

# Stuxnet

---

·  
**Background material for  
Course “Malware/botnet”**

# PLC

A **programmable logic controller (PLC)** or **programmable controller** is a [digital computer](#) used for [automation](#) of [electromechanical](#) processes, such as control of machinery on factory [assembly lines](#), amusement rides, or lighting fixtures.

Programs to control machine operation are typically stored in battery-backed or [non-volatile memory](#). A PLC is an example of a [real time](#) system since output results must be produced in response to input conditions within a bounded time, otherwise unintended operation will result.



# PLC features

- The main difference from other computers is that PLCs are armored for severe conditions (such as dust, moisture, heat, cold) and have the facility for extensive [input/output](#) (I/O) arrangements. These connect the PLC to [sensors](#) and [actuators](#). PLCs read limit [switches](#), analog process variables (such as temperature and pressure), and the positions of complex positioning systems. Some use [machine vision](#). On the actuator side, PLCs operate [electric motors](#), [pneumatic](#) or [hydraulic](#) cylinders, magnetic [relays](#), [solenoids](#), or analog outputs. The input/output arrangements may be built into a simple PLC, or the PLC may have external I/O modules attached to a computer network that plugs into the PLC.

# Timeline

- It was then discovered first June 17 by a Belarus AV development company, VirusBlockAda.
- July 15 **Frank Boldewin**, a security researcher, decrypted the worm and found it targeted Siemens WinCC and PCS7 control systems
- July 22 Siemens posted a tool to identify and repair systems, followed by similar actions from AV vendors.
- July 27 ID hosted their first panel discussion in a webcast, hosted in order to disseminate all available knowledge about the worm.
- Aug 2 Microsoft issued the emergency patch.
  
- (driver signature timestamp: january 2010)

# Stuxnet

- USB worm (works without internet).
- When first run W32/Stuxnet-J copies itself to <User>\Application Data\<random>.exe.
- Modifies registry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced  
Hidden  
0x00000002

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced  
HideFileExt  
0x00000001

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced  
ShowSuperHidden  
0x00000000

- Shortcut bug: When the USB token is opened (e.g. windows explorer), windows automatically starts specially crafted .lnk shortcuts
- Rootkit: malware installs two drivers: “[mrxnet.sys](#)” and “[mrxcls.sys](#).” signed by **RealTek’s private key**...
- Realtek certificate is then revoked (initiated by Microsoft)
- On 17<sup>th</sup> of July, a new version of Stuxnet was discovered: It contains drivers signed with **JMicron Technology Corp’s** private key.

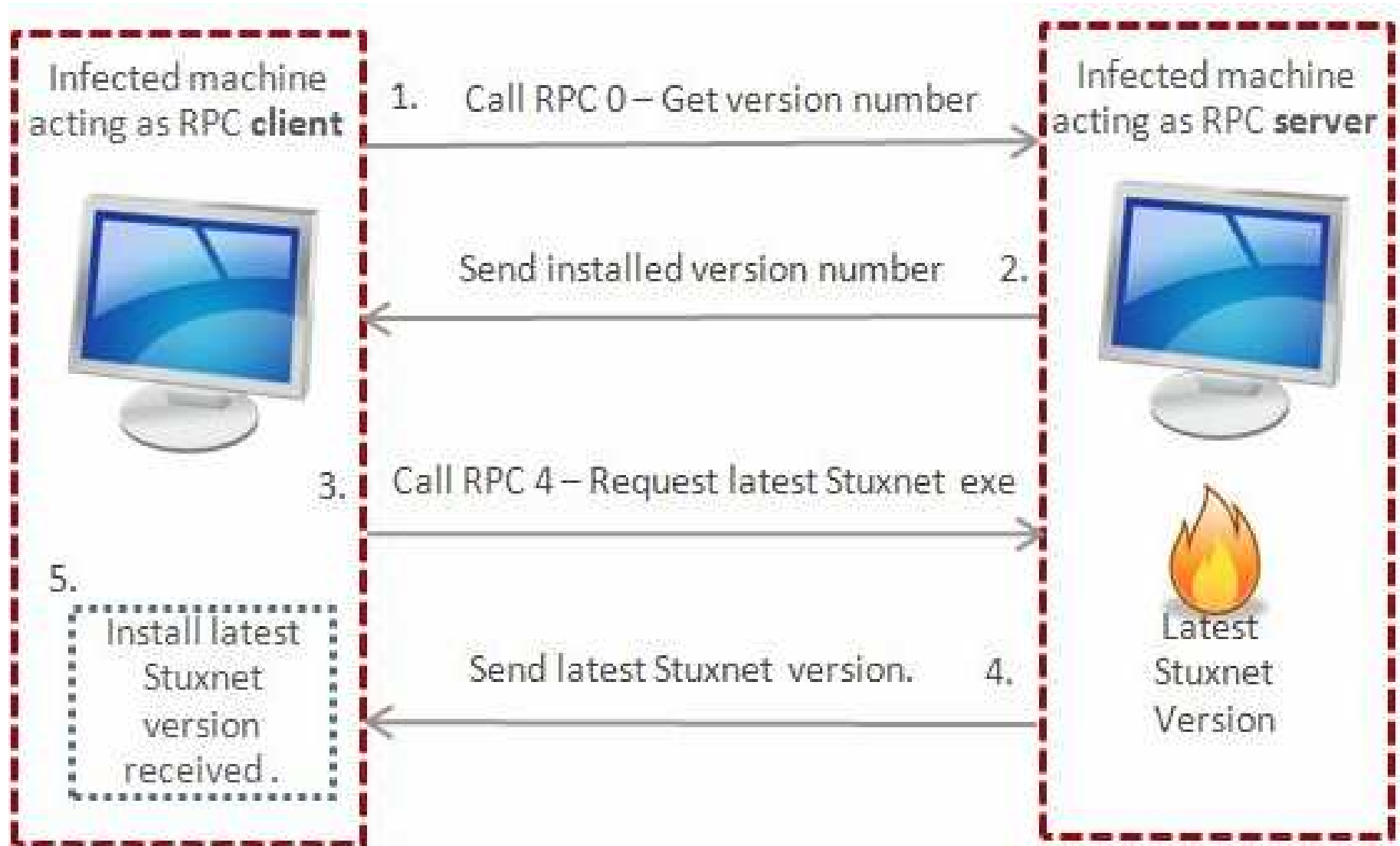
## 4 pieces of 0-day vulnerabilities

- .Ink handling
- Print Spooler (CVE-2010-2729) remote code execution vulnerability (spreading itself to new targets, allows writing to %System% remotely)
- Two other 0-days
- And several known vulnerabilities are also used

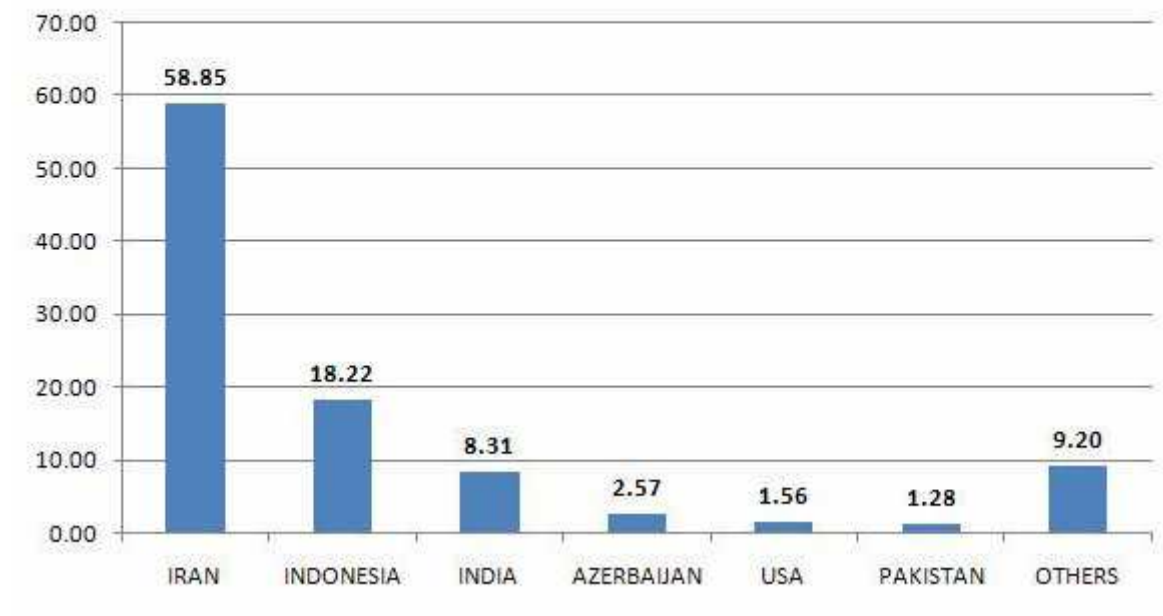
# P2P features

- - 0: returns the version number of Stuxnet installed
  - 1: Receive an exe and execute it (via injection)
  - 2: load module and executed export
  - 3: inject code to lsass and run it
  - 4: Builds the latest version of Stuxnet and send to remote machine
  - 5: create process
  - 6: read file
  - 7: drop file
  - 8: delete file
  - 9: write data records

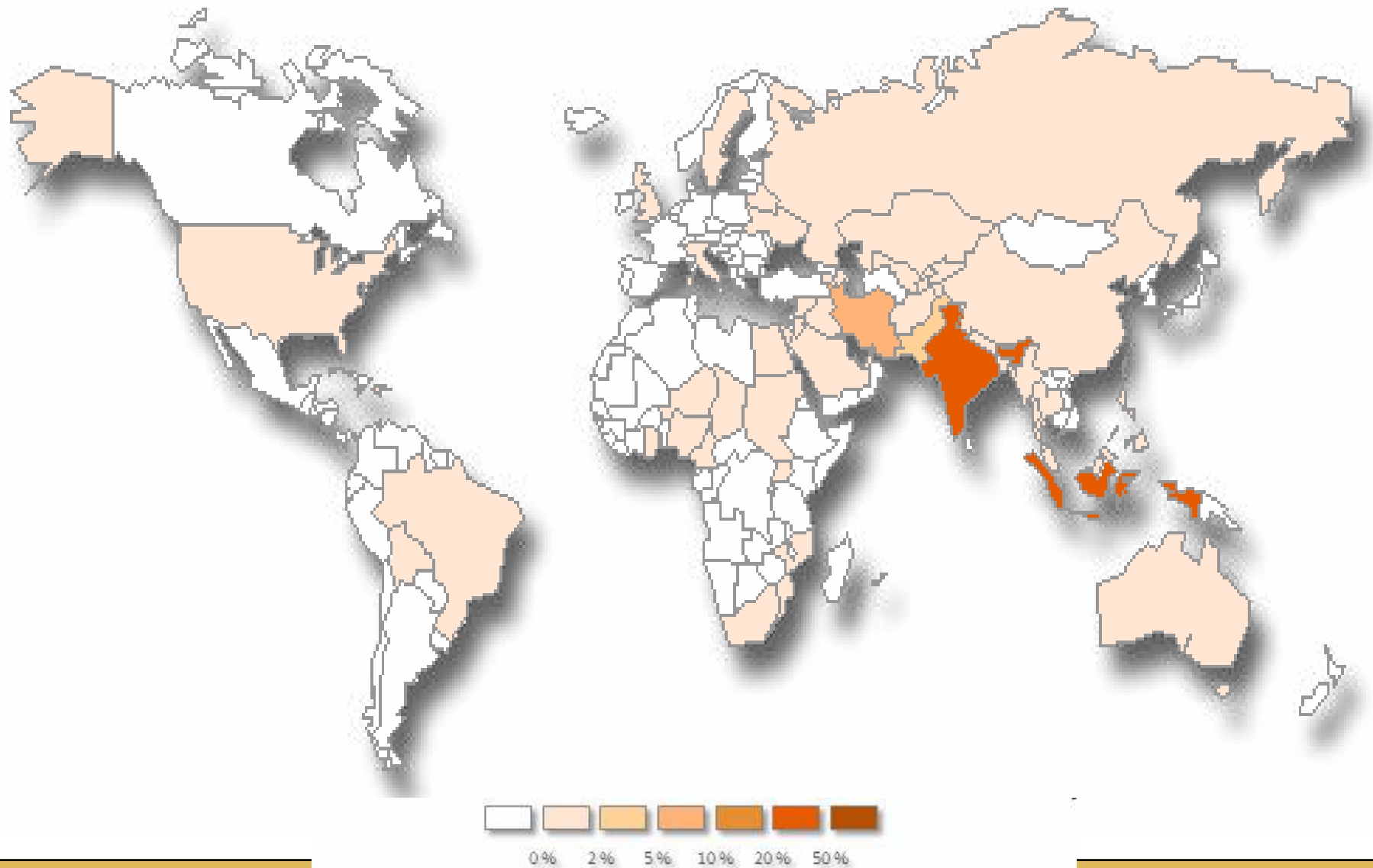
# P2P features of stuxnet



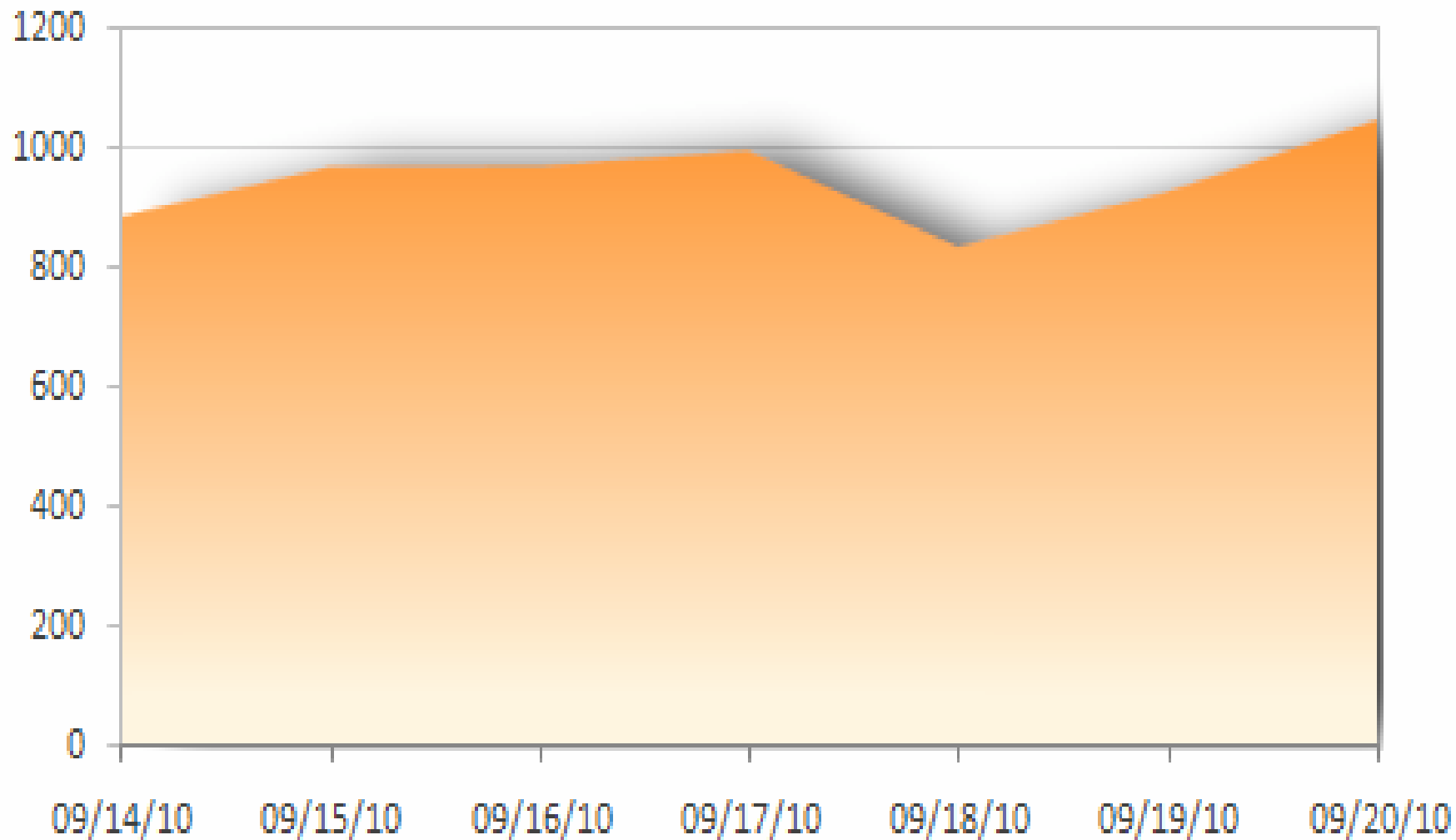
### Percentage of Hits from W32.Stuxnet by Country



# Geographical distribution



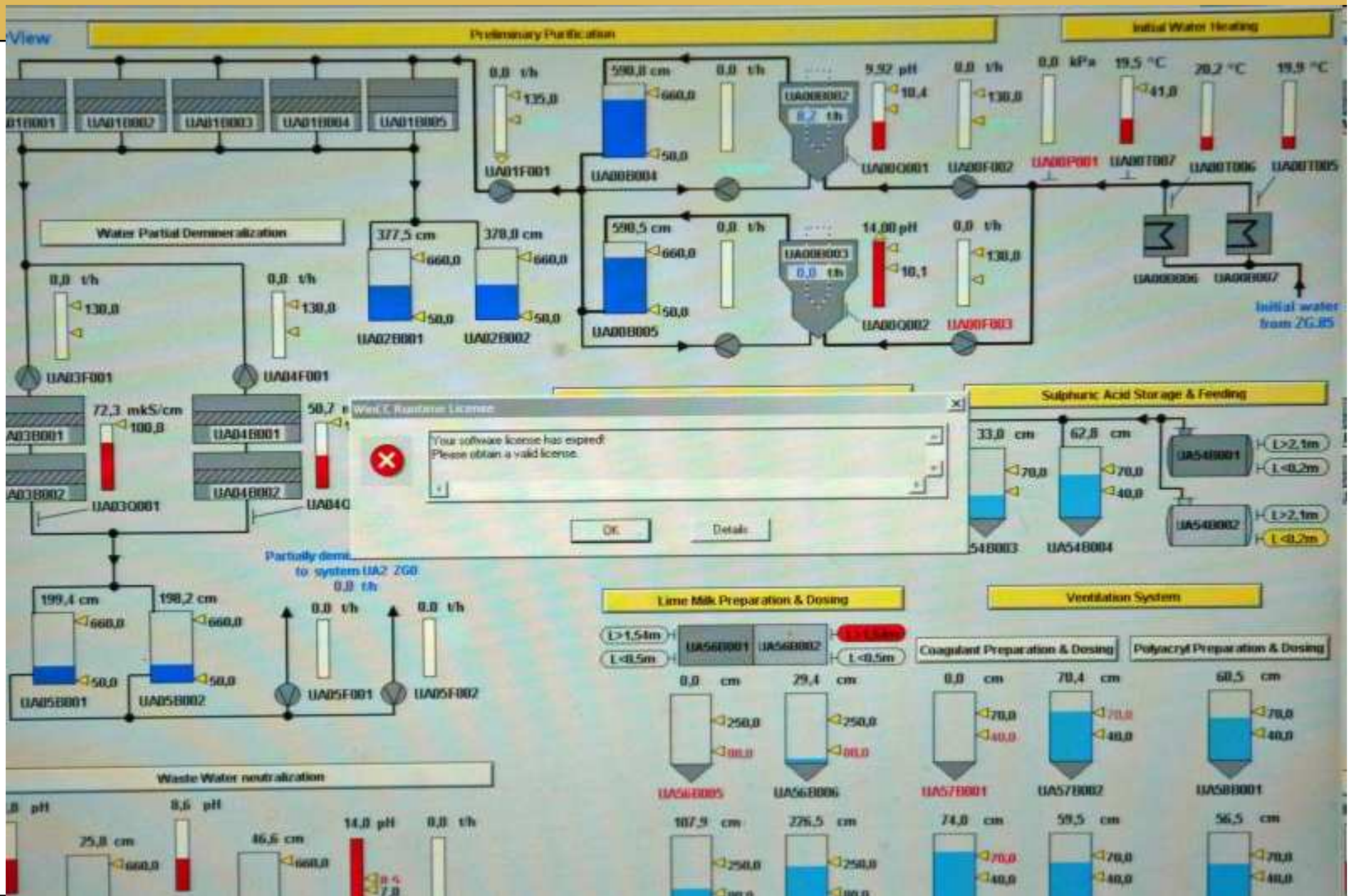
# Infection rate (symantec)



- [Symantec has posted information](#) that suggests this malware was searching for specific file types for design documents from the same Siemens systems that were targeted.
- Other reports note that in addition to malware, SCADA operators' responses were inhibited because [community support mailing lists were undergoing denial of service attacks](#). So not only were the attackers familiar with system weaknesses of particular SCADA installations, they might also have benefited from this reduced ability for site operators to communicate security issues.

# Targeted

- The attack highly targeted. Other sources say that the malware checks the fingerprints of the system (PLC, software version, etc.) and actually it's target is **one single system**.
- Stuxnet infects PLCs with different code depending on the characteristics of the target system. An infection sequence consists of PLC blocks (code blocks and data blocks) that will be injected into the PLC to alter its behavior. The threat contains three infection sequences. Two of these sequences are very similar, and functionally equivalent. We dubbed these two sequences **A and B**. The third sequence was named sequence **C**. Stuxnet determines if the system is the intended target by fingerprinting it. It checks:
  - The PLC type/family: only CPUs 6ES7-417 and 6ES7-315-2 are infected
  - The System Data Blocks: the SDBs will be parsed, and depending on the values they contain, the infection process will start with method of infection A, B or none. When parsing the SDBs the code searches for the presence of 2 values (7050h and 9500h), and depending on the number of occurrences of each of these values sequence A or B is used to infect the PLC.
  - The code also searches for the bytes 2C CB 00 01 at offset 50h in the SDB blocks, which appear if the CP 342-5 communications processor (used for Profibus-DP) is present. If these bytes are not found then infection does not occur.
  - Infection conditions for sequence C are determined by other factors.



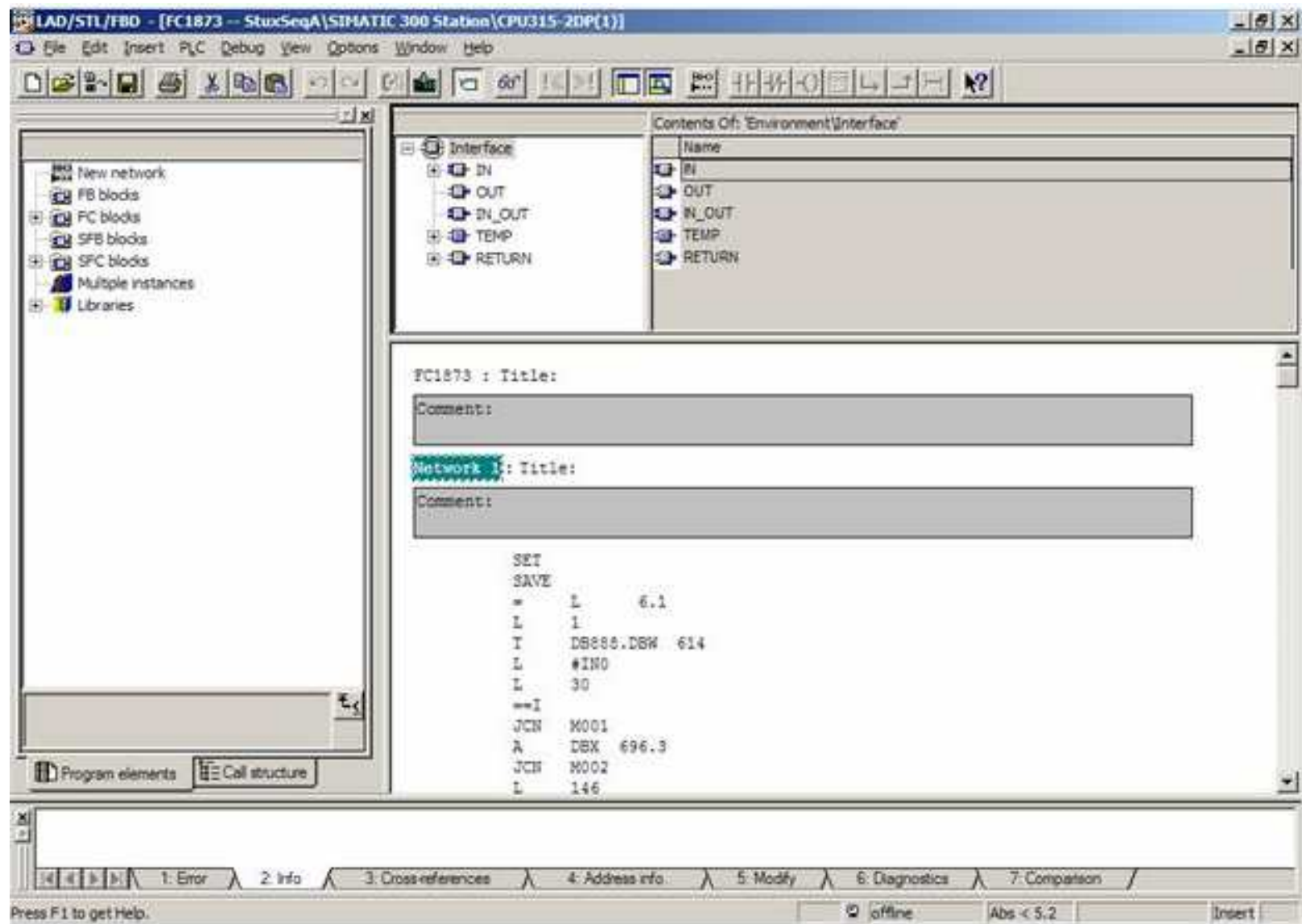
# Interesting

[http://blogs.cisco.com/security/comments/stuxnet\\_exploiting\\_trust\\_relationships\\_and\\_expected\\_behavior/](http://blogs.cisco.com/security/comments/stuxnet_exploiting_trust_relationships_and_expected_behavior/)

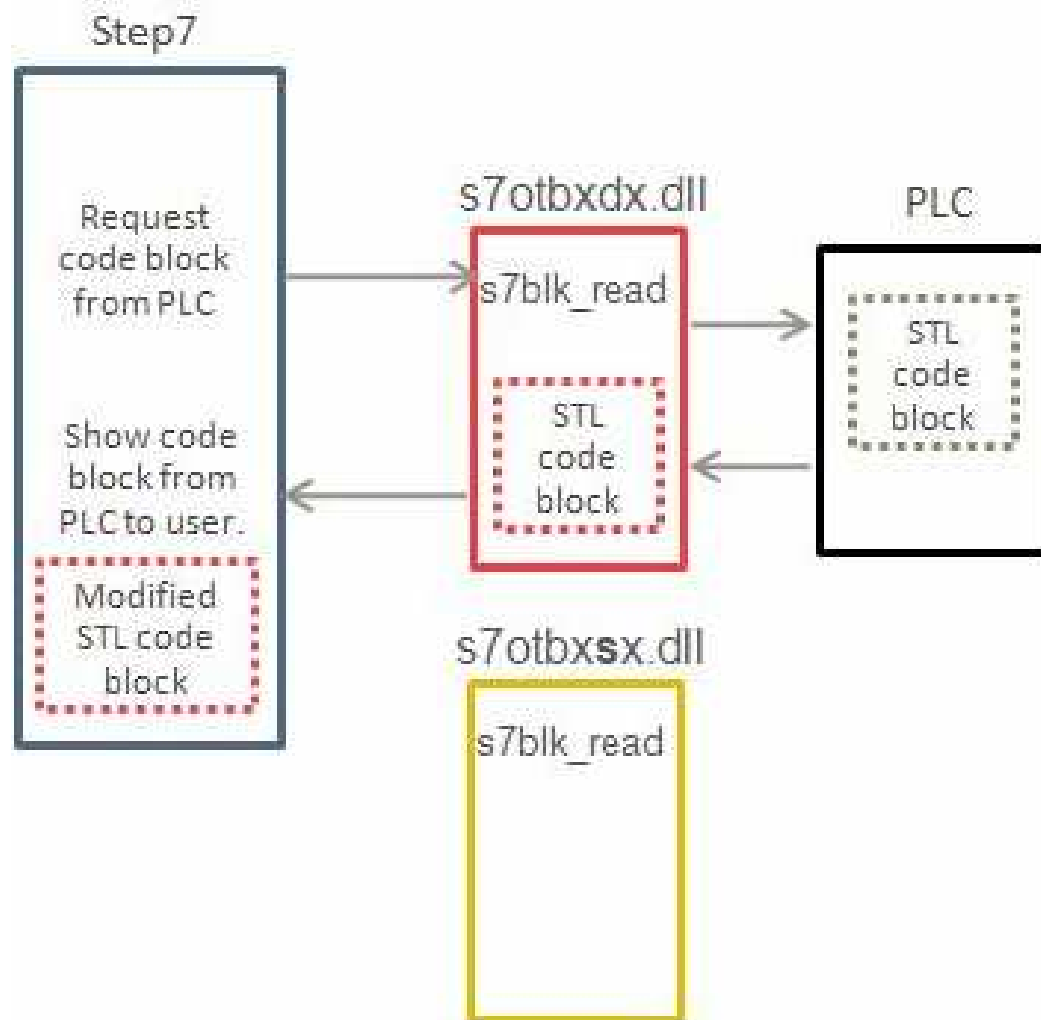
- Further complicating things, the Stuxnet malware relies in part upon a hard-coded authentication in Siemens database backends. These [default credentials must remain in place](#), according to Siemens officials, or else the SCADA systems will not interoperate. Unfortunately, those same credentials provide operating system access and can be a conduit for malware or other intrusions.

- <http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process>
- To access a PLC, specific software needs to be installed; Stuxnet specifically targets the WinCC/Step 7 software used for programming particular models of PLC.



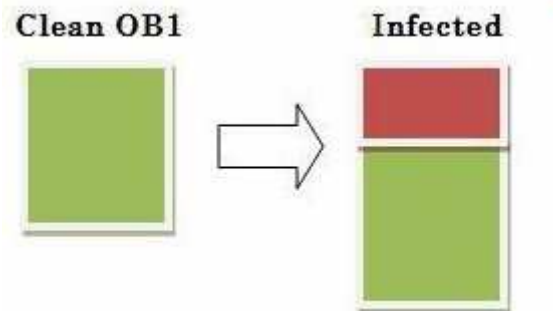


# How PLC is reprogrammed with stuxnet



Stuxnet uses the code-prepend infection technique. When Stuxnet infects OB1 it performs the following sequence of actions:

- Increases the size of the original block
- Writes malicious code to the beginning of the block
- Inserts the original OB1 code after the malicious code



# Infection

As well as infecting OB1, Stuxnet also infects OB35 in a similar fashion. It also replaces the standard coprocessor DP\_RECV code block with its own, thereby hooking network communications on the Profibus (a standard industrial network bus used for distributed I/O).

- The overall process of infection for methods A/B is as follows:
- Check the PLC type; it must be an S7/315-2
- Check the SDB blocks and determine whether sequence A or B should be written
- Find DP\_RECV, copy it to FC1869, replace it with a malicious copy embedded in Stuxnet
- Write the malicious blocks (in total, 20 blocks) of the sequence, embedded in Stuxnet
- Infect OB1 so that the malicious code is executed at the start of a cycle
- Infect OB35, which will act as a watchdog

- Stuxnet is fingerprinting its target by checking data block 890.
- This occurs periodically every five seconds out of the WinCC environment.
- Based on the conditional check in code that you can see above, information in DB 890 is manipulated by Stuxnet.

# The real-time part of the PLC is attacked

Stuxnet Step7 code injected into OB 35 (100 ms timer)



```
UC FC1874
```

every 100 ms, FC 1874 is called

```
POP
```

```
L DW#16#DEADF007
```

if the return code from FC 1874 is "DEADF007", original code is skipped (BEC = block end conditional)

```
==D
```

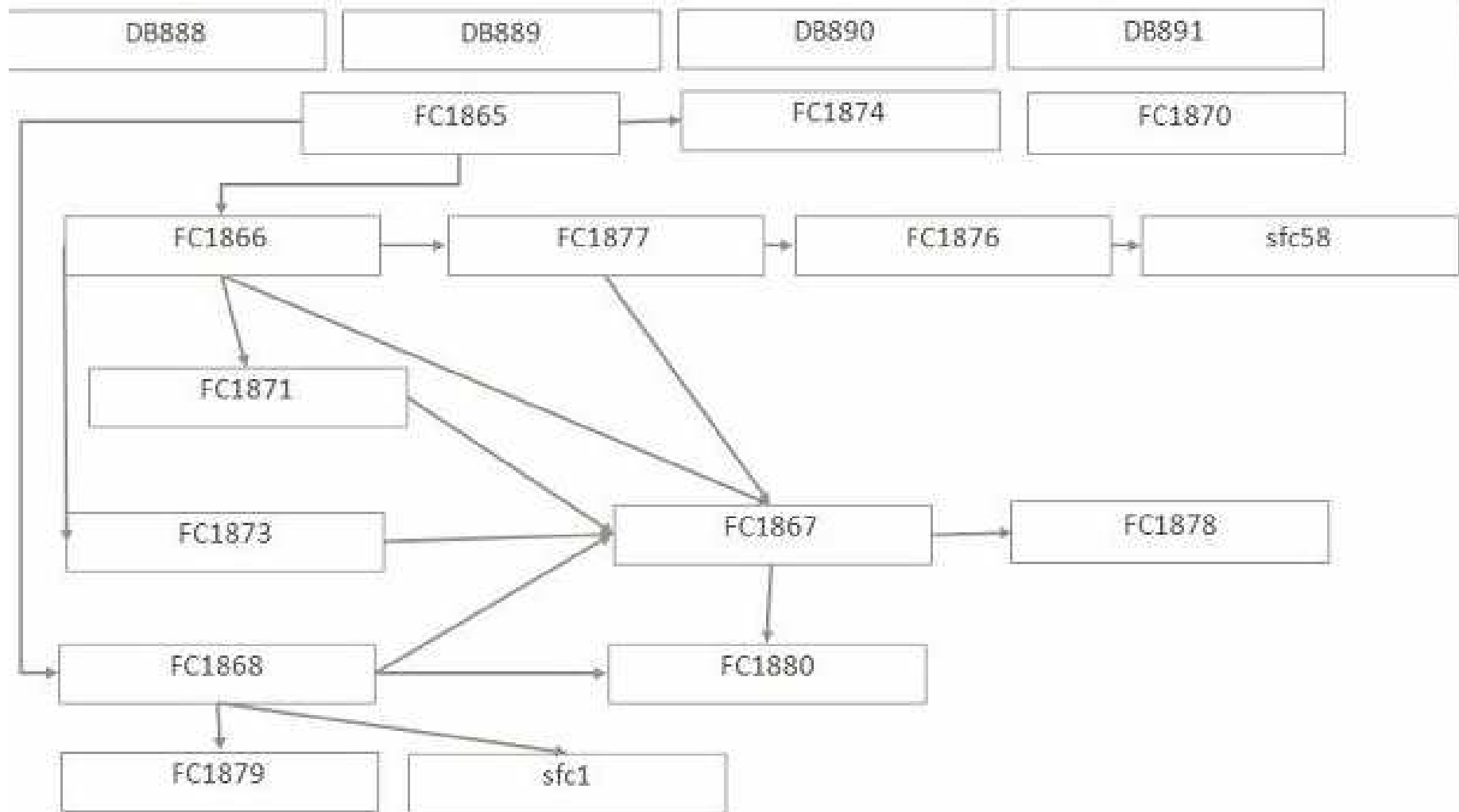
```
BEC
```

```
L DW#16#0
```

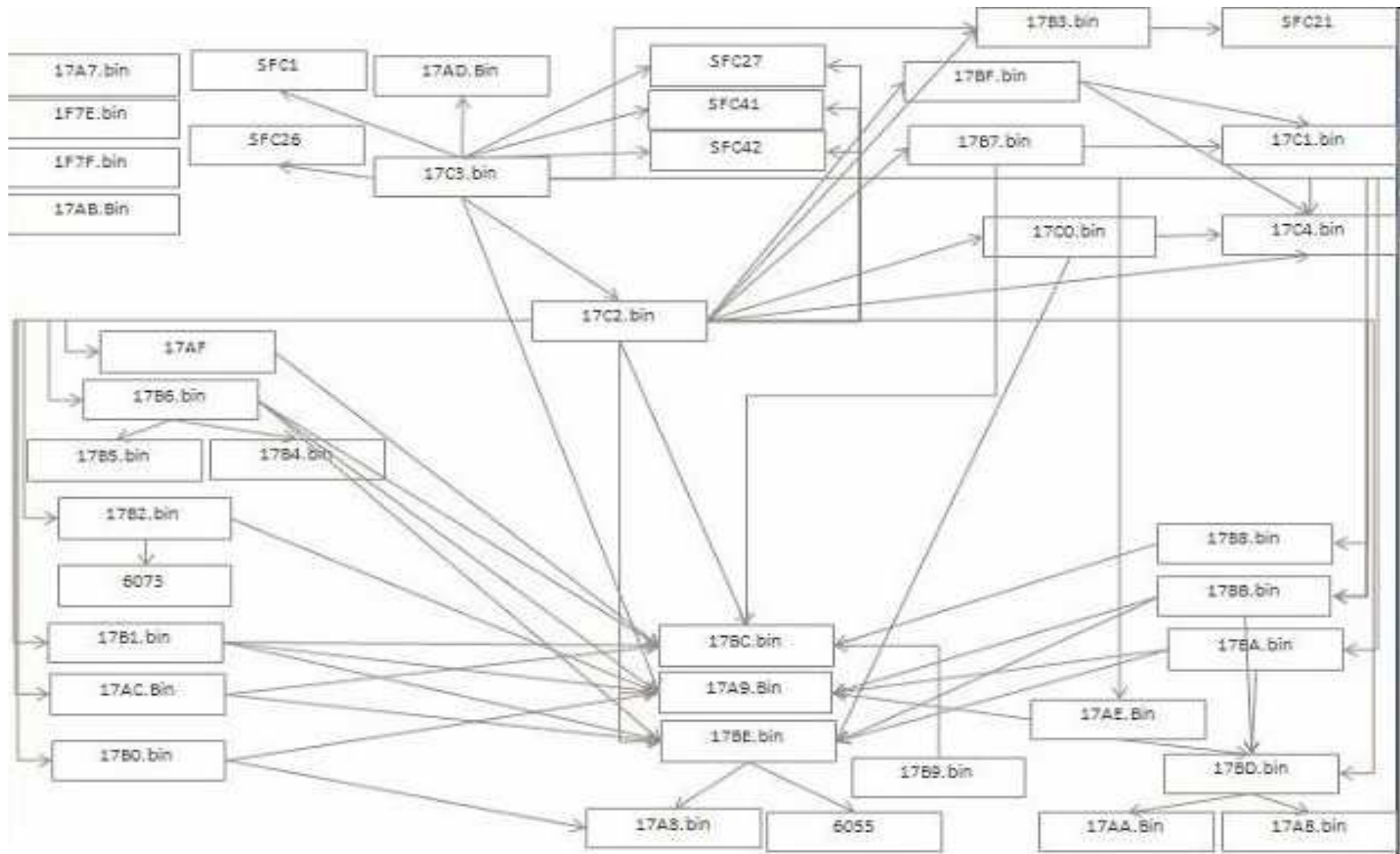
if the return code from FC 1874 does not match, Stuxnet hides the injection by clearing the accumulator register

```
L DW#16#0
```

## Program A & B

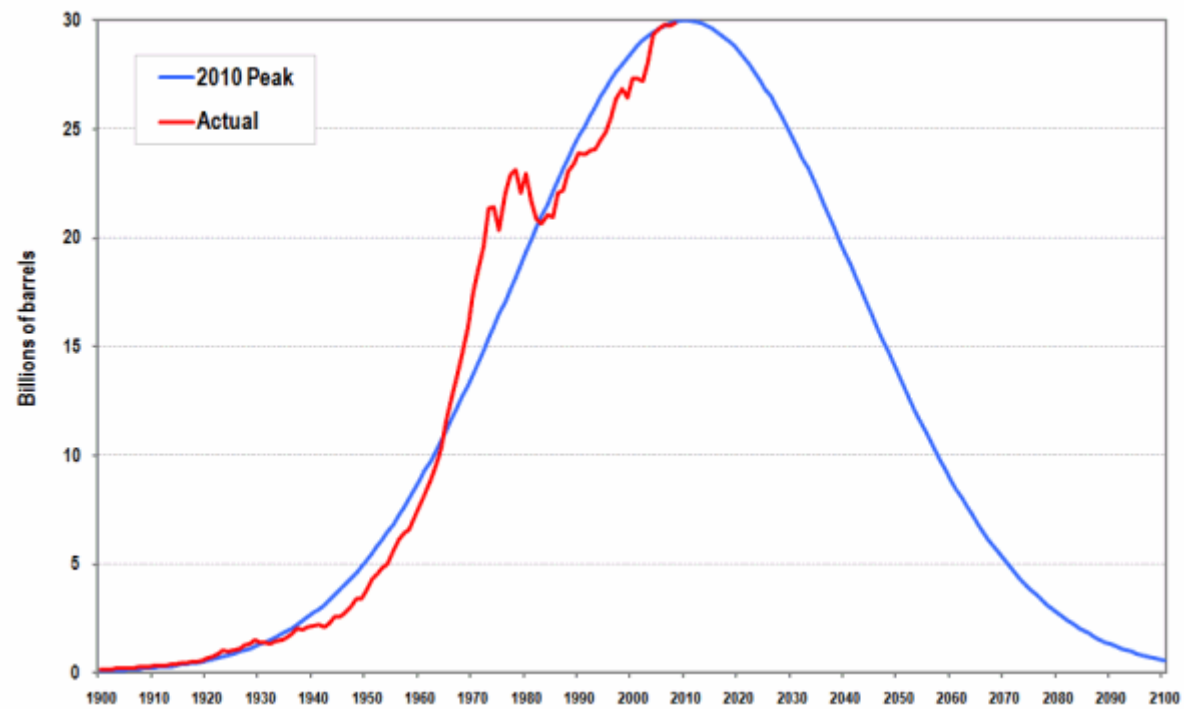


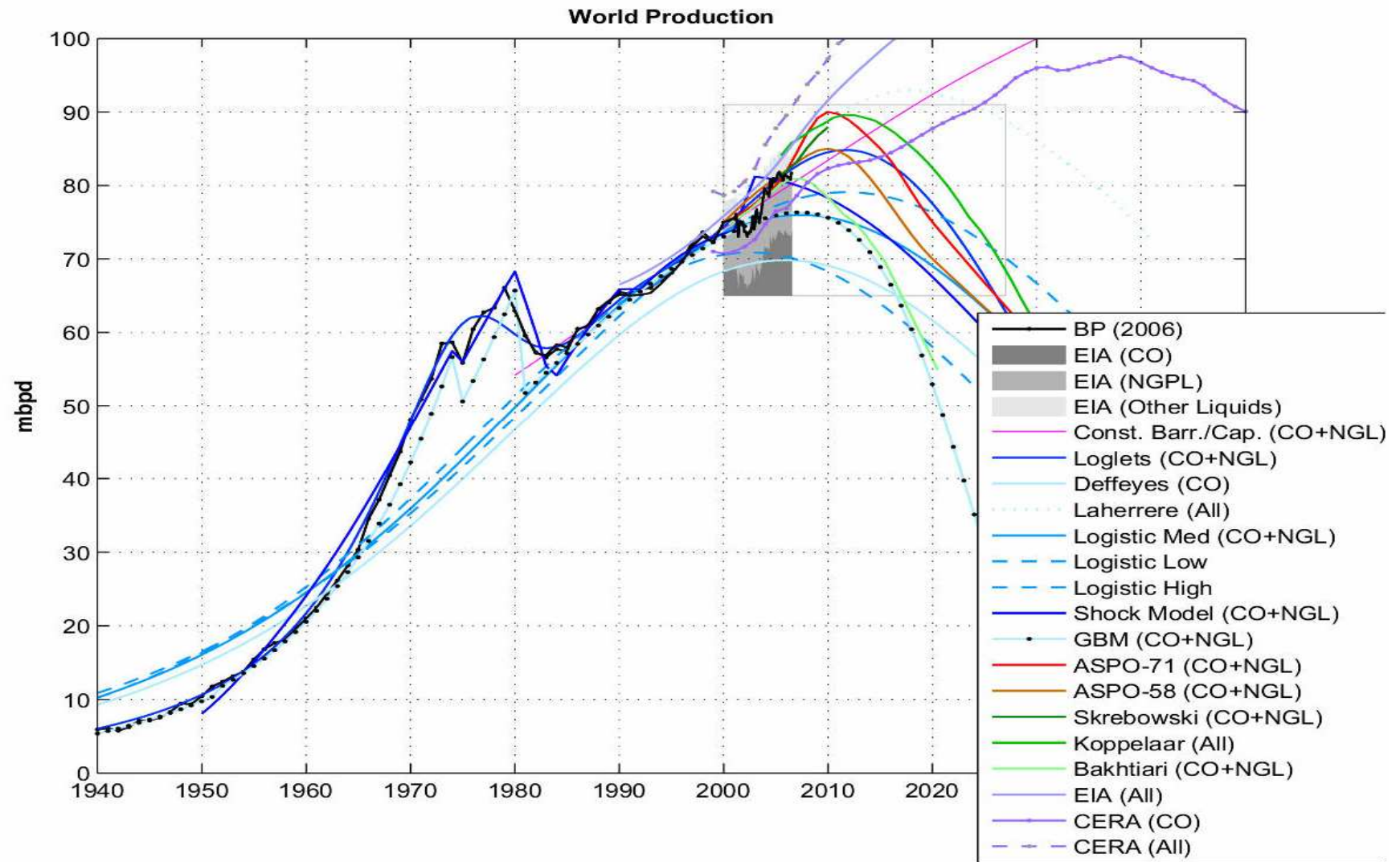
# Sequence C



# Why is Iran so important?

- Oil
- Nuclear weapons





# World Oil Depletion Per Major Producer

Reserves: 1,250B; Depletion: 23.3B/year; Source: 'National Geographic' 6/2004

