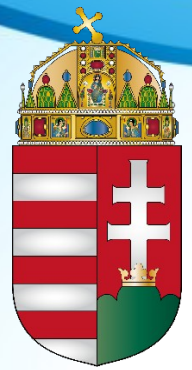
Nemzetbiztonsági Szakszolgálat
Kormányzati Eseménykezelő Központ
GovCERT-Hungary
A Kormányzati Eseménykezelő Központ működésének tapasztalatai

2014. október 08.



GOV CERT MAGYARORSZÁG

NBSZ

Tartalom

GOV CERT MAGYARORSZÁG NBSZ

I./1. Jogszabályi háttér

- **2013. évi L. törvény -** http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.240508
- 301/2013. (VII. 29.) Korm. rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=162279.246005
- **233/2013. (VI. 30.) Korm. rendelet** - http://njt.hu/cgi_bin/njt_doc.cgi?docid=161528.244306
- 65/2013. (III. 8.) Korm. rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=159312.244293
- 1491/2013. (VII. 29.) Korm. határozat - http://njt.hu/cgi_bin/njt_doc.cgi?docid=162282.246014
- 1**139/2013. (III. 21.) Korm. határozat** - http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
- 73/2013. (XII. 4.) NFM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=165312.253034
- 26/2013. (X. 21.) KIM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717
- 34/2013. (VIII. 30.) NGM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=162762.247199
- 16/2013. (VIII. 30.) HM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=162751.247185
- 36/2013. (VII. 17.) BM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=161994.245440
- 484/2013. (XII. 17.) Korm. rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=165583.253867
- 77/2013. (XII. 19.) NFM rendelet - http://njt.hu/cgi_bin/njt_doc.cgi?docid=165667.254105

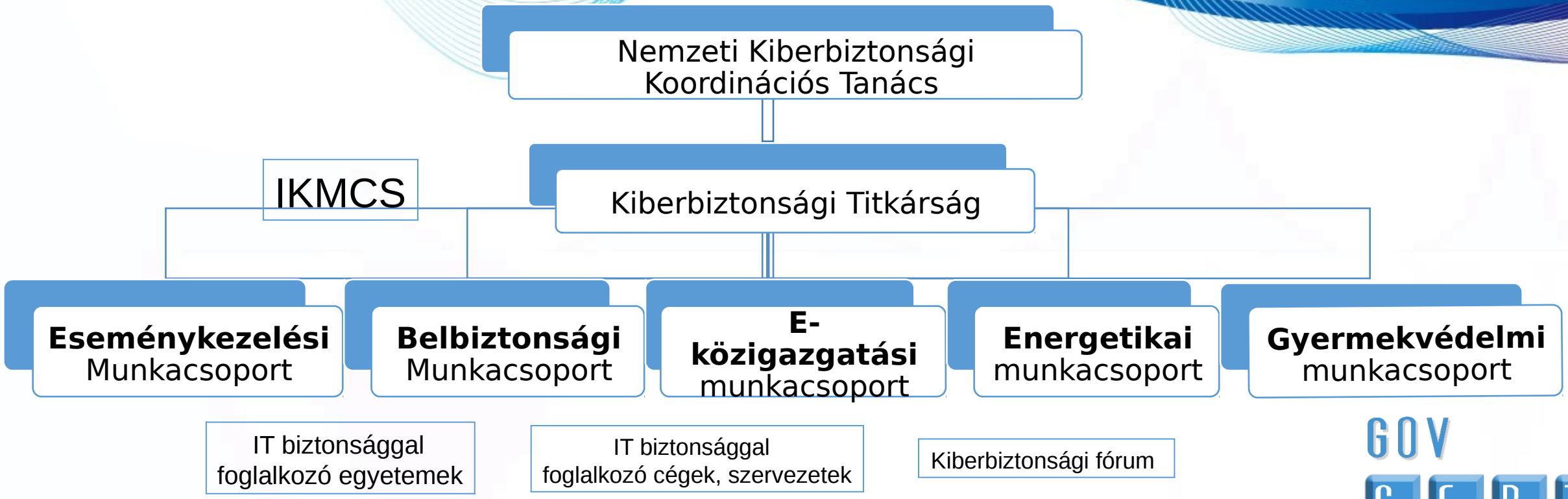
GOV CERT MAGYARORSZÁG NBSZ

A jogszabályi környezet felülvizsgálata

- A törvény szervi hatályának kérdése
- Határidők és szankciórendszer
- Két szintű eljárásrend egyértelmű rögzítése a vonatkozó jogszabályokban
- Ibtv.-ben megjelenő továbbképzési szisztéma pontosítása
- Az incidens bejelentés„egy csatornássá” tétele, a hatóságok közötti együttműködés rendjének pontos kidolgozása
- A szakhatósági tevékenység felülvizsgálata
- A biztonsági szintmegállapításának és ellenőrizhetőségének problémája
- Pontatlan megfogalmazás a hiánypótlás jogintézmények kapcsán
- Továbbképzési szisztéma pontosítása - adatszolgáltatás, adatközlés, adatvédelem -
- Nemzeti és ágazati CERT-ek meghatározása
- Munkacsoportok munkájának, hatáskörének meghatározása
- IBTV és LRTV / IBTV és ÖTV összehangolása

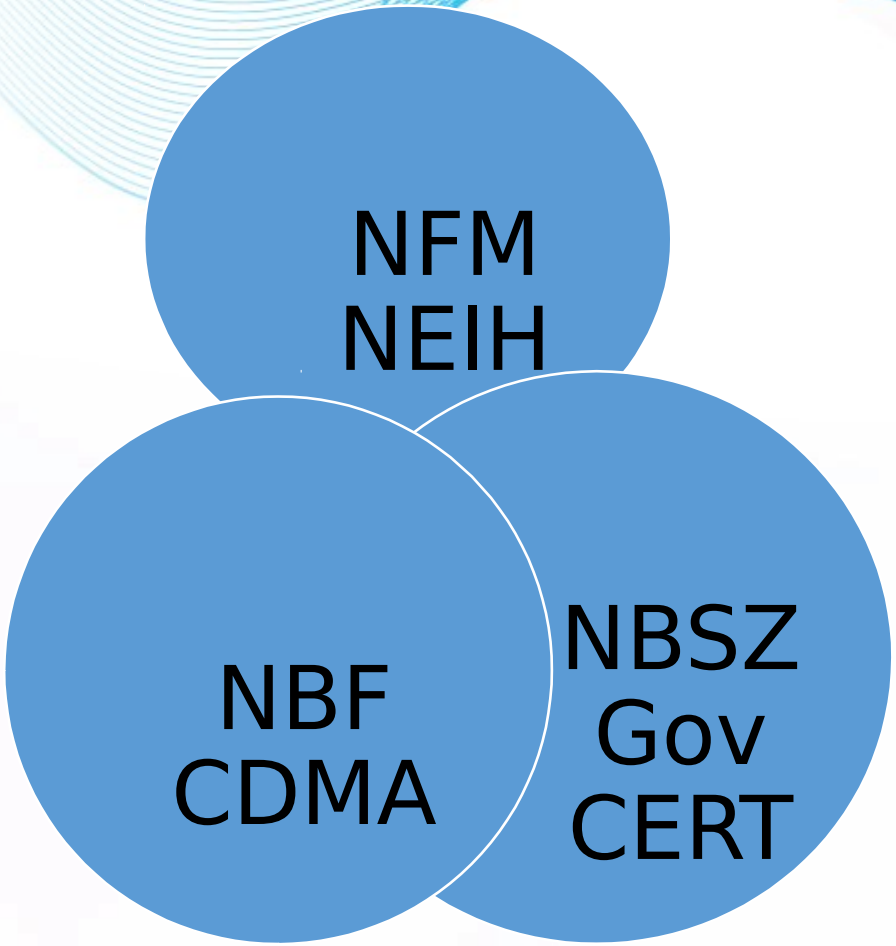
GOV CERT MAGYARORSZÁG NBSZ

II. Kiberbiztonsági struktúra



GOV CERT MAGYARORSZÁG NBSZ

Operatív feladat végrehajtási szint

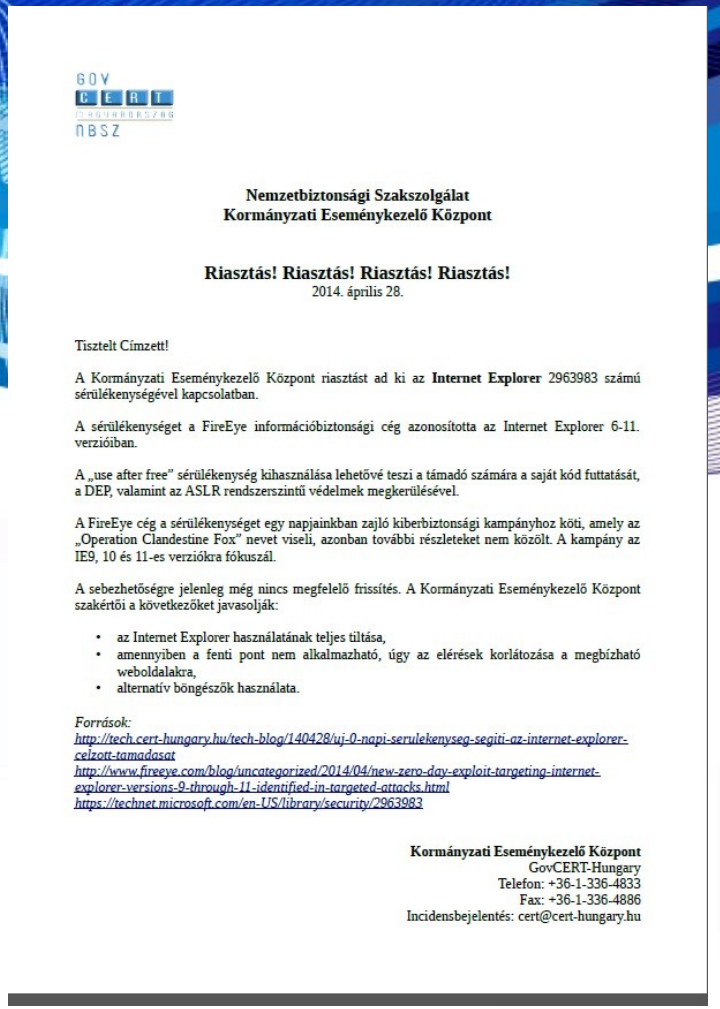


GOV CERT MAGYARORSZÁG
NBSZ

III. GovCERT feladat- és hatásköre

Főbb tevékenységeink csoportosítva:

- Kiberbiztonsági koordinációs tevékenység
- Nyilvántartások vezetése
- Kapcsolat az ágazati eseménykezelő központokkal
- Biztonsági események észlelése
- Incidensek kezelése
- Kapcsolatfelvétel és -tartás
- Megelőző tevékenység
- Tudatosítás



GOV CERT MAGYARORSZÁG NBSZ

Nemzetbiztonsági Szakszolgálat
Kormányzati Eseménykezelő Központ

Riasztás! Riasztás! Riasztás! Riasztás!
2014. április 28.

Tisztelt Címzett!

A Kormányzati Eseménykezelő Központ riasztást ad ki az **Internet Explorer** 2963983 számú sérülékenységével kapcsolatban.

A sérülékenységet a FireEye információbiztonsági cég azonosította az Internet Explorer 6-11. verzióiban.

A „use after free" sérülékenység kihasználása lehetővé teszi a támadó számára a saját kód futtatását, a DEP, valamint az ASLR rendszerszintű védelmek megkerülésével.

A FireEye cég a sérülékenységet egy napjainkban zajló kiberbiztonsági kampányhoz köti, amely az „Operation Clandestine Fox" nevet viseli, azonban további részleteket nem közölt. A kampány az IE9, 10 és 11-es verziókra fókuszál.

A sebezhetőségre jelenleg még nincs megfelelő frissítés. A Kormányzati Eseménykezelő Központ szakértői a következőket javasolják:

- az Internet Explorer használatának teljes tiltása,
- amennyiben a fenti pont nem alkalmazható, úgy az elérések korlátozása a megbízható weboldalakra,
- alternatív böngészők használata.

Források:
http://tech.cert-hungary.hu/tech-blog/140428/uj-0-napi-serulekenyseg-segiti-az-internet-explorer-celzott-tamadasat
http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html
https://technet.microsoft.com/en-US/library/security/2963983

Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@cert-hungary.hu

GOV CERT MAGYARORSZÁG NBSZ

III./1. A GovCERT feladat- és hatásköre

- Éves jelentést készít a lehetséges veszélyforrásokról és elhárításuk lehetőségeiről
- Több szervvel együttműködésben véd a globális kibertérből érkező támadások ellen
- Technikai védelmi, megelőző, koordinációs, szakmai támogató és tájékoztatási tevékenységet végez az állami- és önkormányzati szervek részére
- Felelős a meghatározott szervek, és az NTG biztonsági eseményeinek kezeléséért
- Nemzetközi szinten képviseli hazánkat a kibervédelemre szakosodott szervezetekben
- Fogadja és továbbítja a belföldi és nemzetközi szintről érkező riasztásokat
- Azok elhárításának koordinálásában központi szerepet tölt be
- Sérülékenységről / veszélyekről / intézkedésekről nyilvántartást vezet


GOV CERT MAGYARORSZÁG
Nemzetbiztonsági Szakszolgálat
Kormányzati Eseménykezelő Központ

Heti jelentés

2014. július 14. – 2014. július 21.

Fenyegetettségi szint

Közepes

- 1 -

GOV CERT MAGYARORSZÁG NBSZ

IV. Incidensek, fenyegetések

Bejelentett incidensek típusai

- Kéretlen levelek (spam)
- Robothálózat (botnet)
- Honlap rongálás (deface)
- Szolgáltatás megtagadás (Denial of Service)
- Adathalászat (phishing)
- Adatvesztés, szivárgás (data loss/leak)
- Célzott támadás (Advaced Persistent Threat)

GOV CERT MAGYARORSZÁG NBSZ

Fenyegetések / veszélyek

- Webes tartalmak böngészése
  - Illegális és sokszor egyben káros tartalmak megtekintése, letöltése
- Elektronikus levelezés
  - Feladó egyértelmű azonosítása
  - Téves címzés
- Azonnali üzenetküldő szolgáltatások
  - Káros URL-ek meglátogatása, fertőzött állományok megnyitása
- Közösségi oldalak használatának veszélyei
  - Adathalászat
  - Hamis megszemélyesítés
- Felhőalapú tárhelyek
  - Újabb, többes dokumentumpéldányok létrehozása
  - Az adattárolás pontos földrajzi helye ismeretlen

GOV CERT MAGYARORSZÁG NBSZ

V. Biztonságtudatos viselkedés
Szervezeti kockázatok

- Munkavállalók gyakori fluktuációja
- Gyakori szervezeti változások
- Elnyúló átszervezések
- Tisztázatlan felelősségi viszonyok
- Szabályozatlan információátadási rend
- Rendezetlen illetékességi kérdések
- Szabályozatlan munkakörök

GOV CERT MAGYARORSZÁG NBSZ

Humán kockázatok

- Szándékos károkozás
  - Anyagi ellenszolgáltatás (pl.: külső megbízatás)
  - Bosszúállás (pl.: elbocsátás esetén)
  - Szívesség viszonzása
  - Üzleti kapcsolat fenntartása
  - Jól értesültség sugárzása

- Akaratlan károkozás
  - „Fecsegés”
  - Gondatlanság, képzetlenség
  - (Információ)biztonsági tudatosság hiánya, alacsony szintje
  - Nem tényeken alapuló kockázatérzékelés
  - Alacsony felelősségérzet a virtuális térben

GOV CERT MAGYARORSZÁG NBSZ

Technológiai kockázatok

- Jogosult felhasználók számának növekedése
- Egyszerű(bb) hozzáférés az erőforrásokhoz
- Nagy tárolókapacitású mobil eszközök
- Költséghatékony vezeték nélküli technológiák elterjedése
- Magántulajdonú IKT eszközök növekvő száma (BYOD)

GOV CERT MAGYARORSZÁG NBSZ

VI. Képességek, jövőkép

Jelenlegi képességeink

- Információ csere/megosztás/publikálás
- Információbiztonsági képzések, tudatosító kampányok (együttműködés nemcsak a központi, hanem a megyei, helyi szervekkel, → a lehető legtöbb partnerhez eljutni)
- Kiberbiztonsági incidensek kezelésének koordinációja

Jövőbeli tervek

- Teljes körű, dinamikus, automatizált kártékony kód elemzés
- Automatizált naplóállomány elemzés
- Esemény korreláció
- Online kártékony kód adatbázis és tudásbázis
- Korai előrejelző rendszer

GOV CERT MAGYARORSZÁG NBSZ

VII. Nemzetközi kapcsolatok,tagságok

- Európai Hálózatbiztonsági Ügynökség (ENISA)
- EU-CERT
- CERT-ek globálisan
- ShadowServer Foundation
- Vírusvédelmi cégek
- Rendszeres részvétel a NATO/EU kibervédelmi és krízishelyzet-kezelési gyakorlatokon
- FIRST (Forum of Incident Response and Security Teams)
- TI (Trusted Introducer)
- IWWN (International Watch and Warning Network)

GOV CERT MAGYARORSZÁG NBSZ

IX./1. Esettanulmány:

CryptoLocker

- Típusa: ransomware (zsaroló)
- Működése:
  - A felhasználó számára elérhetetlenné teszi
  - a számítógépen található felhasználói állományokat
  - (pl.: Word, Adobe, Excel, képek)
  - 2048 bites egyedi RSA kulccsal titkosít
  - Ellentételezésért cserébe hozzáférést ígér a fájlokhoz
- Feltehetően a kártevő mögött álló csoport robothálózat gépeire telepítette először a kódot
- A kártevő csak a felhasználó számára fontos, saját fájljait titkosítja
- Rendszerfájlokat nem tesz elérhetetlenné, a rendszert működőképesen hagyja

GOV CERT MAGYARORSZÁG NBSZ

Védekezés

- Megelőzés elsődlegessége, ugyanis a fájlok maradéktalan helyreállítása nem lehetséges
- Biztonsági mentések sűrítése
- Patch-management
  - Folyamatosan frissített tűzfalak, vírusirtó szoftverek
  - Operációs rendszer, alkalmazások naprakészen tartása
- A felugró ablakokra történő kattintás átgondolása
- Ismeretlen címzettől érkező gyanús, ígérettel kecsegtető elektronikus levelek vírusellenőrzése

GOV CERT MAGYARORSZÁG NBSZ

IX./2. Esettanulmány:

Ke3chang

- Széles körű kiberkémkedési kampány, feltehetően kínai eredetű amely 2010. óta aktív. 2013. augusztusában fedezték fel a FireEye kutatói
- Ismertté vált 23 C&C (Command and Control) szerver, az áldozatok között azonosítottak 9 kormányzati szervet (minisztériumot) 5 különböző európai országból
- A kártékony kód terjedése: (e-levél csatolmányban, káros kódot tartalmazó honlapra
- mutató link)

GOV CERT MAGYARORSZÁG NBSZ

Terjedése

- Spear-phising elektronikus levél (e-mail)
- Java 0.-ik napi sérülékenységet használt ki (CVE-2012-4681)
- Microsoft Word sérülékenység (CVE-2010-2883)
- Adobe PDF Reader sérülékenység (CVE-2010-2883)
- Windows Screensaver (.scr)
- Futtatható állományok (.exe)
- Unicode Right-To-Left Override (RTLO) alkalmazása

GOV CERT MAGYARORSZÁG NBSZ

Intézkedés

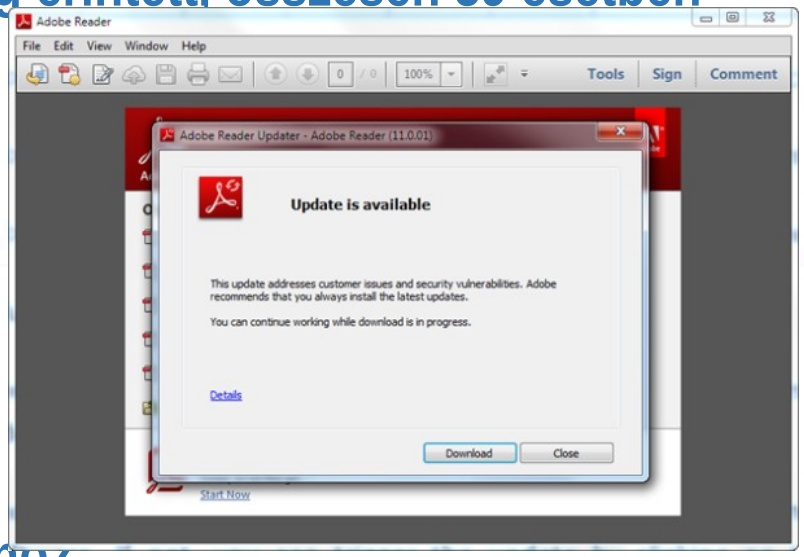
- Információk begyűjtése
- Tűzfalszabályok, IDS/IPS szabályok
- Logelemzés
- Tájékoztatás
- Fertőzött állomás beazonosítása
- Adathordozó vizsgálata
- Fertőzés elhárítása
- Utóelemzés, tájékoztatás

GOV CERT MAGYARORSZÁG NBSZ

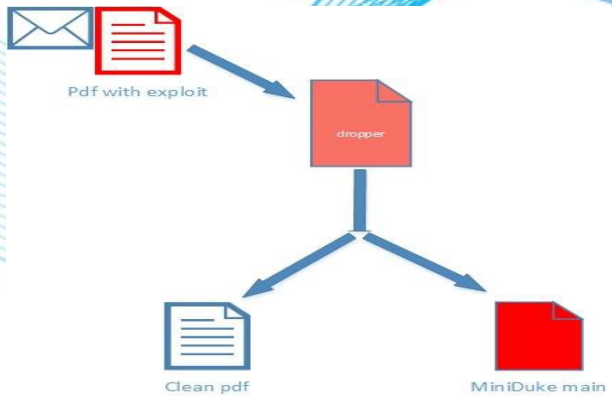
IX./3. Esettanulmány:

MiniDuke2

- A többek között kormányzati szerveket célzott Európában, 23 ország érintett, összesen 59 esetben
- A számítógép felett a számítógépes károkozó az Adobe Reader nulladik napi sebezhetőségét kihasználva veszik át az irányítást
- A Miniduke-ot célba juttató fájlt egy valódinak látszó PDF-dokumentumba csomagolják, amelynek a mérete mindösszesen 20 kB
- Központunk 2014.03.06-án kezdett egy MiniDuke gyanús bejelentés alapján vizsgálódni
- A log állományok elemzése alapján, Magyarországon több érintett
- A támadás sorozat elemei nagyon hasonlítanak a 2013-as kampányhoz
- A C&C szerverekkel való kommunikáció jellemzően: HTTP, Webdav, FTP-n keresztül történik
- Támadás típusok: Malware alapú, RTF hiba kihasználó spear-phising jellegű



GOV CERT MAGYARORSZÁG NBSZ



Miután a trójai bekerült a rendszerbe:

Program Files/Startup /.lnk A futtatható fájljai mellett egyes felhasználói könyvtárakba .tmp kiterjesztésű állományokat valamint egy update.cmd fájlt is elhelyez.

Google keresője felé küld hálózati kéréseket (*www.google.com – port TCP/80 - HTTP*)

csatlakozik különféle Twitter oldalakhoz (*twitter.com –port TCP/443 - SSL*)

felcsatlakozik a geoiptool oldalára, a megtámadott gép földrajzi helyét azonosítja (*www.geoiptool.com –port TCP/80 – HTTP)*

Majd letölt egy körülbelül 300 KB méretű állományt, amely első ránézésre egy kis ikont tartalmazó képállomány, a valóságban azonban egy futtatható kód elindítását szolgálja

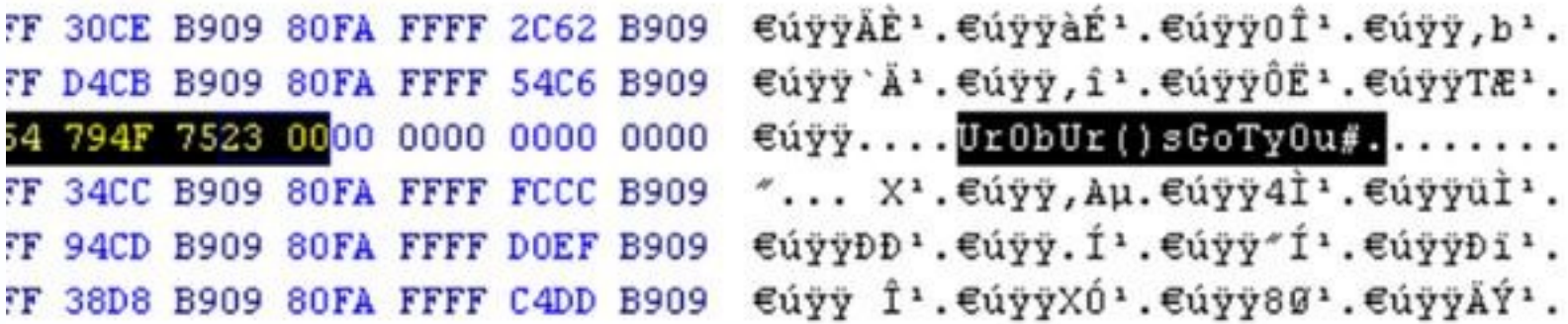
GOV CERT MAGYARORSZÁG NBSZ

X./4. Esettanulmány:

Uroburos URUBUROS/SNAKE/TURLA

A malware egy benne szereplő sztring (Ur0bUr()s) alapján kapta a nevét

- A malware 2011-ig vezethető vissza, valószínűleg több variánsa is létezik, amelyeket még nem fedeztek fel
- Több nyílt forrású rendszereken dolgozó kutató szerint, kapcsolat lehet az Uroburos és egy másik 2008-as malware, az Agent.btz között, amelyet valamikor amerikai kormányzati szervek ellen használtak



GOV CERT MAGYARORSZÁG NBSZ

X./4. Esettanulmány:
Uroburos URUBUROS/SNAKE/TURLA

- Támadás típusok: spear phishing/phishing, watering hole, közvetlen szervertámadás
- Kormányzati Eseménykezelő Központ a Symantec-től kapott információk alapján, 2014. februárjában megkezdte az ügy kivizsgálását
- Log-állományok elemzése
- Érintettek értesítése, incidens koordináció (detekciós segédlet, amelyet antivirus és IT biztonsági cégek
  fejlesztettek ki)

GOV CERT MAGYARORSZÁG NBSZ

Összefoglalás

GOV CERT MAGYARORSZÁG NBSZ

Automatizáció szükséges!

Köszönöm megtisztelő figyelmüket!

GOV CERT MAGYARORSZÁG

Nemzetbiztonsági Szakszolgálat
Kormányzati
Eseménykezelő Központ

Incidens bejelentés (0-24)

E-mail: cert@cert-hungary.hu

Tel: 00 36 (1) 336 4833
Fax: 00 36 (1) 336 4886