INTERNET ATTACKS AGAINST NUCLEAR POWER PLANTS

Kleissner & Associates
IAEA, 1-5 June 2015, Vienna/Austria
International Conference on Computer Security in a Nuclear World

About myself

Programmer and security researcher
Prague, Czech Republic

- 2008-2009 Employee at the antivirus company Ikarus
- 2010 Austrian military
- 2012 External employee at a bank
- 2013-now CEO & Founder of Kleissner & Associates s.r.o.

Main fields: Windows security, banking, malware

Attack Vectors

1. Administrative computers of NPP

Could be used as entry point for targeting industrial computers.
Often have lower security standards and according to Virus Tracker many general infections.
An attacker could be interested to steal sensitive documents.

2. Industrial Computers

Usually air-gapped for security reasons.
USB thumb drives could defeat this air-gap, as done with Stuxnet in connection with exploits. Or via social engineering (delivering fake updates).

Backdoors are never a good idea!

- Backdoors can be potentially used by anyone else
- Abandoned botnets could be taken over by anyone
- Infections often disable antivirus and firewalls and therefore make the system more vulnerable

- Bots might remain for decades
  - => Even if the C&C protocol is properly secured, the encryption technology might get broken in the future; Example: Conficker A with 1024 bits RSA encryption

- Stuxnet infections can be controlled by anyone who owns the C&C domains (!), due to lack of proper protocol encryption

K&A

Stuxnet

- Operation “Olympic Games” since 2006, signed off by the Bush administration [1]
- Discovered in June 2010 by Virusblokada antivirus company [2]
- Multiple versions uncovered by security companies [3]
  - A lot of research by Symantec and Kaspersky
- Based on “Tildet” platform just as Flame, Duqu and Gauss [4]
- Targeting nuclear power plants, specifically Natanz, Iran according to reports
- Modifies S7P projects (the programs for controlling the industrial machines)

- Kill switch set to June 24, 2012 – no more spreading then [5]

How researchers know dates & version numbers

The Windows executable file format (PE) has multiple digital artifacts:

- Compilation Timestamp
- Resources -> Version numbers
- Rich Header with additional linker information
- Debug information (PDB file path) and strings

Historical domain information reveals dates and whois info of domains. Researchers can link different domains to the same owners through DNS records and whois information (by use of reverse lookups).

Virus Tracker

- Detects infected machines by sinkholing (registering C&C domains)
- More than 2.5 million devices per day seen

- Including Stuxnet, Flame & other espionage attacks
- We have Stuxnet since 2013 in the system!

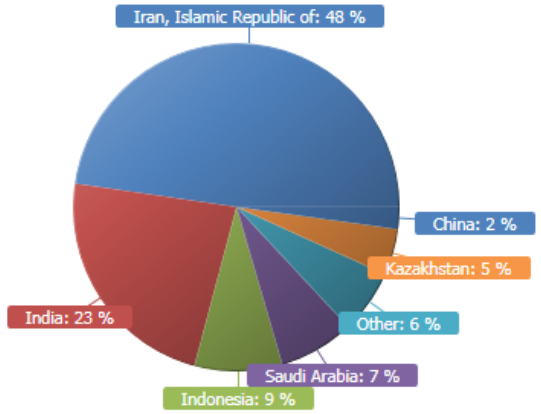
Stuxnet in Virus Tracker

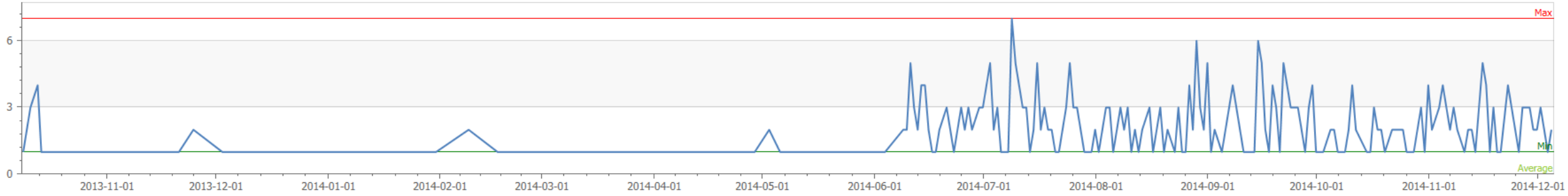
153 unique identifiers as reported by Stuxnet

221 unique decoded Stuxnet requests
268 unique IP addresses
419 infection records in Virus Tracker

Statistics

Percentage	Infection Records	Trojan
47.71	198	Iran, Islamic Republic of
23.13	96	India
8.67	36	Indonesia
7.47	31	Saudi Arabia
6.27	26	Other
4.58	19	Kazakhstan
2.17	9	China





Geographical Distribution

Information sent to the C&C

The data as it arrives at the Virus Tracker sinkhole:

2014-07-25 11:00:43 Pars Online PJS APT Stuxnet
188.245.250.173 Iran, Islamic Republic of Pars

www.mypremierfutbol.com

/index.php?data=66a96e28c013f8202df26332f5f8fcb5ff6b4f896e53b077fd1ccdabb8493f9b5390d446f2a
7645fa21d659d3fb4a87fe20af1d5f5e6c875c2bfe58f280ca956dc8427bdea6c5b1ee87734ff1da972a54fa39
1baa9e542c0b4fded6951ff24f0ba4fb4ce453ed141def05ad8cd19d613f0e5dfd9d21ed0b9f1cf7454c466a5e
757c0f81862fe2db9a907879d59d678d391

Information sent to the C&C

The data as it arrives at the Virus Tracker sinkhole:

2014-07-25 11:00:43 Pars Online PJS APT Stuxnet
188.245.250.173 Iran, Islamic Republic of Pars

www.mypremierfutbol.com <- our sinkhole C&C server

/index.php?data=66a96e28c013f8202df26332f5f8fcb5ff6b4f896e53b077fd1ccdabb8493f9b5390d446f2a
7645fa21d659d3fb4a87fe20af1d5f5e6c875c2bfe58f280ca956dc8427bdea6c5b1ee87734ff1da972a54fa39
1baa9e542c0b4fded6951ff24f0ba4fb4ce453ed141def05ad8cd19d613f0e5dfd9d21ed0b9f1cf7454c466a5e
757c0f81862fe2db9a907879d59d678d391

Hex encoded and XOR encrypted information!

Information sent to the C&C

The infection sends this information to the command & control server:

- Unique identifier of the Stuxnet infection (GUID)
- Main internal IP address
- Computer Name
- Domain Name
- IP address of interface 1
- IP address of interface 2
- IP address of interface 3
- Windows major and minor version
- Windows Service Pack version
- Whether Siemens SCADA software is installed
- Project path of a found SCADA program

Information sent to the C&C

```
-------- STUXNET INFECTION --------
  ID: F6A01E50-AF89-4081-9338-B6E27731FFD5
  Main IP: 188.245.250.173
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: GERDOO-7A1D2321
  Domain: MSHOME
  IP Interface 1: 188.245.250.173
  IP Interface 2: 192.168.1.5
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

```
-------- STUXNET INFECTION --------
  ID: 03C28E58-8C9F-4BF2-83AE-0102FEF9B19C
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: NEWTECH
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.45.94
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

```
-------- STUXNET INFECTION --------
  ID: F4BBB568-A3BC-4062-A37D-C8664B882711
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: H-C16EBB8501304
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.39.254
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

Information sent to the C&C

```
-------- STUXNET INFECTION --------
  ID: F6A01E50-AF89-4081-9338-B6E27731FFD5
  Main IP: 188.245.250.173
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: GERDOO-7A1D2321
  Domain: MSHOME
  IP Interface 1: 188.245.250.173
  IP Interface 2: 192.168.1.5
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

S7P project path of an Industrial program

```
-------- STUXNET INFECTION --------
  ID: 03C28E58-8C9F-4BF2-83AE-0102FEF9B19C
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: NEWTECH
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.45.94
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

```
-------- STUXNET INFECTION --------
  ID: F4BBB568-A3BC-4062-A37D-C8664B882711
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: H-C16EBB8501304
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.39.254
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

Information sent to the C&C

```
-------- STUXNET INFECTION --------
  ID: F6A01E50-AF89-4081-9338-B6E27731FFD5
  Main IP: 188.245.250.173
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: GERDOO-7A1D2321
  Domain: MSHOME
  IP Interface 1: 188.245.250.173
  IP Interface 2: 192.168.1.5
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

S7P project path of an Industrial program

```
-------- STUXNET INFECTION --------
  ID: F4BBB568-A3BC-4062-A37D-C8664B882711
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: H-C16EBB8501304
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.39.254
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

```
-------- STUXNET INFECTION --------
  ID: 03C28E58-8C9F-4BF2-83AE-0102FEF9B19C
  Main IP: 169.254.124.74
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: NEWTECH
  Domain: WORKGROUP
  IP Interface 1: 169.254.124.74
  IP Interface 2: 213.217.45.94
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------
```

2 Stuxnet infections in the same internal network behind 1 public IP

Information sent to the C&C

Those 3 Iranian infections compared:

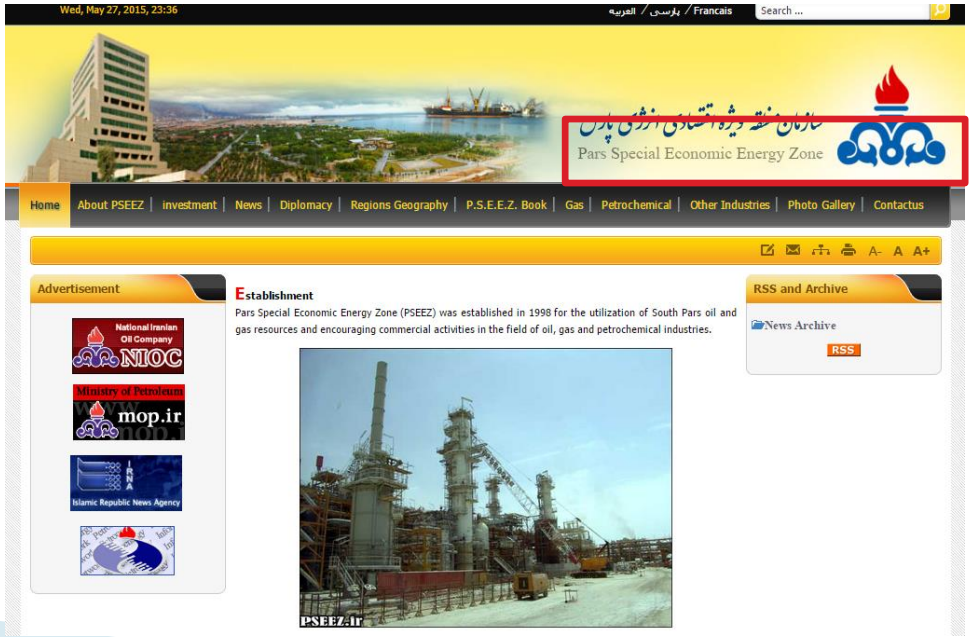
Public IP	OS	Computer	Domain	IP 1	IP 2
188.245.250.173	Windows 5.1	GERDOO-7A1D2321	MSHOME	188.245.250.173	192.168.1.5
213.217.39.254	Windows 5.1	H-C16EBB8501304	WORKGROUP	169.254.124.74	213.217.39.254
213.217.45.94	Windows 5.1	NEWTECH	WORKGROUP	169.254.124.74	213.217.45.94

Public IP is the one as seen by Virus Tracker when the infection checks in. The other info is listed as it was sent by the infection.

All Stuxnet infections with SCADA installed

Date	IP	Stuxnet Id	Country	ASN	Organization by IP lookup
7/25/2014 11:00	188.245.250.173	F6A01E50-AF89-4081-9338-B6E27731FFD5	Iran	AS16322	Rasaneh Pardaz Sepahan Co.
9/8/2014 13:25	213.217.39.254	F4BBB568-A3BC-4062-A37D-C8664B882711	Iran	AS16322	Parsonline-Dynamic-Pool
11/19/2014 16:57	213.217.45.94	03C28E58-8C9F-4BF2-83AE-0102FEF9B19C	Iran	AS16322	Parsonline-Dynamic-Pool
9/1/2014 07:01	31.29.61.10	CD994AB8-46EA-4461-AC05-35B017764E47	Iran	AS48309	Rasaneh Pardaz Sepahan Co.
9/12/2014 12:58	78.39.79.170	6791667B-B507-4681-A7CE-C3009911B0AA	Iran	AS12880	Pars Special Economic Energy Zone,Boushehr,IR
11/30/2014 10:44	113.229.7.74	ACB0AE39-8771-403D-8CC1-ECFFA7DCB5F1	China	AS4837	China Unicom Liaoning province network
12/5/2014 07:22	175.146.209.120	ACB0AE39-8771-403D-8CC1-ECFFA7DCB5F1	China	AS4837	China Unicom Liaoning province network

http://www.pseez.ir/en/home screenshot for reference:



Thanks for attending the presentation! Questions?

For any information please contact:

Email info@kleissner.org

Address Na strži 1702/65
140 00 Praha
Czech Republic

References

[1] NYT, David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran"
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[2] KREBS, B., "Experts Warn of New Windows Shortcut Flaw"
http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/

[3] W32/Stuxnet Dossier, Symantec
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[4] Kaspersky, "Gauss: Nation-state cyber-surveillance meets banking Trojan"
https://securelist.com/blog/incidents/33854/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/

[5] MURCHU, L., Interview
http://gcn.com/articles/2012/06/26/stuxnet-demise-expiration-date.aspx