Stuxnet

Aleksandar Kostadinović

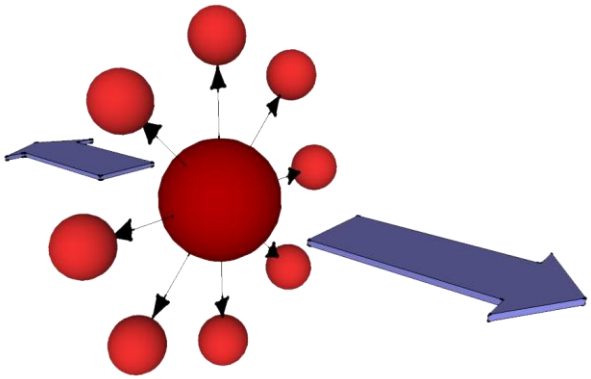
april 2015. Beograd

Maliciozni programi

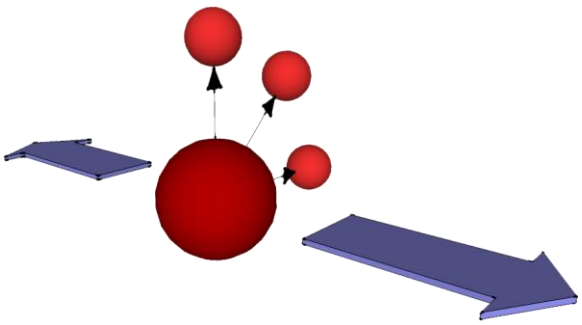
- Virusi
- Worms (crvi)
- Trojanski konji
- Rootkits
- Hoax

Maliciozni programi

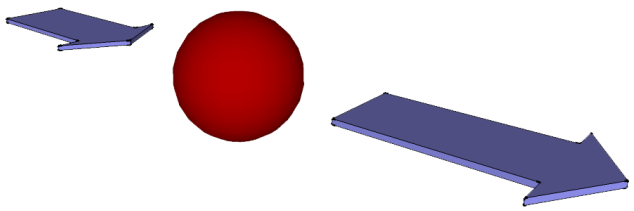
Virus



Worm

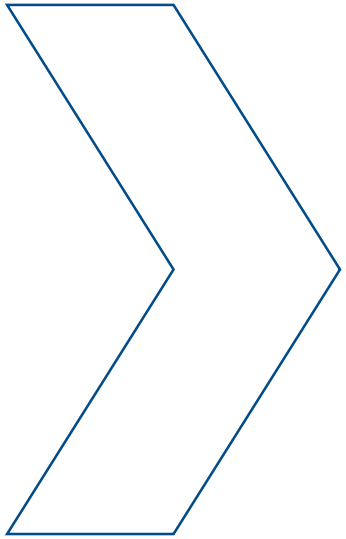


Trojanski konj



Stuxnet

- Virusi
- Worms (crvi)
- Trojanski konji
- Rootkits



Stuxnet

Širenje

- **Prvi korak** - inficiranje (najveći broj inicijalnih infekcija je bio preko USB flash drive korišćenjem ukradenih pravih digitalno potpisanih drajvera)
- **Drugi korak** – upoznavanje okruženja (Stuxnet istražuje da li je inficirani računar vezan za odgovarajuće kontrolere, da li je na mreži, da li je na pravoj lokaciji, nakon toga odlučuje da li deluje, širi se dalje ili se briše sa računara)

Širenje

- Treći korak – ažuriranje (ukoliko je računar onaj na kome će Stuxnet delovati, pokušava da se zakači na internet u pozadini i skine noviju verziju sebe)
- Četvrti korak – kompromitovanje (ukoliko je na pravoj mreži, prepoznaje računare sa kontrolerima, Stuxnet se širi koristeći zero days vulnerabilities, usb, lan, štampači)

Širenje

- Peti korak – osmatranje i kontrola (na računaru koji upravlja kontrolerom, Stuxnet prvo prikuplja podatke i analizira ih, ukoliko može pošalje ih preko interneta ukoliko ne odlučuje kako da deluje)
- Šesti korak – maskiranje i uništenje (pošto je analizirao podatke, naizgled ispravne podatke šalje ljudima koji kontrolišu sistem da ih zavara, u pozadini na potpuno drugačiji način upravlja sistemom i uništava ga)

Komponente - Rootkit

- Zadužena za ulazak u Windows sisteme i preuzimanje kontrole
- Koristi 20 zero-days propusta
- Koristi originalne bezbednosne sertifikate (ukradene npr. od Realtek-a)
- Koristi stvarne administrativne privilegije a ne lažne

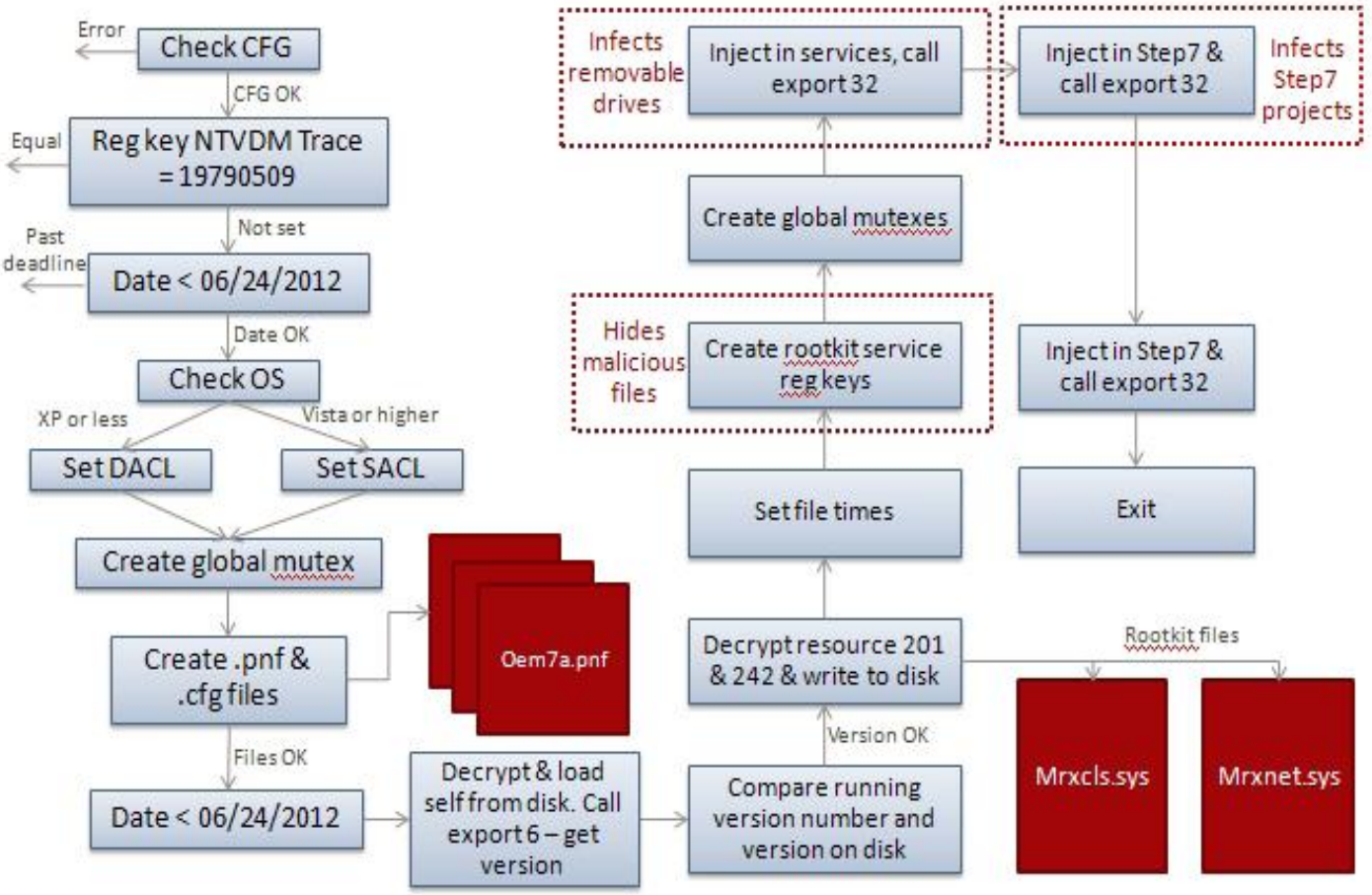
Komponente – Virus i crv

- zadužene za širenje i traženje ciljnog računara
- širenje putem zaraženih fajlova
- zaraženog USB flash-a (MS10-046)
- mrežnih deljenih diskova
- štampača (MS10-061)
- MS10-073 kernel drajver, MS10-092 task scheduler, CVE-2010-2772 standardna lozinka, MS08-067 server servis

Komponente – Trojanski konj

- neutralisanje antivirus servisa
- ažuriranje „Stuxnet“-a
- ispitivanje cilja
- preuzimanje kontrole nad PLC kontrolerom i reprogramiranje
- preuzimanje kontrole nad senzorima i dojavljivačima
- kraj širenja 24.6.2012.

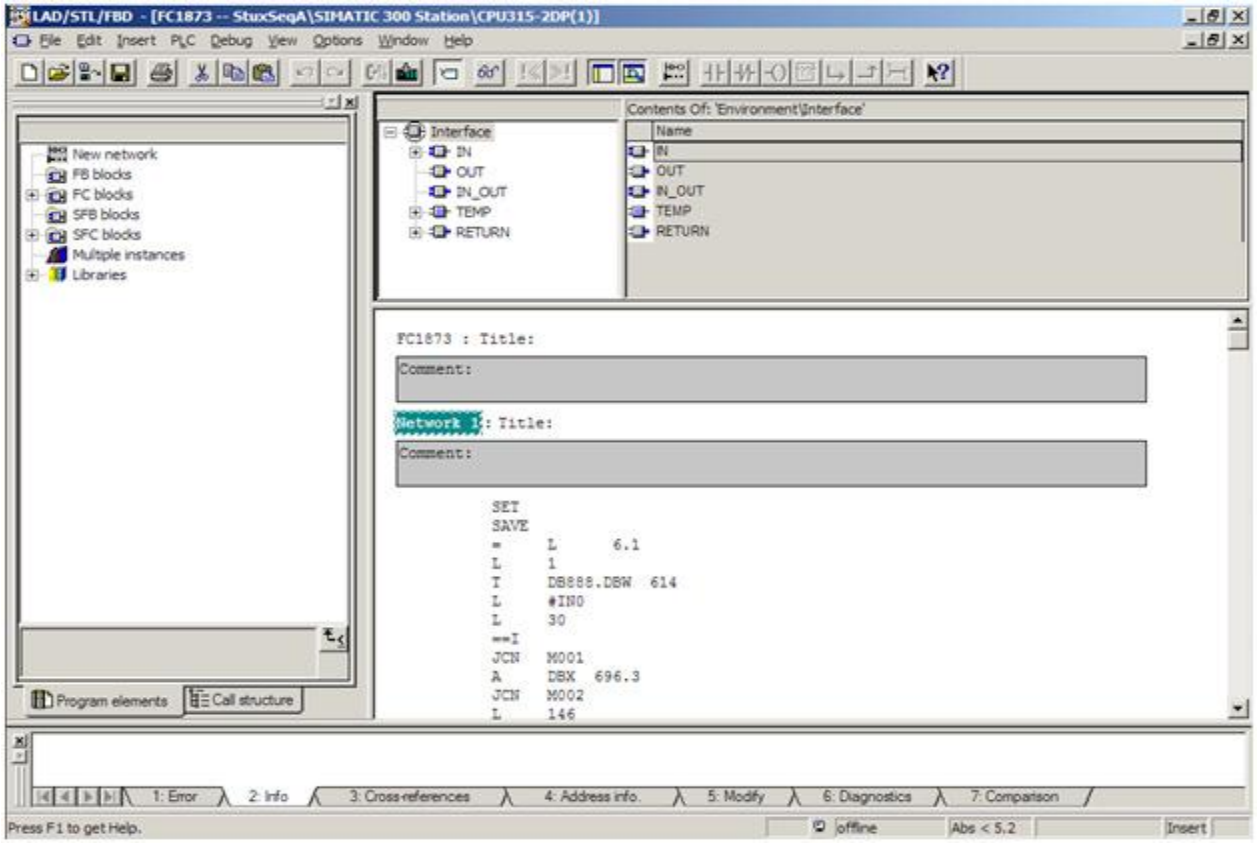
Algoritam širenja



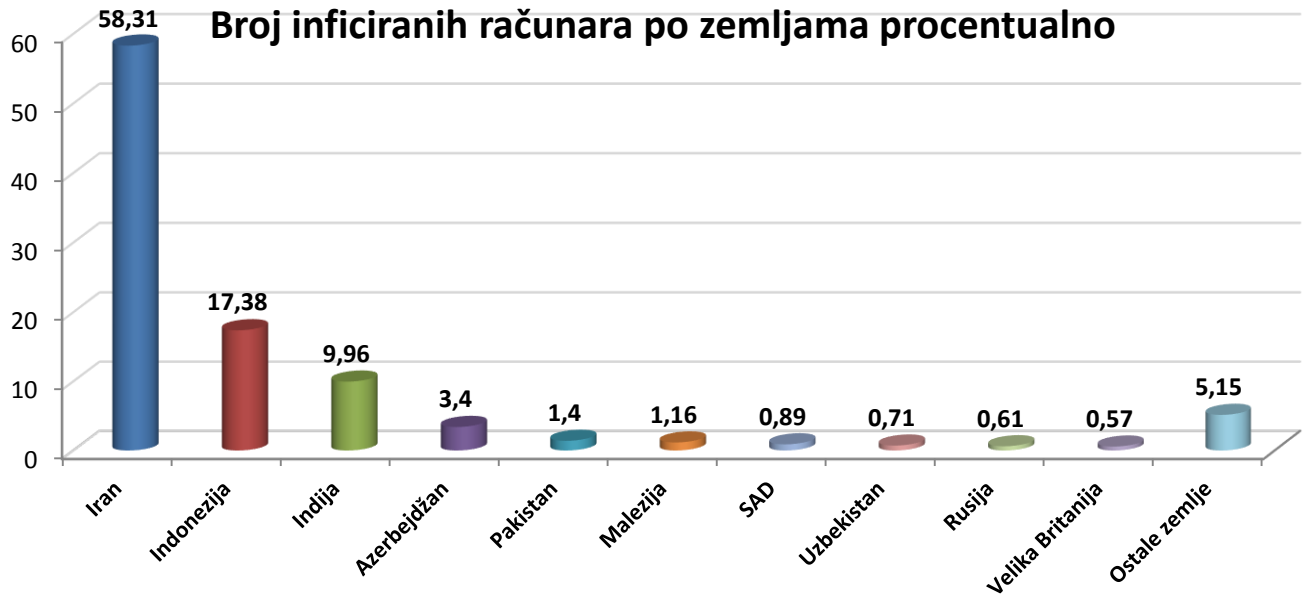
Napadani segmenti

- Windows OS
- Siemens PCS 7, WinCC and STEP7 industrijski softver koji radi pod Windows OS
- Siemens S7 PLCs.

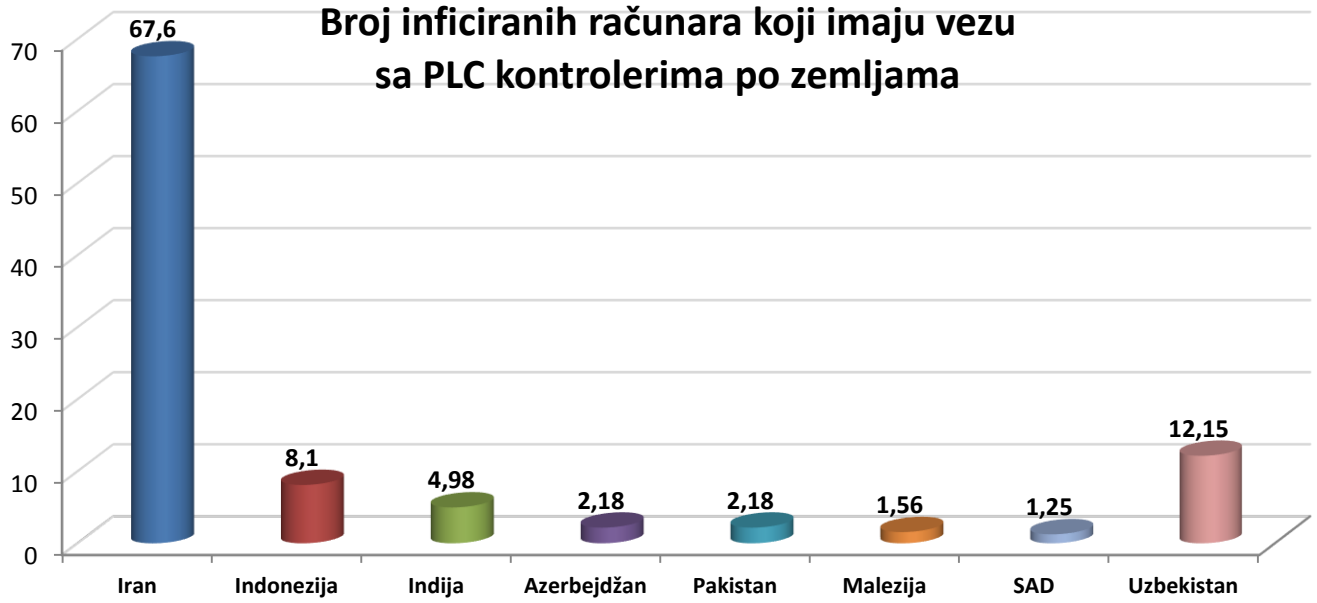
Step7 softver



Ciljane teritorije



Ciljane teritorije



Autori

- Ne postoji potvrda ko su autori, sumnja se:
  - Stuxnet grupa USA
  - Equation grupa USA
  - Unit 8200 Israel
    - Myrtus (mirta, Hadaša- Hadassah ili Esther)
    - "b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb" ili "My-RTUs„ (RTU – remote terminal unit)

```
.rdata:00011D95                 db    0
.rdata:00011D96                 db    0
.rdata:00011D97                 db    0
.rdata:00011D98 aBMyrtusSrcObjf db 'b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb',0
.rdata:00011DC4                 db    0
.rdata:00011DC5                 db    0
.rdata:00011DC6                 db    0
.rdata:00011DC7                 db    0
```

Još o Stuxnet-u

- Pojavio se najmanje godinu dana pre nego što je javno otkriven (jun 2010.)
- Postoje najmanje 3 varijante (jun 2009., mart 2010. i april 2010.)
- Ažurira se kroz LAN peer-to-peer

Otvorena pretnja

Ko je kreirao Stuxnet i njegove sledbenike (Flame, Duqu, Gauss…) postaje manje bitno…

Najbitnije pitanje je ko će ih reprogramirati, učiti iz njihovog koda i pronaći nove destruktivne upotrebne vrednosti za ove maliciozne programe.

Hvala na pažnji

Aleksandar Kostadinović
Aleksandar.kostadinovic@rnids.rs

rnids.rs
рнидс.срб

domen.rs
домен.срб