STUXNET
ÉS AMI MÖGÖTTE VAN

Prof. dr. Kovács László mk. alezredes
ZMNE egyetemi tanár
kovacs.laszlo@zmne.hu

Dr. Sipos Marianna
ZMNE főiskolai tanár
sipos.marianna@zmne.hu

Tartalom

- **A Stuxnet**
- **és ami mögötte van …**

"We've never seen that before."

"***Using four zero-days, that's really, really crazy***," said Symantec's O Murchu.

Neither has Kaspersky, said Schouwenberg.

Ezen kívül használta még a **notorious Conficker** férget, mely 2008-2009 fordulóján gépek millióit fertőzte meg. 2008-ban Microsoft **MS08-067** frissítésében javította.

Kihasznált egy ismeretlen sérülékenységet a Siemens felügyelő szoftverben is.

4 zero-day Windows bug!

- Egy rosszindulatú program jellemzően egy zero-day bug-ot tartalmaz.
- Zero-day bug: javítatlan (unpatched) biztonsági rés.

1. Windows shortcuts bug (link files)
   Felfedezte: VirusBlokAda (Fehérorosz cég)
   jún. közepén, Microsoft javította aug. 2.
2. Print spooler bug (nyomtató puffer)
3. EoP (elevation of privilege) bug
4. Second EoP bug (magasabb hozzáférés)

   A másik hármat felfedezte: Kaspersky lab, Symantec és a Microsoft párhuzamosan.

Digitális aláírás

- Legalább 2 lopott digitális aláírással is rendelkezett, így legitimnek tűnt.
- USB-ről települ, AutoRun használata nélkül, hálózaton fertőz és elrejti a fájljait.
- Ipari vezérlő rendszerek automatikus folyamatait programozta újra. (PLC szoftverek) Ezeket is elrejti.
- A Siemens SIMATIC WinCC/Step7 által felügyelt ipari folyamatokat írt át, default felhasználók és jelszavak felhasználásával. (Amelyik gépen ilyen nem volt, ott nem csinált semmit, csak terjedt.)
- Peer-to-peer frissülés: két stuxnet találkozásakor a frissebb él tovább. 2012 jún. 24-én felszámolja magát.

A cél a működés szabotázsa volt, és hogy ne fedezzék fel, és ez fél-egy évig sikerült is, közben továbbfejlesztették.

Hogyan települt?

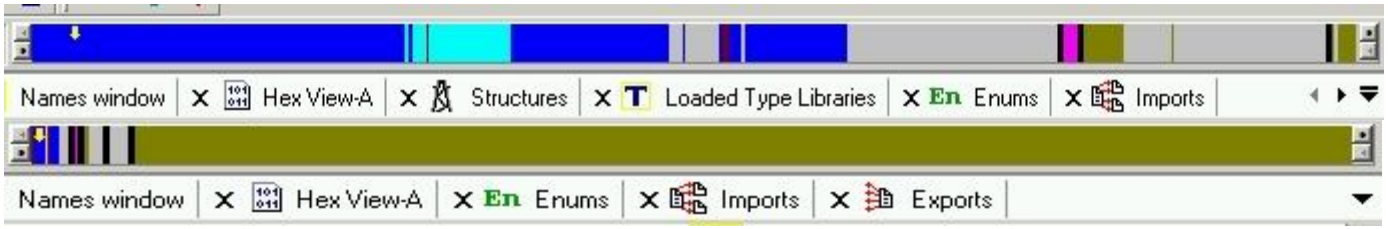
A fertőzött USB meghajtókon a következő fájlok találhatók:

- Copy of Shortcut to.lnk
- Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Copy of Shortcut to.lnk

- ~WTR4141.tmp (~25Kb DLL)
- ~WTR4132.tmp (~500Kb DLL)

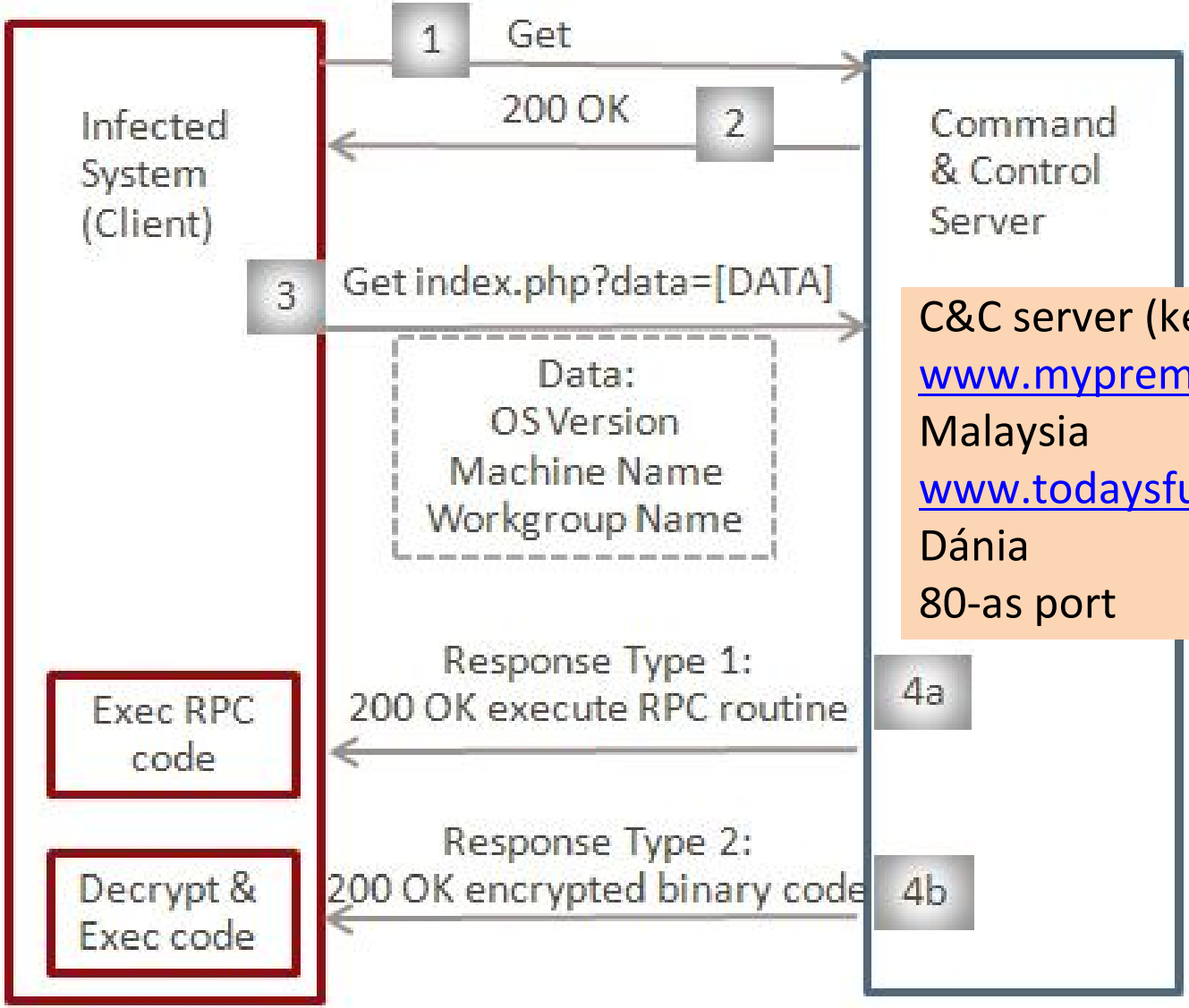
Az USB csatlakoztatásakor ha olyan alkalmazás olvassa, mely ikonokat tud megjeleníteni (Windows Explorer), az .lnk fájlok feltöltik az első .dll-t a memóriába és átadják neki a vezérlést.

Az első .dll elrejti az USB-n levő fájlokat, majd feltölti és elindítja a 2. dll-t, mely adatként tartalmaz egy kódolt .dll-t.



~ WTR4141.tmp

~ WTR4132.tmp



C&C server (kezdetben) URL:
www.mypremierfutbol.com
Malaysia
www.todaysfutbol.com
Dánia
80-as port

1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code

További információk

- http://www.biztonsagpolitika.hu **STUXNET: a virtuális háború hajnala**
- Gregg Keizer: Is Stuxnet the 'best' malware ever?
- http://www.symantec.com/connect/blogs/w32stuxnet-installation-details
- http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

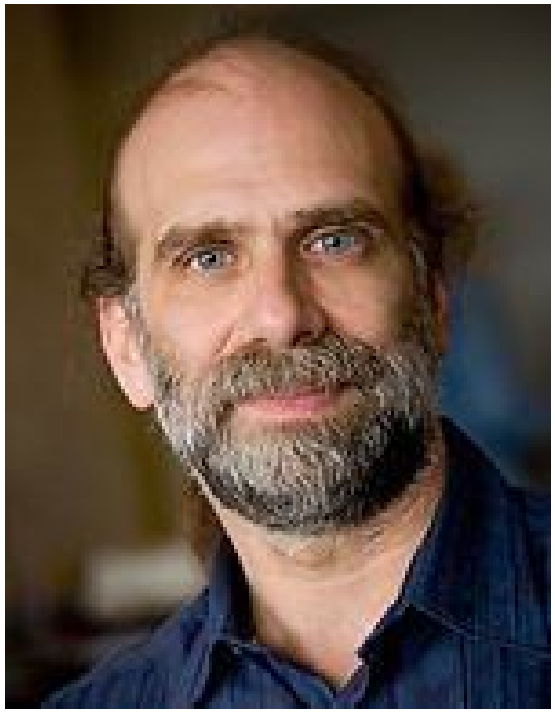
Miért is probléma?

- **50.000 fertőzött gép (SIMATIC WinCC, Siemens S7-400 PLC)**
- **Minimum 14 erőmű, közülük több Németországban (by Siemens)**
- **Az indiai Insat-4B műhold részleges leállása (elektromos ellátási problémák – napelemek becsukása)**
- **További (nagyon) fertőzött országok: India, Indonézia, Pakisztán**

Miért is probléma?

- Nem bankkártya számokat lop
- Nem belépési neveket és jelszavakat lop
- Nem botnetet szervez
- Ipari adatokat lop
- Ipari folyamatokat állít le
- **SABOTAGE!**
- **FŐPRÓBA?**

Schneier's opinion:



„My guess is that Stuxnet's authors, and its target, will forever remain a mystery."

További eszközök

- **denial of service, distributed denial of service,**
- **flooding (TCP SYN packet),**
- **man-in-the-middle attack,**
- **SMTP backdoor command attack,**
- **IP address Spoofing attack,**
- **IP fragmentation attack,**
- **TCP Session High jacking,**
- **Information leakage attack,**
- **JavaScript,- applet attack,**
- **cross site scripting (XSS)**
- **etc ...**

TÖRTÉNELEM

- **1997: LTTE (Tamil Eelam Felszabadító Tigrisei)**
- **1997: Euskal Herria (Baszk Újság)**
- **2000: Aum Shinryko**
- **2002: DoS DNS root ellen**
- **2003: Titan Rain**
- **2007: Orosz-észt konfliktus**
- **2008: Orosz-grúz konfliktus**
- **2009: Stuxnet**

VÉDELEM?

- **Csak informatikai kérdés?**
- **Komplex információbiztonság:**
  - Fizikai biztonság
  - Dokumentum biztonság
  - Személyi biztonság
  - Elektronikus információbiztonság

National Security Strategy: Priority Risks

Tier One: The National Security Council considered the following groups of risks to be those of highest priority for UK national security looking ahead, taking account of both likelihood and impact.

- International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland.
- Hostile attacks upon UK cyber space by other states and large scale cyber crime.
- A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.
- An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.

Tier Two: The National Security Council considered the following groups of risks to be the next highest priority looking ahead, taking account of both likelihood and impact. (For example, a CBRN attack on the UK by a state was judged to be low likelihood, but high impact.)

VÉDELEM? NATO

- **2007: Cooperative Cyber Defence Centre of Excellence (CCDCOE) - Tallinn,**
- **2010: NATO Cyber Defence Management Authority (CDMA) – Iklódy Gábor**

VÉDELEM? MAGYARORSZÁG

- **Jogszabályok:**
  - **2080/2008. (VI. 30.) Korm. Határozat**
  - **1249/2010. (XI. 19.) Korm. Határozata**
- **Szervezet:**
  - **Nemzeti Hálózatbiztonsági Központ**
  - **Információbiztonsági Felügyelet?**

KONKLÚZIÓ (?)

- **Kinek a feladata a védelem?**
- **A Stuxnet csak a kezdet?**
- **Mit tehet az EU?**
- **Hazánk elkésett?**
- **Kell-e terrorizmussal számolni?**
- **Mit tehet a NATO?**
- **Mit tehet az egyszerű user?**

KÖSZÖNJÜK A FIGYELMET!

ROBOTHADVISELÉS 10 TUDOMÁNYOS KONFERENCIA 2010. November 24.

Dr. Sipos Marianna

főiskolai tanár

sipos.marianna@zmne.hu

Prof. dr. Kovács László mk. alezredes

egyetemi tanár

kovacs.laszlo@zmne.hu

Az előadás és a publikáció a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

This paper and presentation was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences