta, de még nem ratifikálta a szerződést.

Rímel az európai konferencián elhangzottakra, hogy Oroszországban megszigorították a domain-regisztrációt. Április 1-jétől csak azonosító okmányok felmutatásával lehet „.ru" kiterjesztésű domain-nevet bejegyeztetni. Az orosz legfelső szintű domaint kezelő koordinációs központnál magánszemélyeknek az útlevelüket, vállalkozásoknak pedig a cégkivonatukat kell bemutatniuk.

Biztonsági szakemberek és az amerikai bűnüldöző hatóságok szerint Oroszország azért olyan népszerű a számítógépes nehézfiúk körében, mert a kontinensnyi államban rendkívül nehéz bíróság elé állítani őket. Így a spammerek, kártevő-terjesztők és társaik szinte büntetlenül tevékenykedhetnek. Az új rendelkezés célja, hogy a kiberbűnözők ne tudjanak olyan könnyen hamis néven domaint bejegyeztetni. Elvégre, ha hamis papírokat is be kell szerezniük, az mégiscsak drágább és tovább tart. Az ugyancsak hacker-paradicsomként számon tartott Kína decemberben vezetett be hasonló szabályokat.

Különösen fontos az országok kritikus infrastruktúrájának védelme. Folyamatosan támadják az energetikai, olaj- és más, létfontosságú szektorok számítógépes rendszereit - figyelmeztetett nemrég egy jelentés.

A kritikus infrastruktúrával foglalkozó szervezeteknek több mint kétszer nagyobb esélyük van arra, hogy kibertámadás érje őket, mint más területen működő társaiknak - állapítja meg a biztonsági szolgáltatásokat értékesítő ScanSafe legfrissebb, kockázatokat áttekintő éves tanulmánya. A cég az elmúlt esztendőben regisztrált egybilliónál több webes kérés feldolgozása alapján jutott erre az eredményre. Mint kiderült, az adatlopó trójaiak elsősorban az energetikai, olaj-, gyógyszer- és vegyipari, kormányzati, valamint a banki-pénzügyi szférában tevékenykedő szervezeteket veszik célba.

"A magánszemélyek hitelkártya-adatainak értéke eltörpül az infrastruktúra, illetve az azzal foglalkozó szervezetek szellemi tulajdonának értéke mellett. Az üzenet világos: az informatikai háború már folyik. A csatamező a web, a vállalatok pedig a frontvonalon vannak" - kommentálta az eredményeket *Mary Landesman,* a ScanSafe vezető biztonsági kutatója.

Mobil veszedelem

Nemcsak a gazdáik szeretik az okostelefonokat, hanem a hackerek is. Úgy tűnik, egyre inkább igaz lesz ez az állítás. Erre ékes bizonyíték egy Spanyolországban történt eset. Akár háromezer ottani Vodafone ügyfelet is érinthetett az a fertőzés, amely a mobilóriás ibériai leányvállalata által szállított HTC Magic okostelefonokat sújtotta.

Március elején érkezett az első híradás arról, hogy egy spanyol vodafone-os HTC Magic fertőzötten került a vásárlóhoz: microSD kártyáján a Mariposa botnet adatlopó kliense mellett több más rosszindulatú programot is felfedeztek. Nem sokkal később egy második esetet jelentettek. Végül a Vodafone bejelentette: háromezer HTC Magic microSD kártyájának lecserélését tervezi, mivel feltételezi, hogy azok is fertőzöttek.

Áradó levélszemét

Nemrég jelent meg a Commtouch internetes fenyegetés-trendekről szóló jelentése 2010 első negyedévéről. Ebből kiderül: az időszak folyamán a teljes e-mail forgalom átlagosan 83 százaléka levélszemét volt. A legmagasabb spamszintet - 92 százalékot - márciusban mérték. Viszonylag a legkevesebb kéretlen levél - a teljes forgalom "mindössze" 75 százaléka - az év elején keringett.

Csakúgy, mit az előző negyedévben, most is a gyógyszer volt a spammerek legkedveltebb témája. A kéretlen levelek 81 százaléka ajánlott valamilyen orvosságot. Messze elmaradva - szintén hagyományosan - az (óra)utánzat-ipar következett, 5,4 százalékkal.

Hasonló adatokról számolt be a VirusBuster spamlaborja is, amely ugyancsak 80 százalékra teszi a kéretlen gyógyszerreklámok részesedését a levélszemétből. A hazai cég azt tapasztalta, hogy 5-10 százalék körüli a pornót ajánló üzenetek aránya, a fennmaradó pár százalékon pedig online egyetemek, főiskolák, karóra-másolatok, kaszinók, torrentek osztoznak. (Az utóbbi nagyméretű állományok, leginkább videók letöltését segítő rendszer). Magyar spamből viszont - 90 százalék körüli részesedéssel - a torrent téma az abszolút rekorder. Emellett kisvállalkozások próbálnak üzenetek szórásával piacot szerezni, kihasználva, hogy ezt - amíg nem sértik a versenyszabályokat - semmi sem szankcionálja.

"A csalárd levelek között sok szól állítólagos nyereményekről. Újabban már a Coca Cola vagy a Shell is "sorsol ki" e-mail címeket. Újdonság, nagyjából az utóbbi fél év jellemzője az online játékok jelszavait megszerezni próbáló adathalászat. Ugyanakkor úgy tűnik, hogy a banki adathalászat némileg visszaszorult. Művelői talán az újabb nagy akciókra készülnek, de az is lehet, hogy az óvatosabb és tapasztaltabb felhasználók már nem dőlnek be olyan könnyen - mondja *Stange Szilárd,* a VirusBuster technológiáért felelős termékmenedzsere. - Elég sok viszont a trójai spam, vagyis az olyan üzenet, amely kártékony szoftvert próbál a címzett gépére csempészni. A trójai programot általában csatolmány tartalmazza, tömörítve vagy szövegnek (dokumentumnak) álcázva, de néha csak link mutat rá.

Szerencsénk, hogy a számítógépes bűnözők, akik eddig hazánkban próbálkoztak - ritka kivételtől eltekintve - nem tudtak magyarul, a fordítógépek pedig (egyelőre) annyira törik a magyart, hogy rögtön szemet szúr az idegenség mondjuk egy banki adatok után tudakozódó levél esetében.

Folt hátán folt

Bőséggel kaptak biztonsági frissítéseket a legelterjedtebb szoftverek az elmúlt hónapokban is. A következőkben a Microsoft, az Adobe és az Oracle foltjairól szólunk röviden, időrendben.

Január

Januári foltozó keddjén (12-én) egyetlen - kritikus - javítócsomagot jelentetett meg a Microsoft.

Nagyobb jelentőséget tulajdonítottak a szakemberek az ugyanakkor napvilágot látott Adobe frissítéseknek. Az Adobe PDF-szoftverek (a Reader és az Acrobat) sérülékenységeit már december közepe óta támadták a hackerek. Az Adobe Reader és az Acrobat 9.2-es vagy korábbi verzióival Windows, Macintosh és Unix környezetben dolgozóknak a programok 9.3-as változatára, az

Acrobat 8.1.7 felhasználóknak a 8.2-re kellett áttérniük.

A fentiekkel egy időben az Oracle is biztonsági frissítésekkel jelentkezett: 24 javítócsomaggal tette védettebbé termékpalettáját.

Január 21-én azután soron kívüli javítócsomagot bocsátott ki az Internet Explorer valamennyi változatára a Microsoft. Így tömte be azt a rést, amelyen keresztül egy sor amerikai vállalatot - köztük a Google-t - ért online támadás.

Február

Február 9-e 13 biztonsági frissítéssel tette védettebbé a Microsoft-felhasználókat. A foltok a Windows és az Office sérülékenységeit orvosolták. A 13 foltból 5 kapott "kritikus" minősítést. Hét javítócsomagot a "fontos", egyet pedig a "mérsékelten fontos" kategóriába sorolt a szoftveróriás.

Pár nappal utóbb bejárta a világsajtót a hír: az egyik javítócsomag, az MS10-015-ös telepítése után a gép újraindításakor egyes felhasználók rendszere végtelen indítási ciklusba került. A jelenség nem volt általános - a VirusBusternek például egy esetet sem jelentettek -, ám elszigeteltnek sem volt mondható. A problémát az érintett gépek fertőzöttsége okozta.

"Valójában nem egyetlen károkozóról, hanem egész kártevő-családról volt szó, melynek újabb és újabb változatai jelentek meg. Érdekesség, hogy elkészült már egy olyan variáns is, amely kompatibilis az említett MS10-015-ös folttal. A VirusBuster szoftvere a legtöbb változatot Rootkit.Alureon.Gen néven ismeri fel - magyarázza *Szappanos Gábor,* a cég víruslaboratóriumának vezetője. - Naprakész szoftverrel dolgozó felhasználóink biztonságban vannak, nyugodtan telepíthetik a szóban forgó foltot."

Persze a Microsoft sietett kijavítani, s újra kibocsátani az MS10-015-ös foltot.

Február közepén minden platformon frissíttette a Flasht az Adobe, hogy orvosoljon egy potenciálisan veszélyes sérülékenységet.

Az Oracle egy szerver-sérülékenységre bocsátott ki soron kívüli foltot. A javítócsomag az Oracle WebLogic Server csomópont-kezelő (Node Manager) összetevőjének hibáját orvosolta.

Március

Március 9-ei menetrendszerű foltozó napján a Microsoft két biztonsági frissítéssel jelentkezett. A foltok a Windows és az Office sérülékenységein segítettek; mindkettő "fontos" minősítést kapott. Két héttel következő, áprilisi foltozó keddje előtt pedig betömött a Microsoft egy, az Internet Explorer 6-on és 7-en tátongó rést, amelyet mind erősebb ostrom alá vettek a hackerek. Ez a soron kívüli, MS10-018-as számú folt a böngésző valamennyi támogatott verziójára "kritikus" minősítést kapott. Jóllehet a folt védelmet nyújt a támadások ellen, a Microsoft sürgette az IE 6-tal és 7-tel dolgozókat: mielőbb térjenek át a böngésző legfrissebb, biztonságosabb 8-as kiadására.

"Kiemelkedő" kártevők

Április 1-jén volt egy éve, hogy a Conficker féreg feléledésétől rettegett a világ, így talán elsőként minden idők eme legkiemelkedőbb kártevőjéről érdemes megemlékeznünk. Jóllehet az egy évvel ezelőttre beprogramozott parancskérő napon végül semmi sem történt, a fertőzött gépek számát még ma is 6,5-15 millióra becsülik.

Az elmúlt negyedév legnevezetesebb Conficker-felbukkanása kétségkívül Nagy-Britanniában volt. A féreg miatt több napra le kellett kapcsolni a nagy-manchesteri rendőrséget a brit országos rendszerről.

Hogy ki(k) áll(nak) a féreg mögött, s milyen céllal szabadították "alkotásukat" a világra, azt csak találgatni lehet. A bűnüldöző szervek és a Conficker Munkacsoport (Conficker Working Group) folyamatosan éberen figyelik a megfertőzött gépeket, s ez valószínűleg nem kis szerepet játszik abban, hogy a hackerek azóta sem vették igénybe az uralmuk alatt lévő gigászi botnetet: nem küldtek vele spamet, nem indítottak szolgáltatásmegtagadási (DoS) támadást, sem más szembetűnő akciót.

A Conficker első változata 2008 novemberében bukkant fel. Egy akkor frissiben betömött Windows-rést aknázott ki. Később elsősorban pen drive-okon és nem kellően védett hálózatmegosztásokon kezdett terjedni. A féreg A és B variánsa összesen mintegy 6,5 millió gépet fertőzött meg. A kártevő újabb, C változata P2P módon terjedt, de elterjedtsége az elmúlt egy év folyamán lassan csökkent. Mind több áldozat tisztította meg gépét, így a C variánssal fertőzött PC-k száma a 2009 áprilisi 1,5 milliós csúcsról napjainkra 210 ezer körüli értékre esett. Egy esztendővel ezelőtt látott napvilágot a Conficker E, amelyet azonban írói úgy programoztak, hogy egy hónappal később törölje magát. Így ez a variáns gyakorlatilag eltűnt.

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. január-március időszakra az alábbi kártevő-gyakorisági lista állt elő:

Kártevő	Részesedés (%)
Backdoor.IRCBot.AAWX	23,04%
Trojan.DL.Agent.SKIT	6,69%
Trojan.Kryptik.LTJ	6,59%
Backdoor.Nepoe.GX	6,54%
Trojan.Buzus.AWEC	5,94%
Trojan.DigiPog.BV	5,20%
Trojan.FakeAV.TF	4,54%
Backdoor.Bandok.GT	4,49%
Trojan.Kryptik.MJR	4,27%
Trojan.FraudPack.YEC	3,52%
Egyéb:	29,19%

Az első helyet egy IRC bot kártevő foglalja el, vagyis egy olyan féreg, amely az MSN Messengeren, illetve a Windows Live Messengeren terjed, s a hacker számára az IRC (Internet Relay Chat) csatornán át nyit hátsó ajtót - hozzáférést - az áldozat gépéhez.

A negyedéves toplista többi szereplője szinte kivétel nélkül mind hamis antivírus alkalmazáshoz köthető kártevő. Ezek az úgynevezett trójaiak fertőzéssel riogatnak, s hamis antivírus programot töltenek le az áldozat gépére - magyarázza *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője. Mit csinál egy hamis vírusirtó? A gép megtisztításával kecsegtet, ám valójában vagy semmit nem végez - ez a jobbik eset -, vagy valamilyen kártékony tevékenységbe fog. Akárhogy is, készítői pénzt kérnek érte - vagyis a trójaiak egy csalárd üzleti vállalkozás eszközei.

Maguk a trójaiak e-mail csatolmányként érkeznek. A kéretlen levelek feladói valamilyen hasznos állománynak - például megrendelés visszaigazolásának - álcázzák őket, ha azonban megnyitjuk a csatolmányt, már meg is fertőződtünk.

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.

Íme január-március legaktívabb kártevő-terjesztő domainjei:

Domain	Földrajzi hely	Fájlok száma	Kártevő-család
cfteam.net	Dél-Korea	492	Virut
screenblaze.com	Houston, USA	346	Delphi.BSO
host127-0-0-1.com	Shalimar, USA	265	Swizzor
rapidshare.com	Németország	220	FakeAlert, Zbot, Palevo
host192-168-1-2.com	Shalimar, USA	183	Swizzor
fileave.com		180	
ripway.com		122	
sunqtr.com	La Habra, USA	109	CKSPost
justfree.com	Gaithersburg, USA	94	LdPinch
3322.org		93	

Táblázatunkban a régóta ismert adware (reklámhordozó) Swizzor kártevő-család a legjelentősebb. Figyelemre méltó, hogy a számítógépes bűnözők saját üzemeltetésű webszerverek helyett nyilvános, ingyenes lerakatokról kezdték el terjeszteni "portékájukat". Ilyenek táblázatunkban a Rapishare, a Fileave és a Ripway. A fő terjesztési pontok listáját amerikai városok uralják.

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 "Fair Business" minősítést kapott, s ugyanebben az évben a cég nyerte el a kisvállalati kategória Üzleti Etikai Díját.

Minősített etikus hekkerek

Az autógyártás területéhez hasonlóan az informatikában is nélkülözhetetlen munkafolyamatnak kellene lennie a biztonság növelését szolgáló töréstesztnek, melyet a szoftvergyárak megfelelő laboratóriumaiban az adott szoftverekre és az érzékeny biztonsági területekre is kiképzett szakemberek végeznek. Azonban a szoftvergyártás esetében ez távolról sincs így. Egy kézen meg lehet számolni a biztonságra ezen a szinten is törekvő szoftvervállalatok számát. Így hát a „törésteszt" külsősökre hárul: fekete- és fehérkalapos hackerekre.

Ne tévedjünk: a biztonsági hibákat, például távoli kódfuttatást lehetővé tévő exploitokat „valakik" mindig megtalálják. A kérdés csupán az, ki ez a valaki? Vagy még inkább így: ki a gyorsabb? Természetesen az informatikai rendszerek üzemeltetőinek kellene gyorsabbnak lennie - ha a megfelelő szakértelem meglenne a vállalatoknál, intézményeknél. Ha lenne legalább egyetlen ember, aki úgy gondolkodik, mint egy hacker, és rutinosan használja azt az ezernyi hekkereszközt, amely a „piacon" ma megtalálható.

Mondjuk ki: amíg a vásárolt, valamint a házilag írt szoftverek olyanok, amilyenek (vagyis bugosak), addig minden intézménynél szükség van olyan szakemberekre, akik a beüzemelt mission critial ócskaságot biztonsági szempontból megvizsgálják, és körbebástyázzák olyan módon, hogy az ismert réseken ne lehessen áthatolni.

A fehérkalapos, vagy etikus hackelés bizalmi kérdés, ezért ér egyre többet piacon a Certified Ethical Hacker minősítés, melynek megszerzéséhez nemzetközi minősítési kritériumokat kell sikeresen teljesítenie a jelöltnek. A folyamatba a szakmai vizsgán kívül beletartozik az illető hiteles azonosítása is (a közhiedelmet megcáfolva: „C" osztályú nemzetbiztonsági átvilágítás viszont nem). Mivel egyelőre kevesen vannak (Magyarországon száz fő körüli ilyen szakember található), a CEH-ek igencsak keresettek a munkaerőpiacon. Tízezer vállalatra jut száz fő… gyatra arány. Van hová javulni!

Talán ennek is köszönhető, hogy ezen a területen a magyar növekedési mutató világviszonylatban is kiemelkedő: egyelőre könnyű duplázni. Az USA-ban, ahol pár évvel korábban felismerték az etikus hekkerek jelentőségét, már nehezebb jelentős növekedést elérni, bár ez 2010 tavaszán megtörtént. Amikor a Pentagon összes informatikai dolgozójára kiterjesztették mind a képzést, mind a vizsgakényszert(!), hirtelen 5-6000 fővel nőtt a CEH-minősítéssel rendelkezők száma az országban és a Pentagont követve a sor folytatódik, folytatódni fog.

Szerencsére hazánkban is elérhetők a Certified Ethical Hacker minősítést nyújtó képzések, melyek az alaptudnivalóktól a specializációkig terjednek (VoIP-szakértő, Secure Programming guru, Penetration Tester és még a cybernyomozó, Forensic Investigator is). Ezen képzések szükségességére és népszerűségére jellemző, hogy a piac majdnem minden szegletébe elhatoló világválság ide nem tudta betenni a lábát: a hackerképzések megszokott létszámmal rendületlenül folynak.

Az idei év slágerképzése egyébként a cybernyomozó (Forensic Investigator). Ez két dolgot jelez:

1.) sajnos van mit nyomozni a magyar intézményeknél;

2.) a megelőzés helyett a tűzoltásra „fektetjük a hangsúlyt”. Ma még. Egyre több intézmény azonban már a megelőzésnél tart. Ehhez kellenek az etikus hekkerek. Nem az etikus kóklerek, hanem a Certified Ethical Hackerek.

Fóti Marcell

A NetAcademia Oktatóközpont és az EC Council Magyarország vezetője
http://www.netacademia.net

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