# Internet Attacks Against Nuclear Power Plants

P. Kleissner[1]

[1]Kleissner & Associates s.r.o., Prague, Czech Republic

*E-mail contact of main author: info@kleissner.org*

**Abstract.** This paper gives a technical overview of existing threats against nuclear power plants and their possibilities. It specifically addresses the state sponsored Stuxnet attack and provides technical insight and statistical information about active Stuxnet infections that still exist today.

**Key Words**: Stuxnet, Malware, Sinkholing, Virus Tracker

## 1. Introduction

Kleissner & Associates' agenda is to detect virus infections worldwide and provide infection information to relevant parties in real-time so that these infections can be removed. Technically, it does not matter whether the virus was developed by a government or an individual or intended for espionage or more generic purposes. There is no difference for our systems in the purpose or origin of the threat

In 2013 we acquired one domain used as a Stuxnet Command & Control server, which allows us to see who is still infected, and, in theory, allows us to potentially control these existing infections. In December 2014, we made a detailed investigation and statistical review of the infection data that we have presented herein.

## 2. Operation "Olympic Games"

Operation Olympic Games started in 2006. Signed off by the George W. Bush administration, this operation targeted the Iranian nuclear facility at Natanz. The operation accelerated after the election of Obama. [1] The computer virus was first discovered by the Belarus antivirus company VirusBlokAda and later analyzed in-depth by the security company Symantec. [2] [3] It is worth mentioning that various security companies reported other malware, such as "Duqu", "Flame" and "Gauss" were sharing the same or similar code and techniques of Stuxnet. [4]

Kleissner & Associates sinkholed (registered) the first Stuxnet C&C domain "www.todaysfutbol.com" on 10/9/2013 and the second "www.mypremierfutbol.com" on 6/8/2014. Through our custom developed Virus Tracker system we are able to monitor infected machines that connect to these domains.

Interestingly, and despite the monetary (likely in the millions EUR) and coding efforts of the Stuxnet developers, the C&C protocol was not properly secured. Information being sent from the infected machine to the C&C server is passed in the HTTP GET string as

"/index.php?data=[data]" where the data is only hex encoded and XOR encrypted with the 31-byte key (hex bytes) 67 A9 6E 28 90 0D 58 D6 A4 5D E2 72 66 C0 4A 57 88 5A B0 5C 6E 45 56 1A BD 7C 71 5E 42 E4 C1 and XOR encrypted with FF.

After decrypting the data, this information from the infected machine becomes clear:

- 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

According to the Symantec analyst who investigated Stuxnet there is a kill switch which will stop Stuxnet from spreading after June 24, 2012. [5]

### 3. Data Collected by Virus Tracker on Stuxnet

This statistical data was generated in December 2014 based on all Stuxnet infections ever discovered via Virus Tracker (since 10/9/2013) – a breakdown:

**Table I. Statistics on Stuxnet infections observed in Virus Tracker**

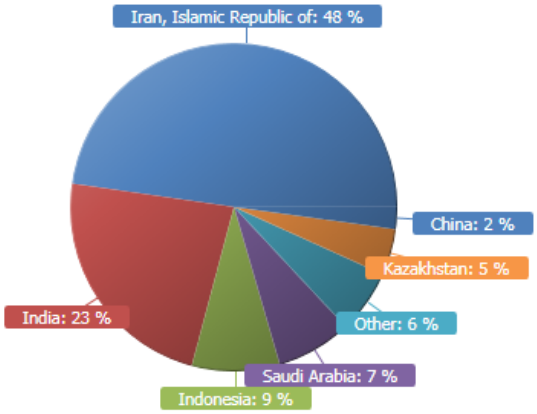
| Count | Name |
|---|---|
| 153 | Unique identifiers as reported by actual Stuxnet infections |
| 221 | Unique decoded Stuxnet requests |
| 268 | Unique IP addresses |
| 419 | Infection Stuxnet records stored in Virus Tracker |

Because a single unique Stuxnet infection might contact the C&C server (in this case the Virus Tracker sinkhole) multiple times, there are multiple infection records per unique infection. Infections might also connect via different IP addresses over time.

The amount of unique identifiers basically equals to unique Stuxnet infections; it is safe to say that in 2013 and 2014 there were at least 153 distinct infected machines with Stuxnet.

The geographical distribution of all Stuxnet infections:


*FIG. 1. Geographical distribution of Stuxnet infections 2013-2014.*




| 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 |

*FIG. 2. Country distribution of Stuxnet infections 2013-2014.*

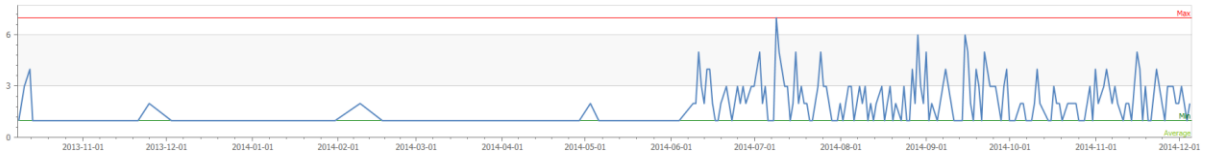


*FIG. 3. Infections contacting the Virus Tracker sinkhole over time 2013-2014.*

6 of the infections reported that they have SCADA development software installed (note that the one Chinese infection reported from 2 different IP addresses):

**Table II. Stuxnet infections with SCADA software installed**

| Date | IP | Stuxnet Id | Country |
|---|---|---|---|
| 7/25/2014 11:00 | 188.245.250.173 | F6A01E50-AF89-4081-9338-B6E27731FFD5 | Iran |
| 9/8/2014 13:25 | 213.217.39.254 | F4BBB568-A3BC-4062-A37D-C8664B882711 | Iran |
| 11/19/2014 16:57 | 213.217.45.94 | 03C28E58-8C9F-4BF2-83AE-0102FEF9B19C | Iran |
| 9/1/2014 07:01 | 31.29.61.10 | CD994AB8-46EA-4461-AC05-35B017764F47 | Iran |
| 9/12/2014 12:58 | 78.39.79.170 | 6791667B-B507-4681-A7CE-C3009911B0AA | Iran |
| 11/30/2014 10:44 | 113.229.7.74 | ACB0AE39-8771-403D-8CC1-ECFFA7DCB5F1 | China |
| 12/5/2014 07:22 | 175.146.209.120 | ACB0AE39-8771-403D-8CC1-ECFFA7DCB5F1 | China |

5 of those are from Iran with the first 3 of them connecting through the Iranian ISP "Pars Online". Out of all Stuxnet infections ever seen at Virus Tracker, these are the only ones having a Siemens Step 7 project path set to "C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p". This project path is likely the source project file for controlling an industrial machine (whether or not for a nuclear power plant remains speculation). Below is the decoded information that was sent from these 3 infections:

```
-------- 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
-----------------------------------
```

*FIG. 4. Data sent from Iranian Stuxnet infections containing an S7P project path.*

## 4. Risks of Similar Operations

It is inevitable that existing malware infections lower the overall security of the particular machines and the entire networks and therefore make it easier (or possible at all) for anyone else to intrude the system. Just as Kleissner & Associates' C&C domain control enables us to control any remaining Stuxnet infected machines, any capable intelligence service (or individual with the knowledge and skills) could seize control and potentially cause considerable damage leveraging the remaining infections.

Regardless of original intent, backdoor access is not exclusive to a designated team or attacker. Everyone has access. Researching other malware families reveals this to be the case for most, if not all of backdoor enabled malware. As soon as someone reverse engineers the protocol and extracts the keys, they can control any similarly infected devices. Securing the command & control protocol with proper state of the art public-private key encryption would certainly hinder 3rd parties from taking over infected systems. But our research shows that many infections remain active for years (perhaps decades). In which case, evolving technologies could easily compromise antiquated encryption standards (if any) and circumvent an infection's safeguards. A good example to this is Conficker A from 2008. Conficker A used an RSA key length of 1024 bits that is breakable by today's standards and has been considered insecure since 2013.

## 5. Entry Points to Nuclear Power Plants

When talking about intruding nuclear power plants by use of malware there has to be the distinction whether to infect administrative or industrial machines. Our Virus Tracker sinkhole data reveals many nuclear facilities have administrative systems infected with common viruses. This is not surprising. Infected administrative computers could be used to mount deeper attacks on machine control systems. Best practices dictate isolating industrial machines control systems from other internal networks with no direct line to the internet. To overcome the "air gap" USB thumb drives, for example, can be used to intentionally and unintentionally infect machine control systems by exploiting "0-day" vulnerabilities as practiced by Stuxnet. Other attack vectors involve installing backdoors in industrial (or networking) devices before they arrive for installation at a targeted facility or using social engineering techniques to install backdoors through vectors such as fraudulent updates.

## 6. Final Notes

Some of above mentioned infections and threat intelligence was shared appropriately within the security and intelligence community.

## 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.