Stuxnet – Modus Operandi

Liam O Murchu
Operations Manager, Symantec Security Response

March 2011
Agenda

1. Time Line
2. Versions - what changed
3. Targets - Initial and Final
4. Success
5. Techniques – moving from initial to final target
Stuxnet Features

• Discovery disclosed in July, 2010
• Attacks industrial control systems likely an Iranian uranium enrichment facility

• Modifies and hides code on Siemens PLCs connected to frequency converters

• Contains 7 methods to propagate, 4 zero day exploits, 1 known exploit, 3 rootkits, 2 unauthorized certificates, 2 Siemens security issues.

• 3 versions, June 2009, March 2010, April 2010
Stuxnet’s Targets

Iranian Uranium Enrichment facilities

Geographic Distribution of Infections

- Iran: 58.31%
- Indonesia: 17.83%
- India: 9.96%
- Azerbaijan: 3.40%
- Pakistan: 1.40%
- Malaysia: 1.16%
- USA: 0.89%
- Uzbekistan: 0.71%
- Russia: 0.61%
- Great Britain: 0.57%
- Others: 5.15%

Frequency Converters

Fararo Paya
Iranian built
Stuxnet’s Targets

Intended Final Target

- S7-315 CPU
- CP-342-5 – 6 modules

31 Vacon or Fararo Paya frequency converters per module

Totaling up to 186 motors
Data Analysis

• Samples:
  – Information about each infected computer is stored in each sample
  – Time stamps of the files tell us when the Stuxnet project occurred.

• Command and control servers statistics
Stuxnet Timeline

**June 2008**
Programming of Stuxnet has begun.

**June 22 2009**
First Version of Stuxnet is compiled. It is ready to be released.

**Jan 2009**
Some components have been completed.

**June 22 2009**
First infection of Stuxnet occur in Iran less than 24 hours after the code was compiled.

**Jan 2010**
Some components for a new version of Stuxnet are completed.

**April 2010**
Another new version of Stuxnet released.

**March 2010**
New version complete. USB zero day code added.

**March 2010**
First infection from this version occur. Spreads very quickly.

**May 2010**
Infections from new version start.

**June/July 2010**
Stuxnet Discovered.
Versions

- June 2009
  - only moderate infection numbers
- March 2010
  - Spreads very quickly
  - Removed old OS’s
  - Added USB zero day
- April 2010
  - Extended time to live
  - Extended spread time for USB
Initial Targets

- 5 organizations with a presence in Iran targeted
- All involved in Industrial processing
- None are Natanz
- No direct access to Uranium enrichment facility
- Infect someone close to Uranium enrichment process
- Piggy back into the facility when that person visits/interacts with someone at the facility
- One organization targeted by all 3 versions
Stuxnet Methodology

• No direct access to target
• Infect organizations that interact with target
• Study how these organizations interact
• Get insider knowledge of facilities layout
  – Plc type, Hardware in use, etc
• Create aggressive spreading worm to target:
  – The relationships of trust
  – The actual physical layout
Success

• 1 year undiscovered – first released in June 2009
• 4 zero days – first time any threat has done this
• Reliable code – professionally written code
• PLC codes appears to work
• Signed drivers – stolen certificates
• > 100,000 infected machine before discovery mostly in Iran
• IAEA report 1000 centrifuges with drawn from service
  – Unknown if Stuxnet caused this..??
Stuxnet Failures

- Discovered 3 months after USB zero day added
- No report of centrifuges out of action since March
- Gained high media attention
- Analysis performed
- Iranian authorities aware
- Traces left in code
How Stuxnet Attacks

Stuxnet uses 7 different methods to propagate!

1. USB drives – Zero Day
2. Print Spooler Vuln – Zero Day
3. Ms08-067 Vuln
4. Network Shares
5. P2P sharing
6. Wincc Hard coded Password
7. Step7 projects
Attack Execution

1. Initial Delivery

2. Network Exploits

3. Reporting Updates

4. Bridge AirGap

5. Deliver Payload

Internet Etc

Corporate LAN

Stuxnet – Getting to the target
Self-Replication
Step 7 Project Files

- MyProject.s7p
  - ApiLog
  - hOmSave7
    - S7HK40AX
      - s7hkimdb.dll
    - S7HK41AX
      - s7hkimdb.dll
    - ... 
  - xutils
    - links
      - s7p000001.dbf (Stuxnet datafile)
      - listen
      - xr000000.mdx (encrypted Stuxnet)
      - s7000001.mdlx (Stuxnet config data file)
    - ...

```
| types:           |
| DB 14 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| +00 WORD count   |
| +02 BYTE[] records |
```

- %Step7%\S7BIN
- %SYSTEM32%
- %SYSTEM%
- %WINDIR%
- project's hOmSave7/* subdirectories
New Version

- Not simple to create new version
- Cannot just drop in new zero days
- Target specific information required
- PLC programming knowledge
- Exploit knowledge

- Real danger is the idea
- Now people know it can be done
- People can start their own projects knowing it is possible
Solutions & lessons learned

• Insider/Contractor threat is significant
• IP is extremely valuable, protect it at all costs
• Monitor systems and networks
• Watch for red flags
• Accept that network separation is not possible and protect computers inside the traditional air gap more vigorously
• White listing, behavior blocking and reputation based solutions can mitigate threat.
• Device blocking – USBs, contractor laptops, etc..
• Vigilance is key
Response

- Need dedicated resources in place in advance that can switch focus to a new threat quickly
- Need engineers who are familiar with the latest developments in the threat landscape
- Need to respond quickly – critical infrastructure may be at risk
- Private public partnership will be important
- Growing market
- We will see more of these types of threats in the future, need to prepare for that.
Summary

• Stuxnet is the first publicly known malware to intend real-world damage

• Required resources at the level of a government

• While as a whole extremely sophisticated, the technique to inject code into PLCs is not

• Enterprises should assume attackers know how these systems work

• Has changed our job at Symantec

• We expect to see more of these threats
White Paper Available

W32.Stuxnet Dossier

• Stuxnet Technical Details Available here:

Thank you!

Liam O Murchu - liam_omurchu@symantec.com