Outredda IT-brott –
Hot mot samhället och rikets säkerhet

FOI

Överdriven rubrik?

FOI

Pop quiz

- Nämn en sektor eller tjänst i samhället som både
  - Är viktig för samhället
  - Fungerar om datorerna försvinner

FOI

Operation Olympic Games

FOI

Kufikvadrater

FOI

Men det var då det..

FOI

Det intressanta ligger här:

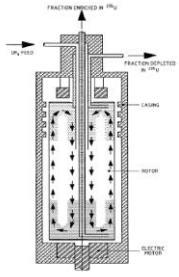
The gas centrifuge uranium enrichment plant at Natanz, Iran.

Under ytan ..

- 100,000 m2
- 8 meter under jorden
- Tak av stålarmerad betong 2.5 meter tjockt
- Med ytterligare 22 meter packad jord ovanpå.
- En stor mängd centrifuger.

Urananrikning for dummies

- Extraherar U235 from UF_6
- Genom centrifugal-extraktion
- Israel, EU och USA var emot att Iran anrikade Uran
- Iran hävdade att deras kärnkraftsprogram var fredligt



FOI

Tidslinje

- 2002 <200 centrifuger
- 2003 Underjordiskt komplex påbörjas
- 2006 FN-resolution 1696 kräver att Iran upphör med all anrikning.
- 2006 ~3000 centrifuger
- 2007 IAEA rapporterar: Endast 2/3 centrifuger i drift

FOI

Tidslinje fortsättning

- 2009 Projektet har allvarliga svårigheter på grund av kvalitetskontroll. Minst 1000 centrifuger har skrotats. Chefen för kärnkraftsprogrammet avgår.
- 2010 IAEA: 3772 fungerande, 5084 fortfarande inaktiva centrifuger
  - Prof Massoud Ali Mohammadi mördad 12 Januari
  - Dr Majid Shahriari mördad 29 November
  - Kemiingenjör Fereydoon Abbasi Davani överlever mordförsök 29 November, blir chef över kärnkraftsprogrammet
- 2011 Darioush Rezaeinejad mördad 23 Juli (USA förnekar inblandning)
- 2012 Dr Mostafa Ahmadi Roshan mördad 11 Januari (USA förnekar inblandning)

FOI

Stuxnet

- Juni 2010 VirusBlokAda hittar en ny malware.
- 15 Juni publicerar de sina data.
- 15 Juni, något senare under dagen, DDOS av okänt ursprung slår mot mailinglistor för SCADA-säkerhet. Många prenumeranter missar publiceringen.
- Malware:t döps senare till Stuxnet, och det är ~~MAGNIFIKT!~~ mycket farligt.

FOI

Stuxnet tidslinje/version

- 0.500 3 november 2005, C&C server registreras
- 0.500 4 juli 2009, Infektionsstoppdatum
- 1.001 June 22, 2009 Main binary compile timestamp
- 1.100 March 1, 2010 Main binary compile timestamp
- 1.101 April 14, 2010 Main binary compile timestamp
- 1.x June 24, 2012 Infection stop date

FOI

Vad gör det?

- Det angriper ICS på ett mycket lömskt sätt.

FOI

Infektion

- USB-sticka
  - Primärinfektion är via en USB-sticka i ett MS Windows-system.
  - Vapnet använder en sårbarhet i Windows shortcuts för att installera sig utan användarens hjälp
- RPC-exploit för Windows
  - Används för att sprida sig genom Windows-nätverk
- Rootkits, både för user-mode and kernel-mode används för att dölja vapnet medan det sprider sig.
- Vapnet uppdaterar sig själv och äldre kopior den stöter på, via C&C Servrar i Tyskland och Burma.

FOI

Infektion fortsättning

- Vapnet använde fyra Zero-day-sårbarheter, plus CPLINK och Conficker exploits för att utföra infektionen.
- Rätt hyfsad vapenlast.

FOI

Målsystem

- Men allt detta var bara för att kunna nå ett specifikt mål
- En Windows server som kör WinCC
- WinCC används för att uppdatera PLC:er i ett ICS
- Vapnet hade två äkta certifikat från företagen Jmicron och Realtek med vilka programvaruuppdateringen hade signerats.
- Med ytterligare en Zero-day-sårbarhet och certifikaten förmås WinCC att uppdatera PLC:erna med ny mjukvara.

FOI

Om inte…!

- Stuxnet hade en säkerhetsspärr:
  - Siemens S7-300 PLC:er..
  - ..som kontrollerade motorstyrningsenheter..
  - ..från antingen Fararo Paya, eller Vacon..
  - ...som är inställda på frekvenser mellan 807-1210Hz

FOI

Verkansdelen

- Rootkit som gömmer vapnet, men också döljer dess aktivitet från operatören
- Ibland ändrar den styrfrekvensen upp till 1402Hz, ner till 2Hz upp till 1064Hz och tillbaka till normal drift
- Om detta hände med en centrifug, som är en tunn aluminiumcylinder, skulle den antagligen skaka sönder sina kullager, och kanske också börja spricka.
- Även om ingen fysisk skada sker kommer anrikningen att dramatiskt försämras.

FOI

Notera skillnaden:

Kontorsnätverk

- Fyra Zero-days
- Två kända exploits
- Två root kits
- C&C nätverk
- P2P nätverk
- Två stulna certifikat

ICS-nätverk

- Root kit

FOI

Varför?

PC

PLC

FOI

Intressant, men so what?

- Vad har det här med forensik att göra?

FOI

Varför bygger vi system så här?

FOI

Att tänka cyberangrepp

FOI

Varför begås IT-brott?

- Tillfälle
- Vinning
- Låg risk för konsekvenser

FOI

Låg risk – många mål –stora vinster

FOI

Vad händer om vi fortsätter?

Aktörer

- Enskilda individer
  - Hacktivister, Vandaler, Hämnare, Insiders
- Spioner
  - Företag, länder, övriga
- Terrorister
- Kriminella
  - Organiserad brottslighet
- Främmande stater
  - Militära förband eller OGA
- Automatiska angrepp via datorprogram som maskar eller virus.
- AI-vapen

Hotskalan illustrerad.

Sammanfattning: Forensik…

- Talar om vad som hänt när något gått fel
- Ger underlag för att patcha sårbarheter
- Ger underlag för bättre systemdesign
- Är en förutsättning för att kunna lagföra IT-brott

FOI

Slut, frågor?

FOI