



Stuxnet - Infecting Industrial Control Systems

Liam O Murchu

Operations Manager, Symantec Security Response

Sep 2010

Agenda

- 1 60 second Intro to PLCs
- 2 Programming a PLC
- 3 How Stuxnet infects
- 4 What Stuxnet does
- 5 Demonstration

PLCs

Programmable Logic Controller

- Monitors Input and Output lines
 - Sensors on input
 - switches/equipment on outputs
 - Many different vendors
- Stuxnet seeks specific Models
 - s7-300 s7-400

Stuxnet is Targeted

Targeting a Specific type of PLC

Searches for a Specific Configuration



Hardware configuration

System Data Blocks

- Each PLC must be configured before use.
- Configuration is stored in **System Data Blocks (SDBs)**
- Stuxnet parses these blocks
- Looks for magic bytes **2C CB 00 01** at offset **50h**
- Signifies a Profibus network card attached - CP 342-5
- Looks for **7050h** and **9500h**
- Must have more than **33** of these values
- Injects different code based on number of occurrences

How Stuxnet Infects PLCs

Programming a PLC

Step7, STL and MC7

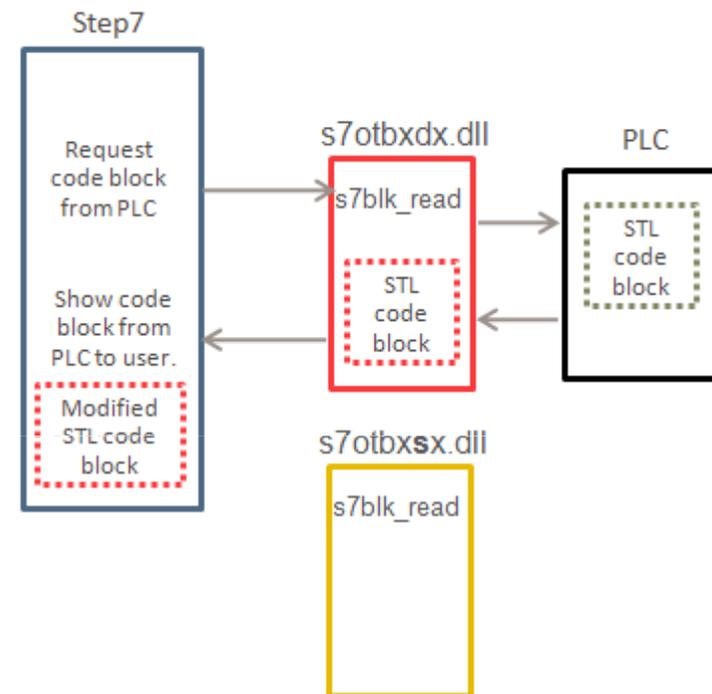


- Simatic or Step 7 software
 - Used to write code in STL or other languages
- STL code is compiled to **MC7 byte code**
- MC7 byte code is transferred to the PLC
- Control PC can now be disconnected

Stuxnet: Man in the Middle attack on PLCs

“Man in the App” attack

- Step7 uses a library to access the PLC
 - S7otbxdx.dll
- Stuxnet replaces that dll with its own version
- Stuxnet’s version intercepts reads and writes to the PLC and changes the code at this point.



Stuxnet MC7 Byte code

- Stuxnet contains at least 70 binary blobs of data
- They are encoded and stored in the fake dll
- These are actually blocks of MC7 byte code
- This is the code that is injected onto the PLCs
- Must be converted back to STL to understand it
- Difficult task but we have now converted all the MC7 byte code to **readable STL code**
- **Just unsure of real world effects of this code.**

OB1 and OB35

Stuxnet changes these blocks

- OB1 = main() on PLCs
 - Stuxnet inserts its own code at the beginning of OB1 so it runs first.
- OB35 is a 100ms interrupt routine
 - Used to monitor inputs that would require fast action
 - Stuxnet infects OB35 too
- Stuxnet will return clean versions of these functions when they are read from the PLC.

Demo

Show Infection of a PLC

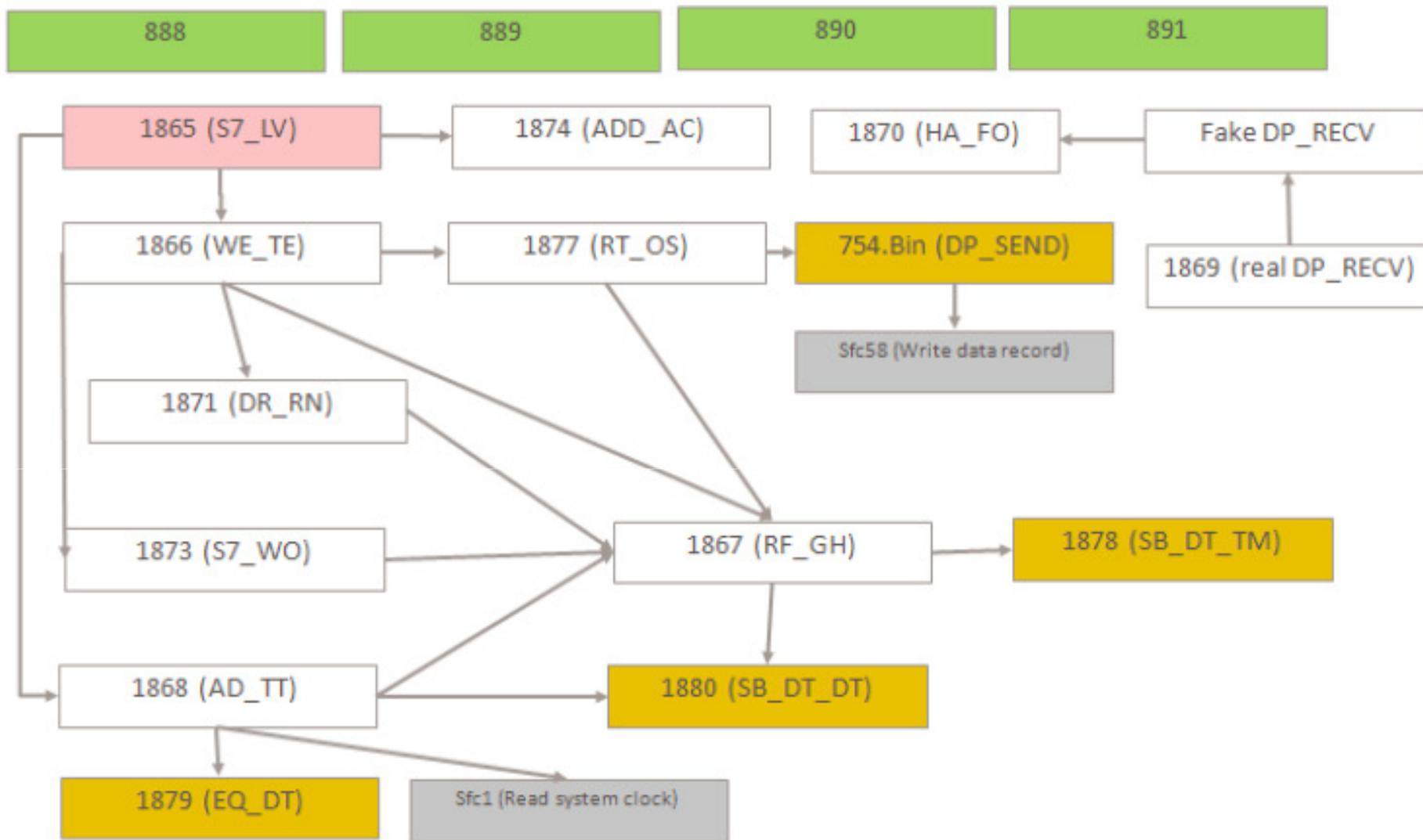
- Inflate a balloon for 5 seconds
- Infect the PLC
- Inflate balloon again for 5 seconds

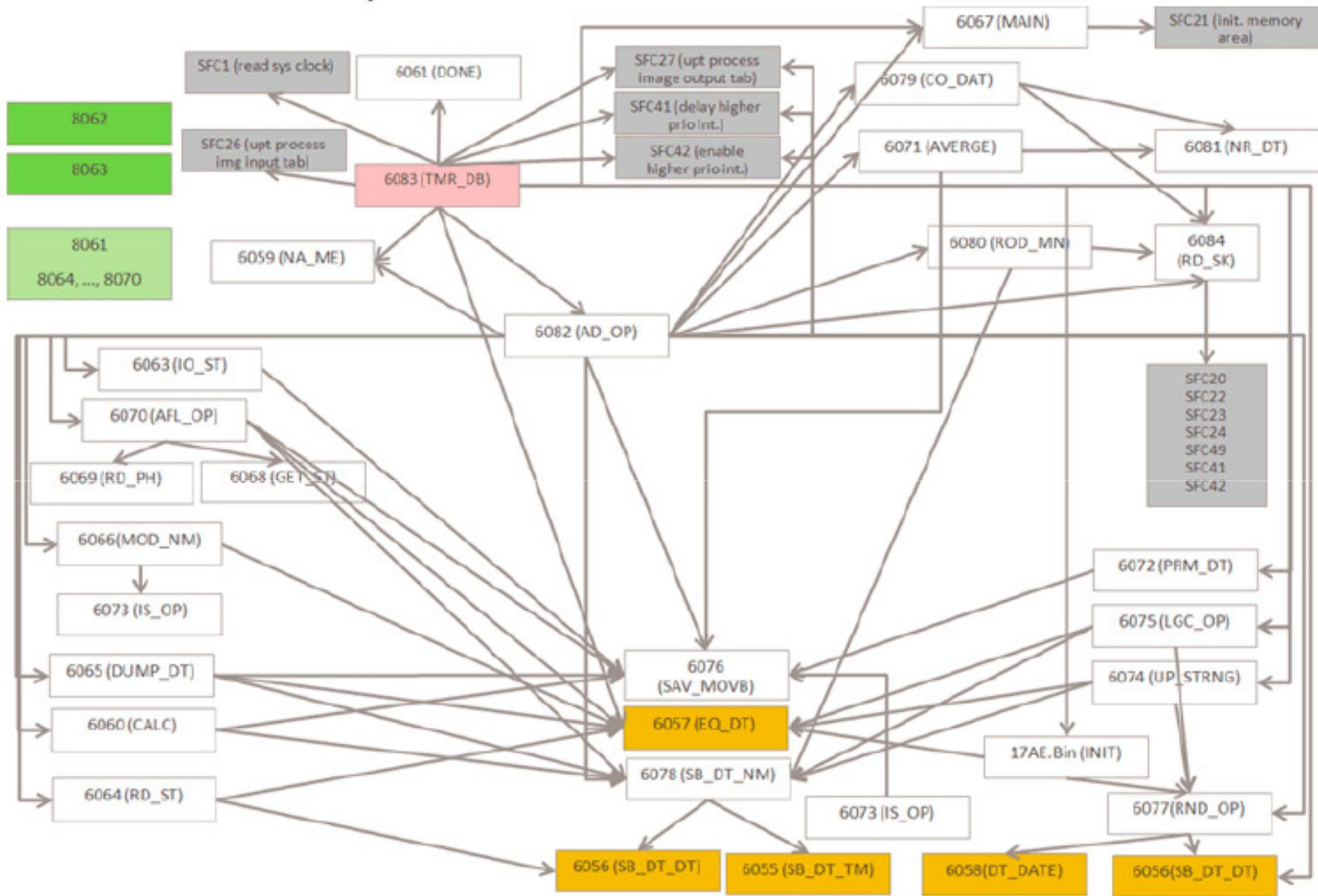
Stuxnet's PLC code

Complex and large amount of code

- Demo was just 8 lines of code.
- Stuxnet contains hundreds of lines of code
- It is difficult to understand the real world actions without knowing what is connected on the inputs and outputs.

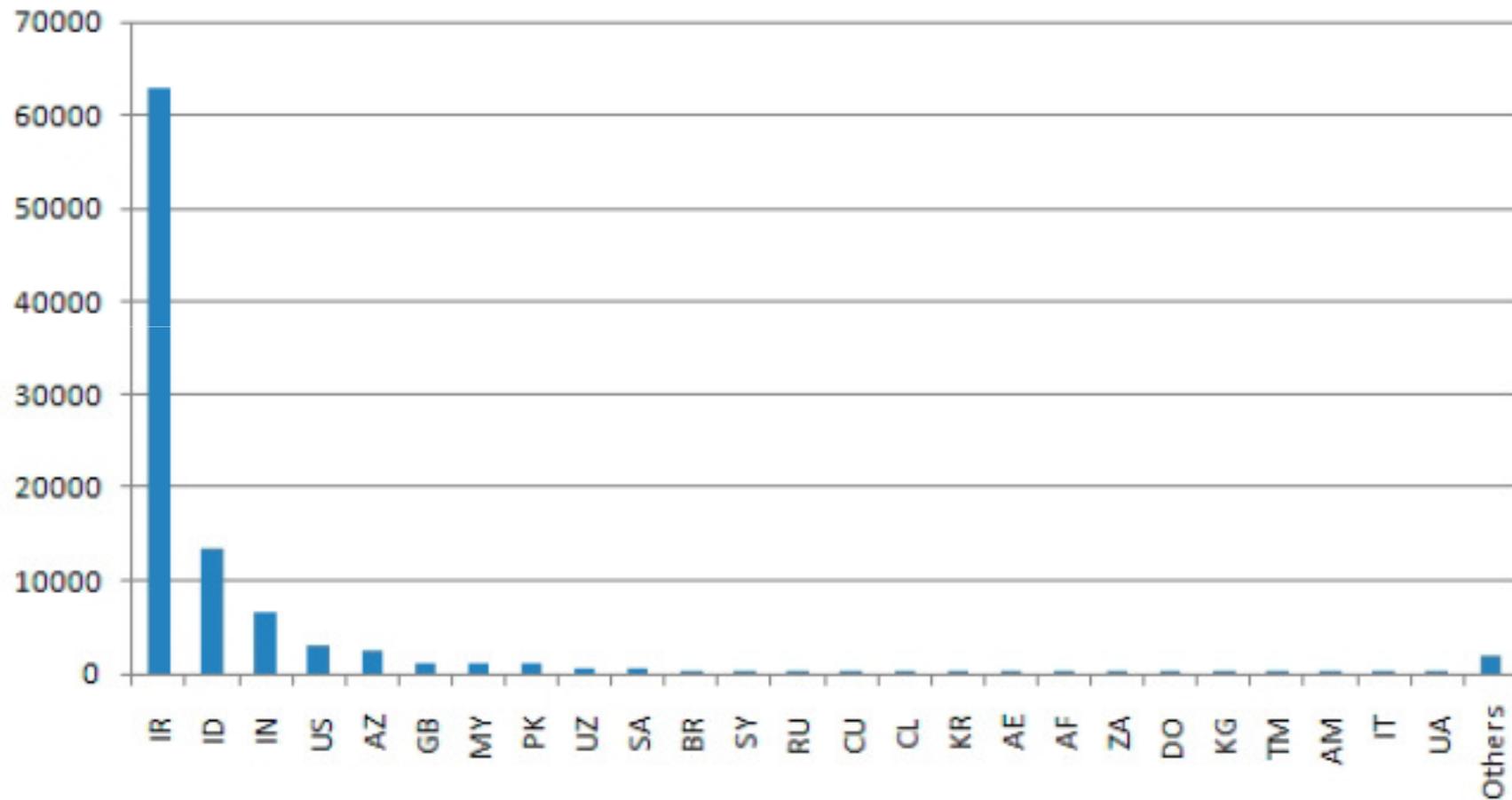
```
UC FC 1865;  
POP ;  
L DW#16#DEADF007;  
==D ;  
BEC ;  
L DW#16#0;  
L DW#16#0;
```





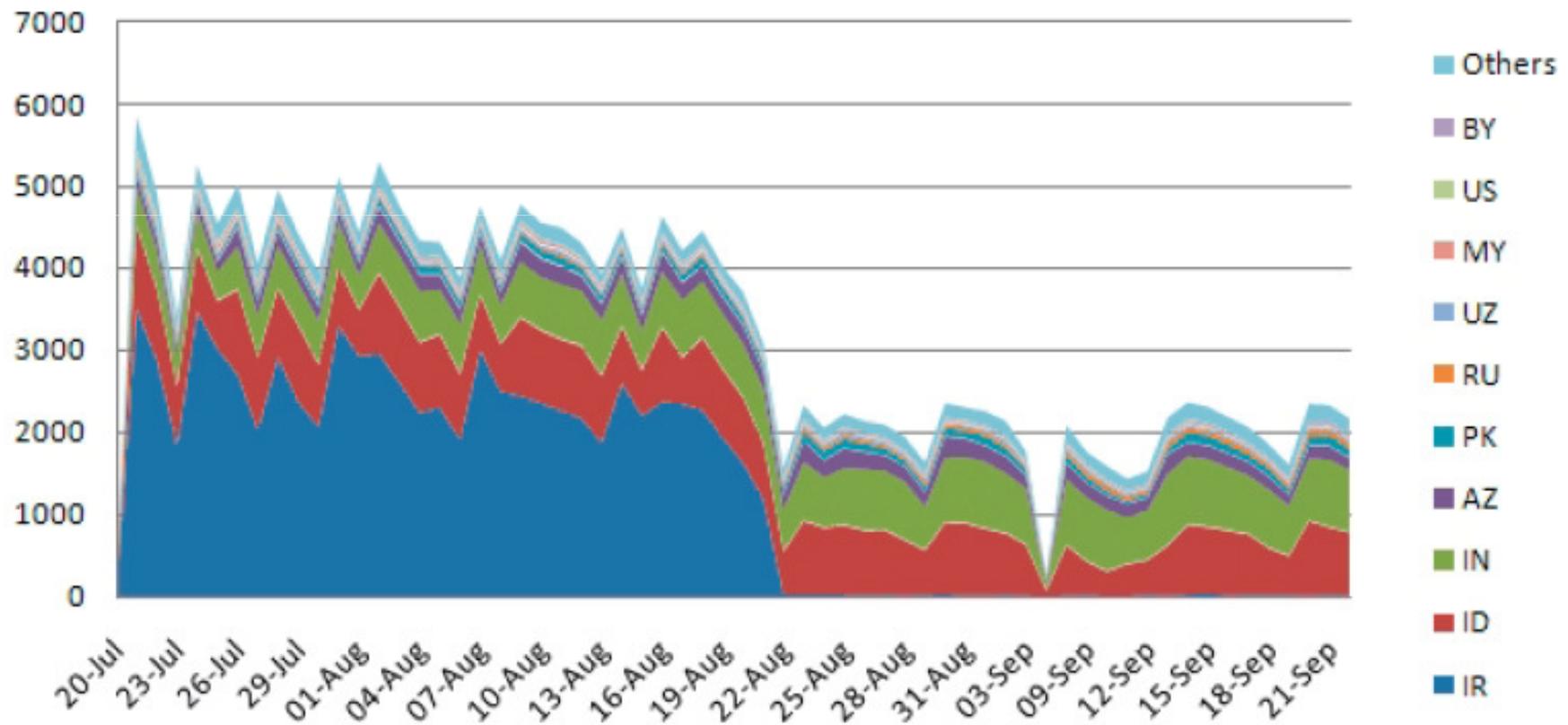
Targets

Stats for Command and Control Servers



Stuxnet Infections

Figure 5
Rate of Stuxnet infection of new IPs by Country



White Paper Available

W32.Stuxnet Dossier

- Stuxnet Technical Details Available here:
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



Thank you!

Liam O Murchu - liam_omurchu@symantec.com

Nicolas Falliere

Eric Chien

Threat Intelligence Team

All Stuxnet Reverse Engineers

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.