HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Rosszindulatú szoftverek (Malware)

VIHIBB01 – Kódolás és IT biztonság (2020)

Dr. Bencsáth Boldizsár (PhD, OSCP)

CrySyS Lab, BME
bencsath@crysys.hu

www.crysys.hu

MŰEGYETEM 1782

Tartalom

- A kártékony kód, a malware nem új jelenség, évtizedek óta okoz gondokat
- Mégsem oldottuk meg a kérdést, ma is aktuális
- Bemutatom a történetét
- Az APT támadások kihívásait
- Néhány esetet, amikor a malware konkrét jelenlétén túl gyűjtünk össze fontos információkat, hogy feltérképezzük a helyzetet

Bevezetés, definíciók

Malware

- malware = **mal**icious soft**ware kártékony szoftver**
  - a.k.a. malicious code or malcode
  - Mármilyen olyan programkód, ami hátráltatja a rendszer működését, ami bármi problémát okoz, káros, az malware
- Általában a korábban használt kategóriák elemei: vírusok, férgek, trójeiaik

Alapvető malware típusok

- virus
- Worm - féreg
- Trojan horse – trójai faló

- Egy idő után a kategorizáció teljesen bénává vált, nem lehetett egyetlen kategóriába beosztani a kártevők többségét, ezért nem járunk el ennek megfelelően.

A malware alapvető típusai

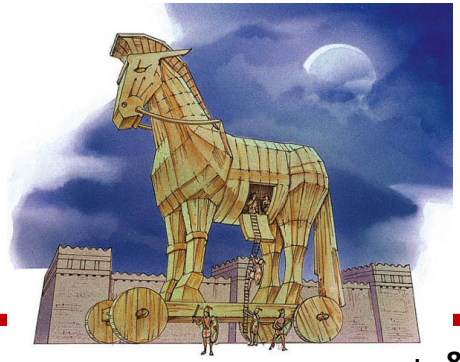
- virus
  - Ha lefuttatjuk, másolatait más számítógépes programokba, adat fájlokba, vagy a mrevelmez és floppy boot szektorába másolja át (vagy pl. USB)
    - » A kapcsolódó adathelyet (pl. program) fertőzőttnek nevezzük, mert a vírus kódja beleépül
  - Önmagában nem életképes, kell neki egy működőképes közek pl. egy progra,
    - » A vírus kódja akkor fut le amikor aktivizáljuk a hordozóját pl. a programot
    - » Valamilyen mechanizmussal replikálódik, pl. egyik programról a másikra
  - Azon túl, hogy terjed, kárt is okozhat
    - » e.g., információ lopás, rombolás, zsarolás, bármi egyéb

Alapvető malware típusok

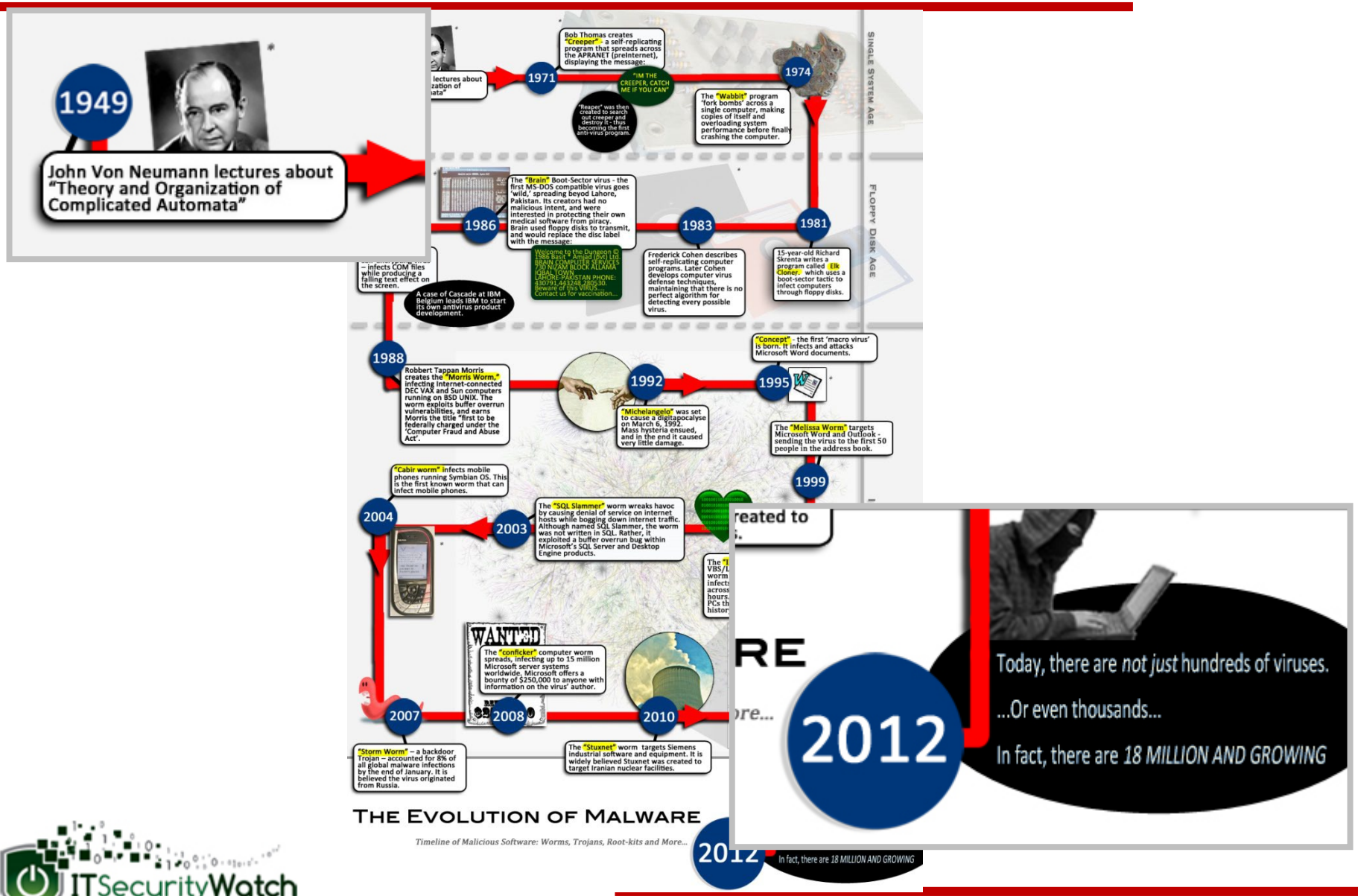
- virus
- Worm / féreg
  - Egy önmagában is életképes program ami terjed a hálózatokon
    - » A vírussal ellentétben nincs szüksége egy hordozóra, önmagában „élőképes”
  - Tipikusan azokat a kártevőket hívjuk így, amelyek valamilyen biztonsági sérülékenység kihasználásával tömegesen és gyorsan tud terjedni, nem kell felhasználói beavatkozás
  - A féreg is tud kárt okozni
    - » e.g., adat lopás, fájl törlés, üzenet megjelenítés, minden egyéb
    - » A terjedés nagy sávszélességet igényelhet
- Trojan horse / trójai

Malware típusok

- virus
- Worm / féreg
- Trojan horse / trójai
  - Olyan önálló program, ami úgy tesz, mintha hasznos lenne, de eközben nem kívánt, káros dolgot is végez
    - » Pl. információt lop, vagy hozzáférést enged: *backdoor/kiskapu* (Remote Access Trojan – RAT – távoli hozzáférést lehetővé tevő kód)
    - » Időzített is lehet, sokáig nem felismerhető majd hirtelen kárt okoz
    - » A mobil malware nagy része trojan horse, mert másnak teszi ki magát, mint ami

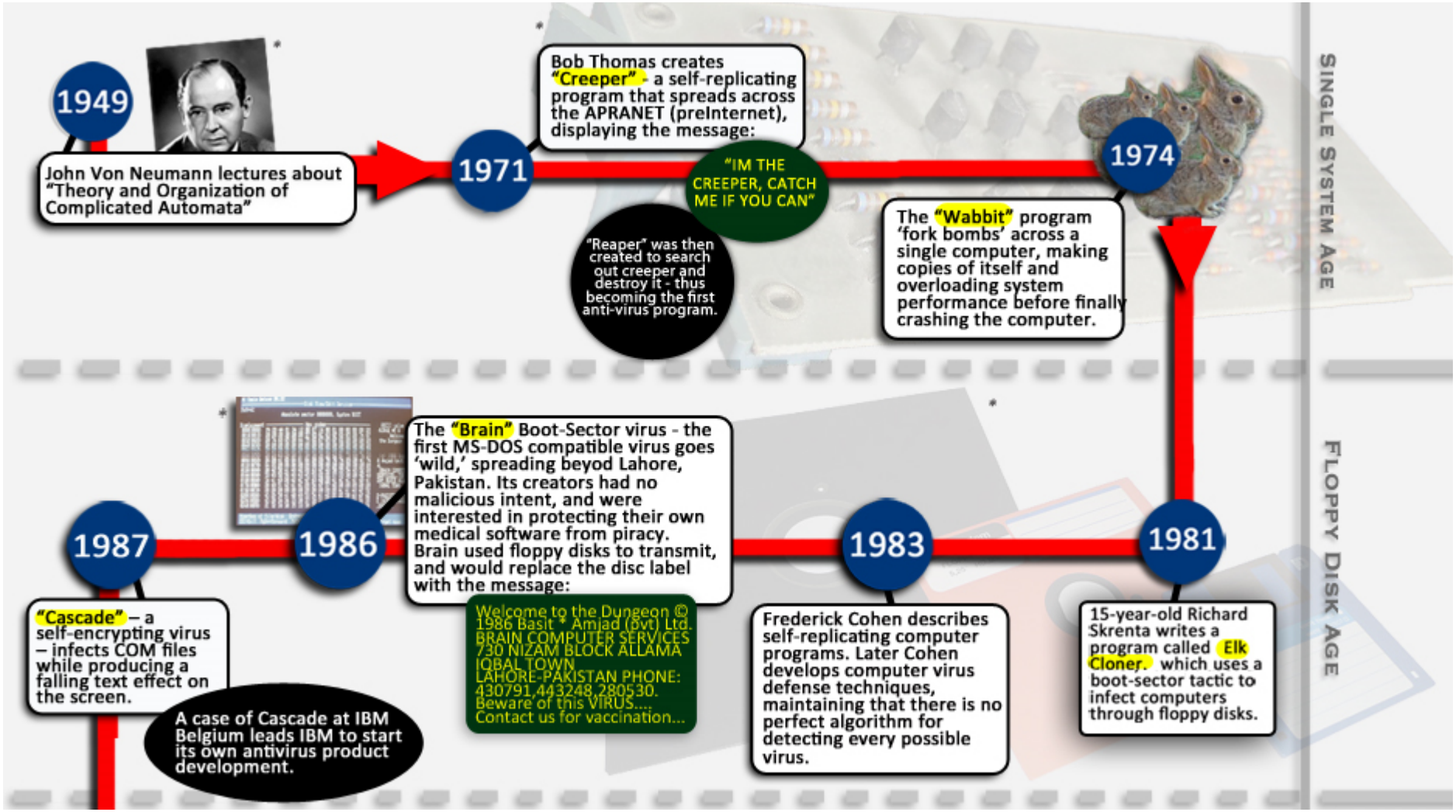


Történelmi áttekintés

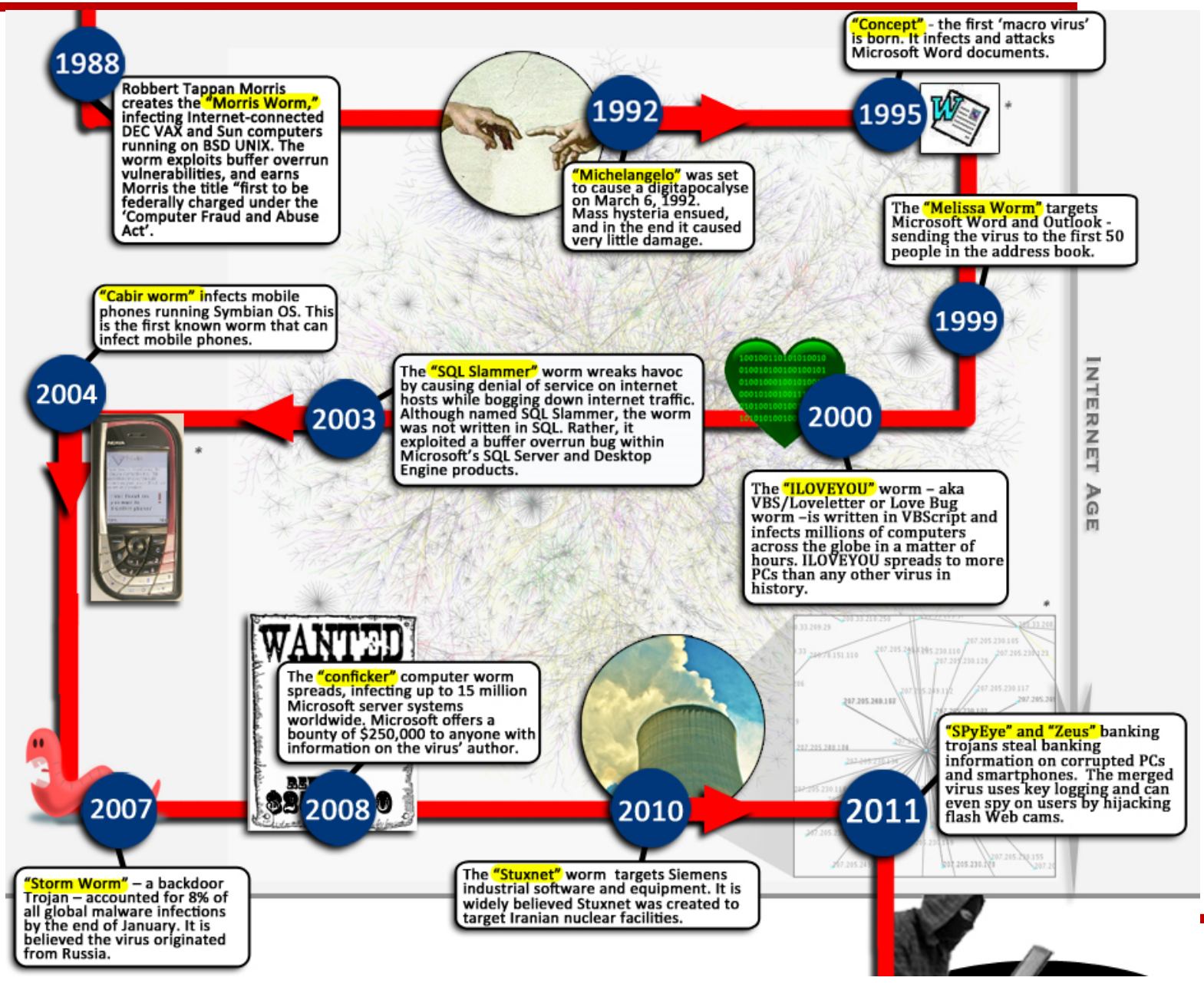


ITSecurityWatch
www.ITsecuritywatch.com

Történelmy áttekintés 1 - kezdetek

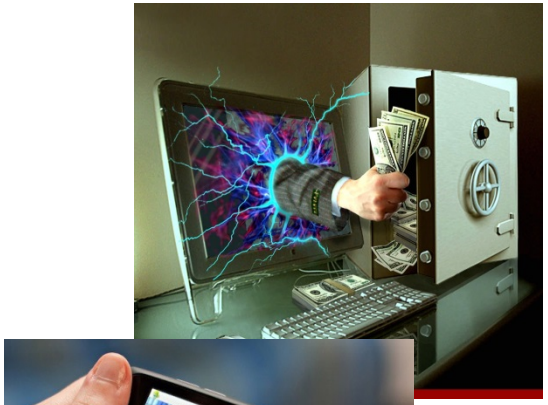


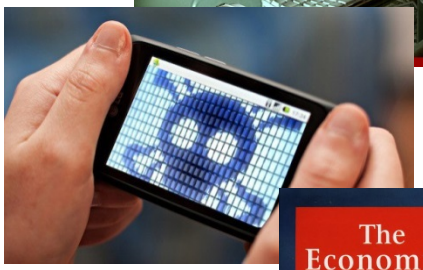
Történelmi áttekintés – internet kora



Mostanában…

- Tömeges malware előfordulás a cybercrime nagysága miatt
- Okos eszközök, IoT, ipari eszközök malware támadásai
- Malware támadások célzott, nemzetek közötti hadviselésben (APT, stb.) kiber-háború?





Potyogós virus - cascade

- 1987-ben friss vírus, hiradó is bemonta
- 1071 byte hosszú
- Egyike az első PC vírusoknak ami Magyarországon is tömeges fertőzést okozott
- Obfuszkációt használ, így a kód nagy része más-és-más minden példányban (nem kriptográfiai)
- Károkozás: Néha a betűk elkezdenek leesni a DOS képernyőn
- TSR code (nem volt multitasking, a háttérben tudott maradni és aktiválódni)
- http://www.youtube.com/watch?v=UWLg6tTeQRg
- Továbbá: http://kannan.jumbledthoughts.com/index.php/21-virus-and-other-malware-payload-videos/

Potyogós – in action

Célzott támadások

Célzott támadások

- Sokan várták, hogy a célzott támadások kora el fog jönni. De senki nem tudta hogyan és mikor
- A felfogás a Stuxnetnél (2010) indult meg, de valójában akkor már régen folyt (Hydraq, DoS attacks, etc.)
- Új esetek százait fedezték fel meg az elmúlt 10 évben és néha már nem is követhető
- APT: Advanced Persistent Threat -> Ezt a definíciót nem szeretjük a célzott támadásra (targeted attack) mert úgy tesz, mintha a támadó lenne nagyon okos, közben sokszor a védekező buta
- A célzott támadók kezelésére nem elégségesek a hagyományos módszerek, azóta sok új kezelési módszert javasoltak, de egyik sem olda meg mindent azonnal

CrySyS Lab – Mit csináltunk mi?

- 09/2011 felfedeztük, analizáltuk és elneveztük a Duqu malware-t ami az iparágban világszintű ismertséget okozottt
- 05/2012 részletes technikai analízis dokumentumoat adtuk közre a **Flame** támadásról (mi sKyWIper néven említettük) – világhír volt
- 02/2013 A Kaspersky Lab-bal közösen mutattuk be az addig nem felismert **MiniDuke** malware támadást
- 03/2013 A magyar NBF közös munkájával dolgoztunk a **TeamSpy** támadáson
- … Azóta is több célzott támadáson dolgoztunk, de az ügyek egyre bonyultabbak is lettek és picit átalakult a kezelési módszertan.
- És átalakultak az operációs rendszerek is
- És még mindig a primitív támadások uralják a terepet

Duqu kapcsán felmerült eredmények

- Felfedeztük, elneveztük és analizáltuk a Duqu malware-t
  - Írtunk egy 60 oldalas riportot, hogy bebizonyítsuk, ez a Stuxnet rokona
  - Megosztottuk az eredményeinket anti-virus gyártókkal és a Microsofttal
  - A riportunk anonimizált, rövidített változata került bele a Symantec közleménye mellékletébe. Azért volt rá szükség, hogy a megtámadott cég ne bukjon le

- **Az ún. dropper, malware telepítő felismerése és kezelése**
  - MS word doksi 0-day Windows kernel exploit tartalommal
  - Meg kellett osztani a dokumentumot, de céges információk voltak benne, különleges kezelést kellett végezni, személyes kommunikáció szerepe nagy volt

- Készítettünk egy open source ún **Duqu detector toolkit**
  - Nem szignatúra alapú detekciós eszközök amelyek felismerhetnek ismeretlen duqu verzióket
  - Nyomokat is felismerhetnek, ha már a duqu törlődött is
  - Speciális környezetekben is használható, mert a forráskódot kiadtuk, bárki ellnőrizheti. Különleges környezetekben nem futhat vírusírtó.

- Mediáció különféle résztvevők között, információ megosztás, stb. koordinációja
  - Nagyon bizalmon alapvó kommunikáció a felek között
  - Hogy és mit oszthatunk meg
  - Néha összeegyeztethetlen ellentétek vannak a felek céljai között
  - Sikerült a dropper mintát úgy megosztani, hogy ne sérüljenek az áldozat lehetőségei
  - Ez volt a legnagyobb munka, ami a legtöbb időt igényelte!

Flame

- 2012. Májusában egy új célzott támadáson dolgoztunk, közösen másokkal, úgy nezevztük: sKyWIper
- 27/05 – National CERT of IRAN (Maher) közleményt adott ki egy malware mintáról amit “Flamer” néven jelzett
- 28/05 – CrySyS kiadott egy tech reportot a Flame/sKyWIper támadásról; Kasperksy ugyanekkor kiadott egy hasonló cikket a “Flame” malware-ről.
- ~ 10000 áldozat, Middle East (Iran, Sudan), később kapcsolódó malware minták merültek fel: Gauss, SPE/MiniFlame.
- Egy vezérlőszerver, azaz C2 vagy CC szerver lefoglalása után klt cég is analizálva lett: C&C analysis made by Symantec and Kaspersky

Miniduke

- FireEye talált egy 0-day PDF exploit lehetőséget 12/02/2013
- PDF fájlokat lehetett azonosítani a Virus Total segítségével, de a tartalmon nem volt azonos.
- A dokumentumok elnevezése, támadások túli tartalma arra utalt, hogy magas rangú célpontok lehetnek a célzottak
- Sikerült információt kinyerni a támadó C2 szerverekről
- Kb. 60 cím szinte rögtön előkerült akiket megtámadhattak. Ezek jelentős része diplomáciai célpont volt.
- A különleges dolog, hogy az egész vizsgálat dokumentációval és információ-megosztással kevesebb, mint egy hét volt
- Ukrajna, Orosz ügyek….

Teamspy

- 2013 Márciusában az akkor magyar NBF megkért, hogy segítsük egy általuk már felfedezett célzott támadás kezelésében
- A fő kérdés az volt, hogy célzott támadás, vagy kiberbűnözők véletlen áldozata a diplomáciai célpont
- A mi szerepünk az volt, hogy analizáljuk és használjuk fel kapcsolatainkat
- Elemeztünk mintákat és információkat amit a parancsszerverek (CC, C&C, C2 = ugyanaz) szerverekről előkerülnek
- A támadás úgy 8 éves múltra nézett vissza
- A támadásban kihasználták a TeamViewer szoftvert is, de saját malware kommunikciós moduljuk is volt
- A fő céljuk: információ lopás
- Apróságok már korábban nyilvánosak voltak a támadásról, de mi tettük egységes keretbe

Mit végeztünk el a Duqu malware kapcsán?

- Egy ideig nem is lehetett tudni, de mi voltunk a Duqu megtalálója
- 2011 szeptemberében egy incidenskezelés kapján olyan futtatható fájlokat találtunk, amelyek adatlopásra alkalmasak, illeve a Duqu billetnyűzet-leütéseket rögzítő része
- Később sikerült tovább modulokat felfedezni a támadásból amelyeket megosztottunk először titokban egy nagyon zárt körben. Később nyilvánosan egy lecsökkentett, rövidített verzió jelent meg a részletekről a Symantec Duqu jelentése mellékeleteként 2011.10.18. napján
- A dropper, azaz a telepítő modul, vektor csak október végén került felfedezésre, általunk és a célpont cég segítségével. Egy 0-day hiba volt a windowsban, aminek a segítségével nagyon sok dokumentum formátummal bármilyen windows feltörhető volt. Ez egy nagyon súlyos hiba, titokban tartottuk, a Microsoft javította november elején
- Nagyon sok munka volt az információ megosztással. Több, mint a műszaki kutatással. Kinek mi árulható el, hol és hogy kell rejtjelezni.

Áttekintés a Duqu / Stuxnet tulajdonságokról

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	C-Media
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	Duqu ☺	✓
PLC functionality	✓	✗ (different goal) Stuxnet ☺
Infection through local shares	✓	Possible – Symantec
Exploits, 0-day	✓	Zero-day word, win32k.sys
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
Port 80/443, TLS based C&C	?	✓ similar
Special “magic” keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Careful error handling	✓	✓
Initial, dropper, deactivation timer	✓	✓
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

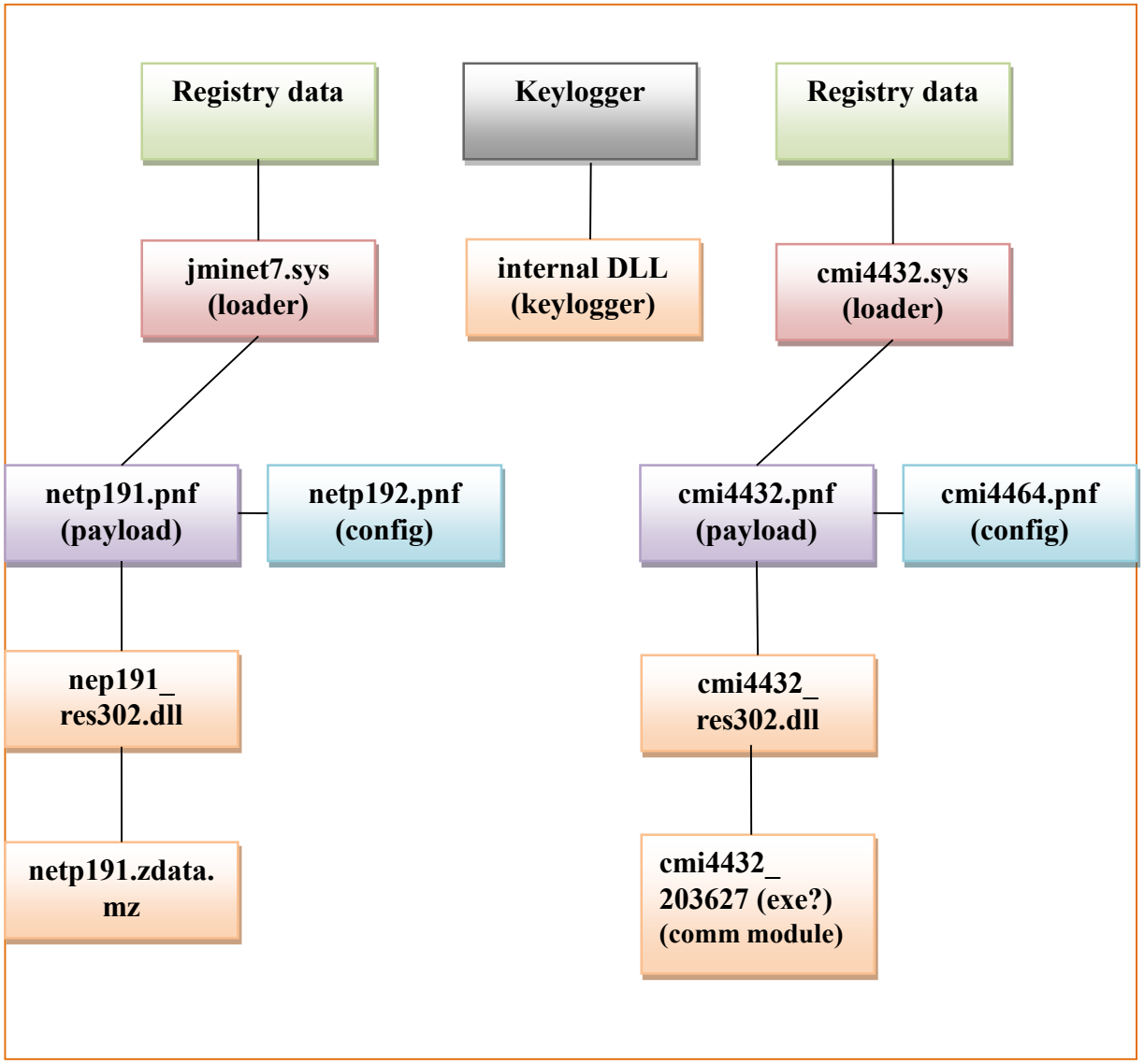
Egyéb funkcionalitás

- **Communication module**
  - Parancsok fogadása és információ küldése a vezérlőszerverre
    - » A mi esetünkben a C&C szerver 206.183.111.97 (India)
    - » Későbbi adatokból úgy tűnt minden áldozat külön vezérlőszerverekkel beszélt (tehát mindenki extra-fontos voltÖ
  - Kommunikáció: HTTP port 80 és HTTPS port 443
  - A kamu HTTP/80 kommunikáció egy képletöltés volt ahol a kép egy része rejtjelezett adat, nem valódi kép adat. Így nem tűnik fel bizonyos feldolgozó eszközöknek (2011)
  - **Keylogger module**
  - Rögzít billentyűleütéseket és korlátozottan képernyőfotókat
  - A %TEMP% directoryban tárolja tömörítve, saját formátumban, erről neveztük el
  - Maga a futtatható tartalmazott egy töredéket egy különleges képből, egy dupla galaxis rendszerről

Interacting Galaxy System NGC 6745

- Köze lehet a „stars” malware-hez ami 2011 áprilisában volt vagy nem is volt?

A duqu két változata modulárisan



Duqu decryptor

```
SUB_L00011320:
                        push    esi
                        mov     ecx,08471122h
                        xor     esi,esi
                        jmp     L00011330
                        Align   8
L00011330:
                        xor     [esi+L00015190],cl
                        ror     ecx,03h
                        mov     edx,ecx
                        imul    edx,ecx
                        mov     eax,1E2D6DA3h
                        mul     edx
                        mov     eax,ecx
                        imul    eax,04747293h
                        shr     edx,0Ch
                        lea     edx,[edx+eax+01h]
                        add     esi,00000001h
                        xor     ecx,edx
                        cmp     esi,000001ACh
                        jc      L00011330
                        mov     ax,[L00015198]
                        test    ax,ax
                        pop     esi
                        jnz     L00011382
                        movzx   ecx,[edi]
                        mov     edx,[edi+04h]
                        push    ecx
                        push    edx
                        push    L00015198
                        call    jmp_ntoskrnl.exe!memcpy
                        add     esp,0000000Ch
L00011382:
                retn
```

Stuxnet decryptor

```
SUB_L00011C42:
                        push    ebp
                        mov     ebp,esp
                        sub     esp,00000010h
                        mov     edx,eax
                        xor     edx,D4114896h
                        xor     eax,A36ECD00h
                        mov     [ebp-04h],esi
                        shr     dword ptr [ebp-04h],1
                        push    ebx
                        mov     [ebp-10h],edx
                        mov     [ebp-0Ch],eax
                        mov     dword ptr [ebp-08h],00000004h
                        push    edi
L00011C6A:
                        xor     edx,edx
                        test    esi,esi
                        jbe     L00011C87
                        mov     al,[ebp-0Ch]
                        imul    [ebp-08h]
                        mov     bl,al
L00011C78:
                        mov     al,[ebp-10h]
                        imul    dl
                        add     al,bl
                        xor     [edx+ecx],al
                        inc     edx
                        cmp     edx,esi
                        jc      L00011C78
```

Calling the decryption routine

Stuxnet's 1st decryption call

```
L000103E1:
        mov     byte ptr [L00014124],01h
        mov     dword ptr [ebp-1Ch],L00013E80
L000103EF:
        cmp     dword ptr [ebp-1Ch],L00013E84
        jnc     L00010409
        mov     eax,[ebp-1Ch]
        mov     eax,[eax]
        cmp     eax,ebx
        jz      L00010403
        call    eax
L00010403:
        add     dword ptr [ebp-1Ch],00000004h
        jmp     L000103EF
L00010409:
        xor     eax,eax
L0001040B:
        cmp     eax,ebx
        jnz     L000104BA
        mov     al,[L00013E98]
        test    al,al
        jz      L00010433
        xor     eax,eax
        mov     esi,00000278h
        mov     ecx,L00013E99
        call    SUB_L00011C42
        mov     [L00013E98],bl
L00010433:
        mov     eax,[L00013E99]
        test    al,01h
        jz      L0001044C
        mov eax,[ntoskrnl.exe!InitSafeBootMode]
        cmp     [eax],ebx
        jz      L0001044C
```

Duqu's 1st decryption call

```
L000105C4:
        mov     byte ptr [L00015358],01h
        mov     esi,L00015180
L000105D0:
        mov     [ebp-1Ch],esi
        cmp     esi,L00015184
        jnc     L000105E8
        mov     eax,[esi]
        test    eax,eax
        jz      L000105E3
        call    eax
L000105E3:
        add     esi,00000004h
        jmp     L000105D0
L000105E8:
        xor     eax,eax
L000105EA:
        test    eax,eax
        jnz     L00010667
        mov     edi,[ebp+0Ch]
        call    SUB_L00011320

        mov     eax,[L00015190]
        test    al,01h
        jz      L00010611
        mov     ecx,[ntoskrnl.exe!InitSafeBootMode]
```

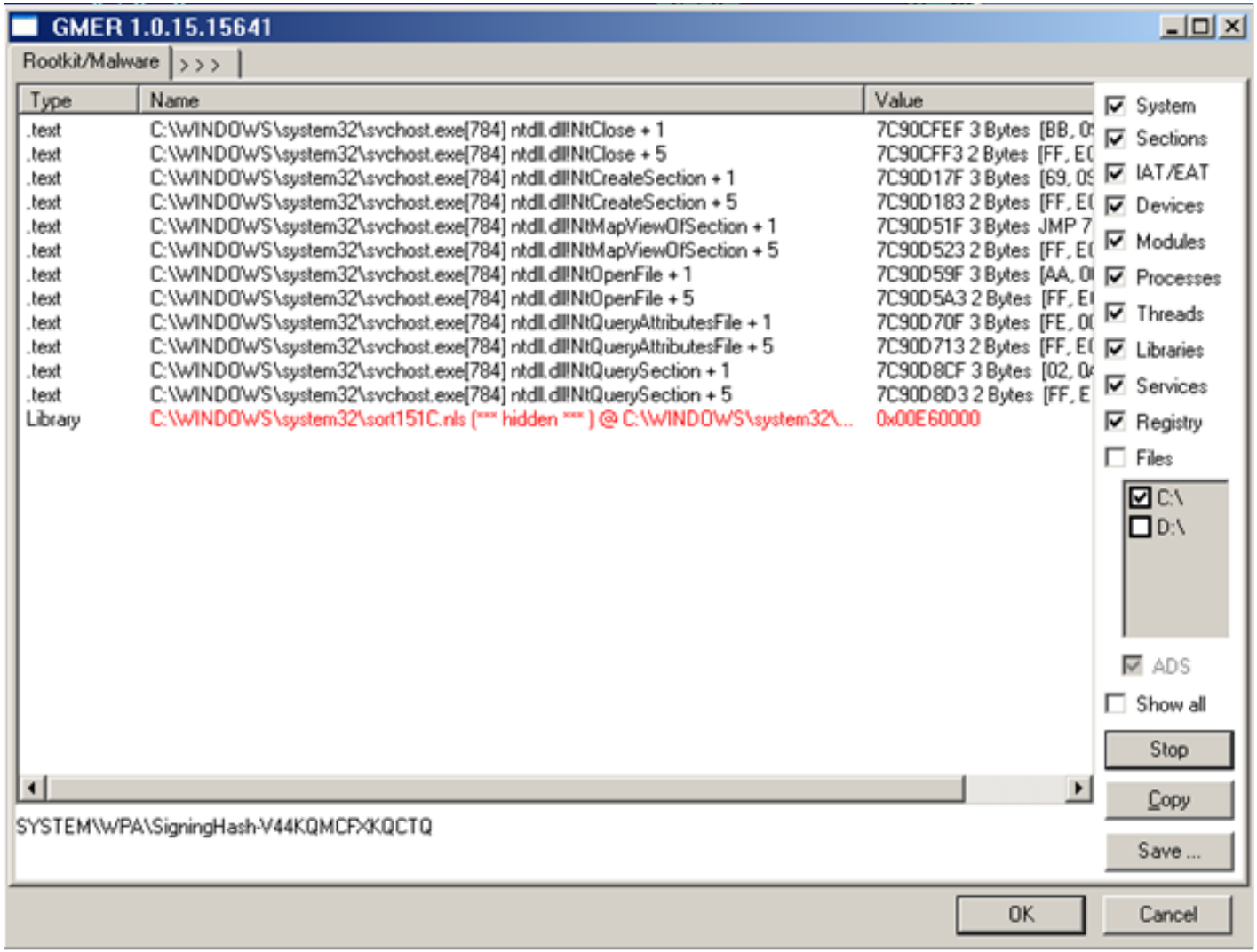
Stuxnet vs. duqu

Feature	oem7a.pnf (Stuxnet)	netp191.pnf (Duqu)
Packer	UPX	UPX
Size	1233920 bytes	384512 bytes
Exported functions #	21	8
ntdll.dll hooks	ZwMapViewOfSection ZwCreateSection ZwOpenFile ZwClose ZwQueryAttributesFile ZwQuerySection	ZwMapViewOfSection ZwCreateSection ZwOpenFile ZwClose ZwQueryAttributesFile ZwQuerySection
Resources	13 (201, 202, 203,205, 208, 209, 210, 220, 221,222, 240,241,242, 250)	1 (302)

PE headers-file dátumok

File	Date
CMI4432.PNF	17/07/2011 06:12:41
cmi4432_res302.dll	21/12/2010 08:41:03
cmi4432_203627.dll	21/12/2010 08:41:29
netp191.PNF	04/11/2010 16:48:28
nep191_res302.dll	21/12/2010 08:41:03
Keylogger.exe	01/06/2011 02:25:18
Keylogger internal DLL	01/06/2011 02:25:16

GMER


GMER 1.0.15.15641
Rootkit/Malware
>>>
Type
Name
Value
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtClose + 1 7C90CFEF 3 Bytes [BB, 0
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtClose + 5 7C90CFF3 2 Bytes [FF, E
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtCreateSection + 1 7C90D17F 3 Bytes [69, 0
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtCreateSection + 5 7C90D183 2 Bytes [FF, E
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtMapViewOfSection + 1 7C90D51F 3 Bytes JMP 7
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtMapViewOfSection + 5 7C90D523 2 Bytes [FF, E
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtOpenFile + 1 7C90D59F 3 Bytes [AA, 0
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtOpenFile + 5 7C90D5A3 2 Bytes [FF, E
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtQueryAttributesFile + 1 7C90D70F 3 Bytes [FE, 0
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtQueryAttributesFile + 5 7C90D713 2 Bytes [FF, E
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtQuerySection + 1 7C90D8CF 3 Bytes [02, 0
.text C:\WINDOWS\system32\svchost.exe[784] ntdll.dll!NtQuerySection + 5 7C90D8D3 2 Bytes [FF, E
Library C:\WINDOWS\system32\sort151C.nls (*** hidden ***) @ C:\WINDOWS\system32\... 0x00E60000
System
Sections
IAT/EAT
Devices
Modules
Processes
Threads
Libraries
Services
Registry
Files
C:\
D:\
ADS
Show all
Stop
Copy
Save ...
SYSTEM\WPA\SigningHash-V44KQMCFXKQCTQ
OK
Cancel

Duqu registry key data

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\JmiNET3]
"Description"="JmiNET3"
"DisplayName"="JmiNET3"
"ErrorControl"=dword:00000000
"Group"="Network"
"ImagePath"="\\??\\C:\\WINDOWS\\system32\\Drivers\\jminet7.sys"
"Start"=dword:00000001
"Type"=dword:00000001
"FILTER"=hex:a0,35,58,da,32,ee,d5,01,c0,15,8b,1f,4b,5c,d1,a1,0b,8b,e7,85,1c,7f,\
  6e,f2,ef,31,6a,18,3c,80,78,c7,d4,c5,50,90,7a,78,66,9d,6b,93,00,a1,f5,3d,26,\
  ce,cb,1c,1e,45,b0,ff,a0,dd,c0,a3,e8,58,31,0c,b2,a1,dd,11,37,ba,aa,1e,66,d3,\
  1f,b4,2f,e1,7c,eb,b6,a2,58,a0,25,62,77,b5,41,d3,71,02,1a,be,cb,bb,52,43,76,\
  43,b6,d0,67,25,19,10,27,67,a5,15,38,9f,8f
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\JmiNET3\Enum]
"0"="Root\\LEGACY_JMINET3\\0000"
"Count"=dword:00000001
"NextInstance"=dword:00000001
```

Kulcsok a két támadásban

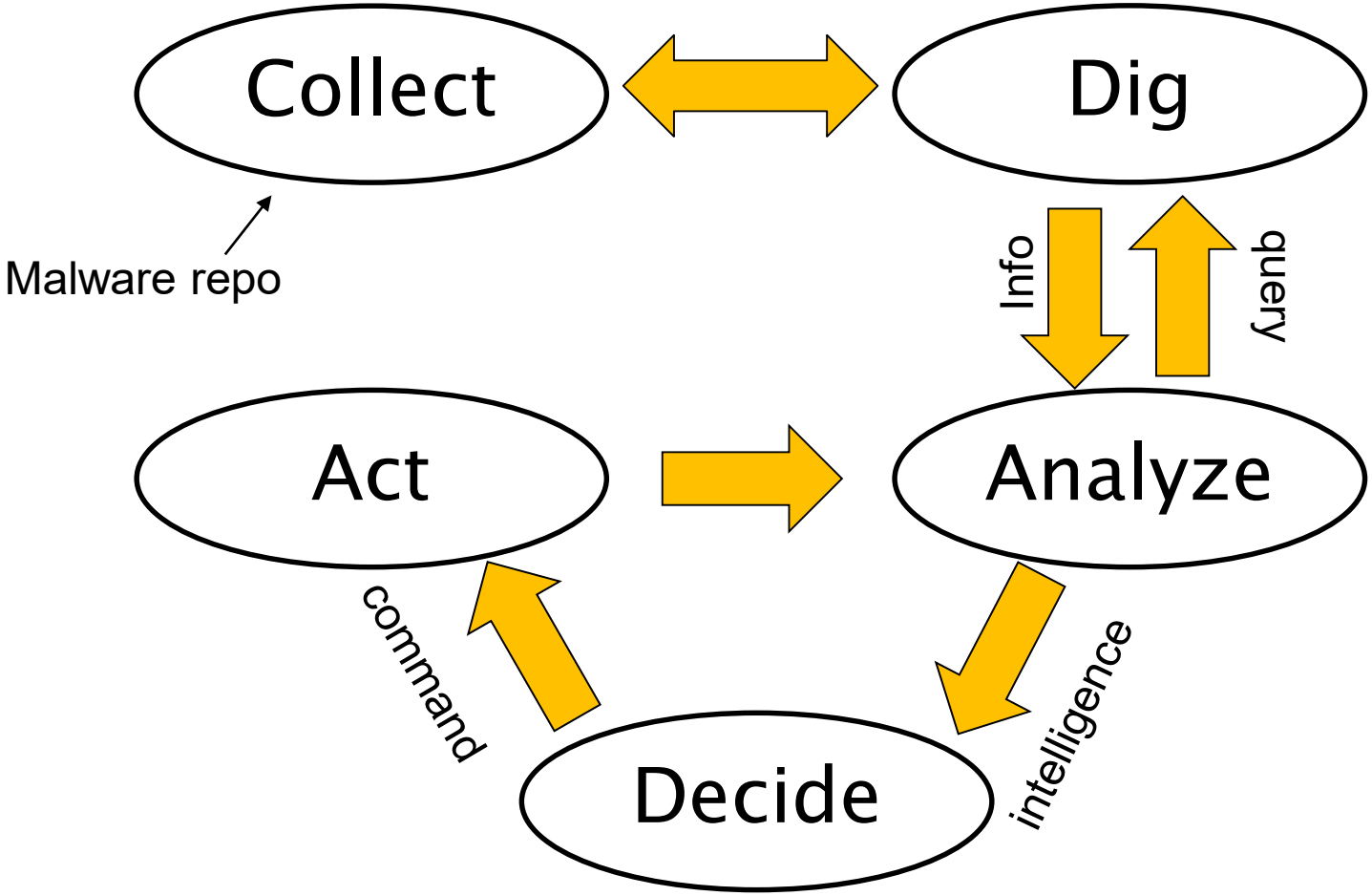
Description	Duqu Key
Compiled-in configuration (Config-1)	No key set, fixed decryption routine (essentially the same as key=0)
Variable configuration in registry (Config-2)	0xAE240682 (loaded from Config-1)
Decryption key for netp191.pnf	0xAE240682 (loaded from Config-2)

Description	Stuxnet Key
Compiled-in configuration (Config-1)	key=0
Variable configuration in registry (Config-2)	0xAE240682 (loaded from Config-1)
Decryption key for oem7a.pnf	0x01AE0000 (loaded from Config-2)

Description	Key
Compiled-in configuration (Config-1)	key=0
Variable configuration in registry (Config-2)	0xAE240682 (loaded from Config-1)
Decryption key for oem7a.pnf	0x01AE0000 (loaded from Config-2)

Threat intelligence, nyomozások, gyűjtögetések

Threat intelligence process - a model

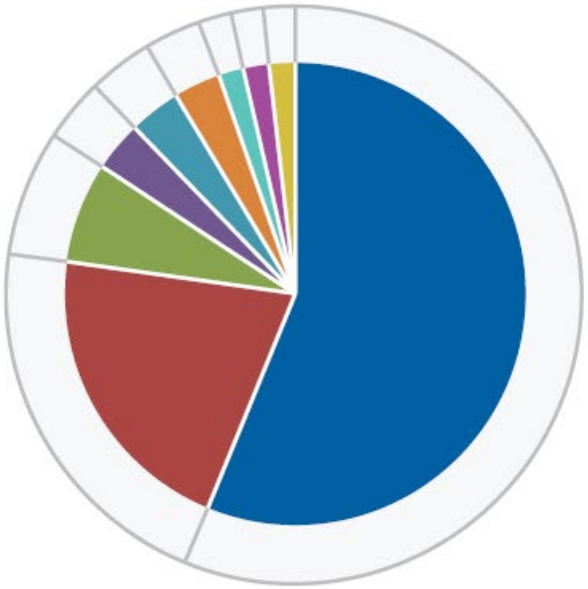


Snake/Uroburos – BAE – Hungarian victim

Nem biztosan áldozat!

SNAKE SAMPLES

In total we have collected over 100 unique files related to this espionage toolkit. Many of these were submitted to online malware analysis websites by victims and investigators over several years. In many cases the source country information of the submission is available. These allow us to visualise the distribution of countries where this malware has been seen:



#Samples	Submission Year					
Source country	2010	2011	2012	2013	2014	Total
Ukraine	1	3	6	8	14	32
Lithuania				9	2	11
Great Britain				4		4
Belgium				2		2
Georgia					2	2
United States		1	1			2
Romania				1		1
Hungary					1	1
Italy					1	1
Total	1	4	7	24	20	56

1 HU upload

VT uploads

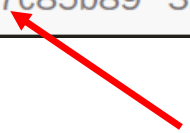
- Sample: 2eb233a759642abaae2e3b29b7c85b89
- Submissions:

2014-03-11 08:12:18	3	add5c61e (web)	CN
2014-03-10 12:26:32	vti-rescan	c98a3f59 (community)	FR
2014-03-09 18:39:34	vti-rescan	7d422d74 (community)	US
2014-03-09 10:20:30	vti-rescan	fe3ba116 (community)	IN
2014-02-10 15:32:10	wileman.dll	883db971 (web)	UA
2014-02-10 12:45:16	wileman.dll	a1bf5bda (community)	UA
2014-02-10 12:42:36	wileman.dll	c2c2a9a8 (web)	UA
2014-01-29 07:40:12	**blbtes.dll**	**11ea2c5b (web)**	**HU**

- Csak egy hash ismert Magyrarországról és az ehhez a mintához tartozik
- Természetesen az sem biztos, hogy ez magyar, csak az ip cím itt lehetett

What is 2eb233a759642abaae2e3b29b7c85b89 ?

MD5 Hash	File Type	FileSize	Compile Time	Notes
Kernel-centric architecture				
f4f192004df1a4723cb9a8b4a9eb2fbf	32-bit driver	206 KB	2011-06-24 07:49:41	fdisk.sys, Ultra3.sys
626576e5f0f85d77c460a322a92bb267	32-bit dropper	1,669 KB	2013-02-04 13:19:21	fdisk_mon.exe
90478f6ed92664e0a6e6a25ecfa8e395	64-bit driver	584 KB	2013-02-04 13:17:56	fdisk.sys, Ultra3.sys
1c6c857fa17ef0aa3373ff16084f2f1c	32-bit driver	219 KB	2013-02-04 13:20:00	fdisk.sys, Ultra3.sys
Usermode-centric architecture				
973fce2d142e1323156ff1ad3735e50d	32-bit driver	673 KB	2013-08-29 07:34:54	msw32.sys, cmbawt.sys
2eb233a759642abaae2e3b29b7c85b89	32-bit DLL	416 KB	2013-07-25 05:58:47	dropped DLL



Mi is itt a C&C server?

- A magyarországról feltöltött malware három CC szevert is tartalmaott, de ebből kettő még élt:
- winter.site11.com - offline
- swim.onlinewebshop.net - online
- july.mypressonline.com - online

(forrás: a minta)

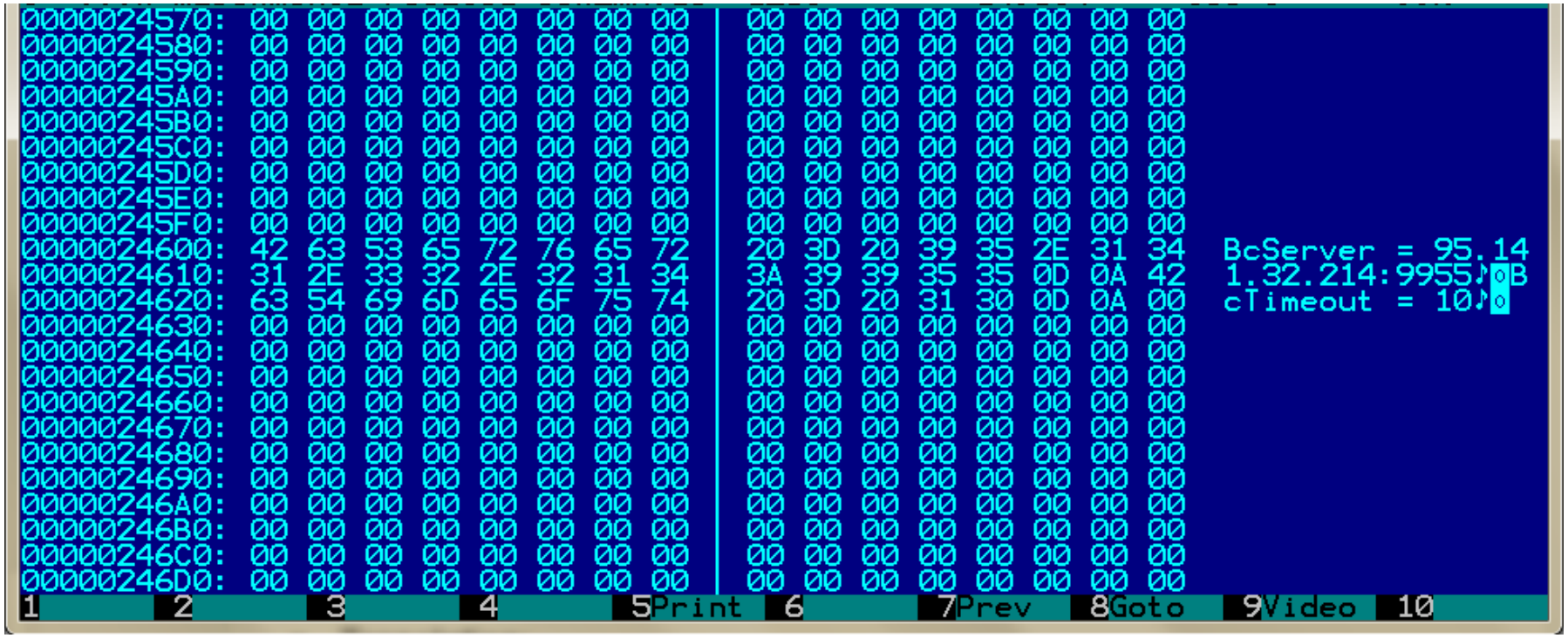
- Ami még akkor működött, lehet hogy információt tartalmazott az áladozatról és a támadóóról
- Természetesen az egy kérdés, hogy lehet ilyen információkhoz hozzájutni (bűnügyi eljárás, elkérjük a szolgáltatótól, valaki feltöri a szervert)
- Senki nem tudja hogy kellene csinálni profi módon
- Magát a támadót szinte biztos, hogy nem kapjuk el így

Malware repository – miért gyűjtögetünk?

- APT támadások esetében egyes malware minták lehet, hogy csak a konfigurációban különböznek
  - E.g. CC (vezérlőszerver) beállítások
- Minden minta különbözik
- De a minták nagyon hasonlóak lehetnek
- Egy adott malware család tagjai közeli hasonlóságot mutathatnak egymással. Átlapoló függvények, vagy akár a teljes kód is hasonló
- Ha megtalálunk kapcsolódó malware mintákkal azzal plusz információhoz juthatunk
- Persze rögtön nem lehet biztosra mondani a rokonságot

RCApp VNCDLL C&C server

- RCApp kapcsolata volt Zeus kampánnyal – innen indultunk
- Delphi program, előre írt rutinkönyvtárokkal
- C&C szerrver bele van hard-kódolva, itt láthathó
- Ha kapcsolódó mintákat találunk, úgy más C&C szervereket is találhatunk
- C&C szerverek valamiért információt szivárogtattak minden áldozatról



Találtunk más RcAPP mintát is

; Файл инициализации для VNCDLL. Прикрепляется к DLL посредством утилиты FJ.

; При загрузке DLL ищется этот файл, и если он найдет, ативируется сервер с заданными в файле параметрами.

; Адрес бэкконект сервера

BcServer = 46.21.159.253:443

; Время, через которое повторять подключение если бэкконект недоступен (секунд)

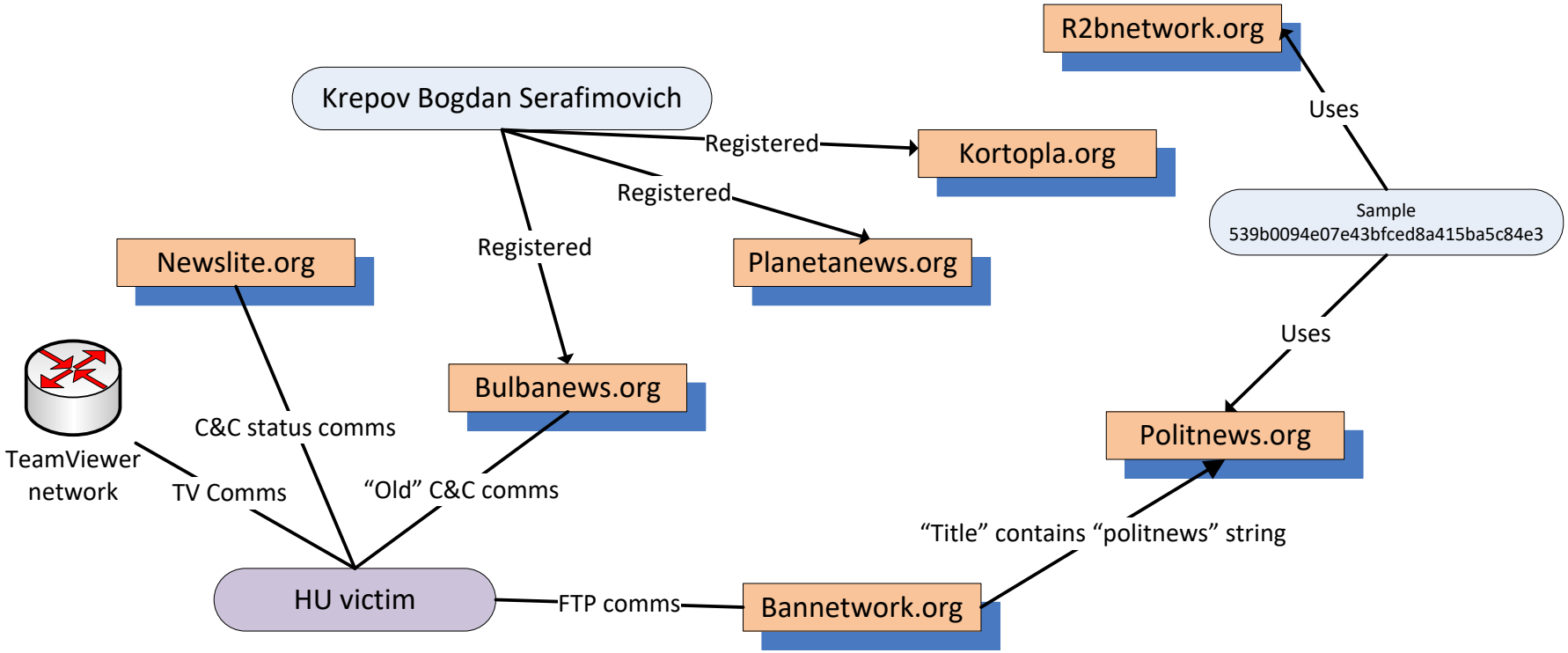
BcTimeout =

- Translation (Google):

; The initialization file for VNCDLL. Attached to the DLL using a utility FJ.
, When you download this DLL file is searched, and if he finds ativiruetsya server with the specified parameters in the file.

A kapcsolódó minta eredetijében

APT feltérképezése a domain kapcsolatok által



Köszönöm a figyelmet!

- Vége