{TechForum
/eXplore/
“year”:2015}

STUXNET – How did it spread ?

21

apogeewallpapers.com

- Used 4 exploits
  - .LNK to execute code from USB sticks
  - In keyboard driver → elevated privs
  - In task scheduler → elevated privs
  - In print spooler to spread on LAN

- Upgrade mechanism

- Connected to Command & Control Servers

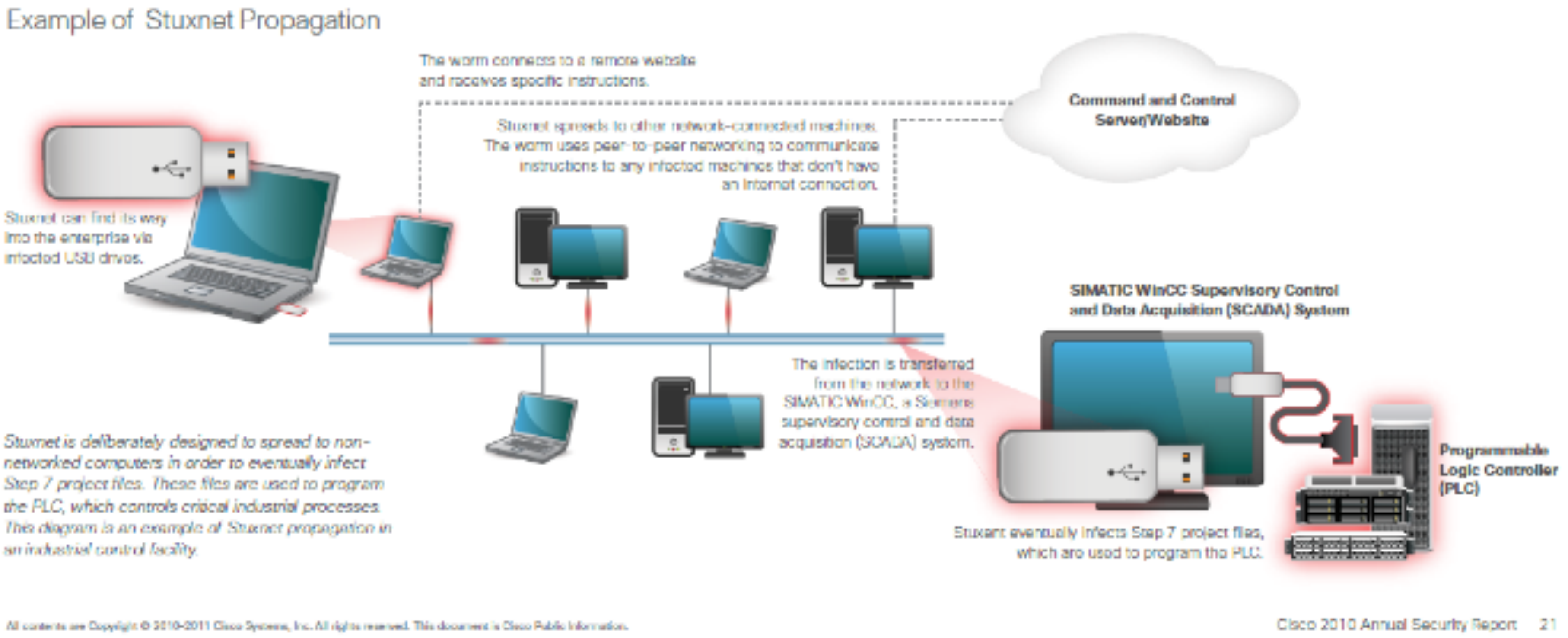
STUXNET – How did it spread ?

- Used 4 exploits
  - .LNK to execute code from USB sticks
  - In keyboard driver → elevated privs
  - In task scheduler → elevated privs
  - In print spooler to spread on LAN

- Upgrade mechanism

- Connected to Command & Control Servers

STUXNET – How did it spread ?


Command and Control
Server/Website
SIMATIC WinCC Supervisory Control
and Data Acquisition (SCADA) System
Programmable
Logic Controller
(PLC)

Example of Stuxnet Propagation

The worm connects to a remote website and receives specific instructions.

Stuxnet spreads to other network-connected machines. The worm uses peer-to-peer networking to communicate instructions to any infected machines that don't have an Internet connection.

Stuxnet can find its way into the enterprise via infected USB drives.

The infection is transferred from the network to the SIMATIC WinCC, a Siemens supervisory control and data acquisition (SCADA) system.

Stuxnet eventually infects Step 7 project files, which are used to program the PLC.

Stuxnet is deliberately designed to spread to non-networked computers in order to eventually infect Step 7 project files. These files are used to program the PLC, which controls critical industrial processes. This diagram is an example of Stuxnet propagation in an industrial control facility.

All contents are Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco 2010 Annual Security Report 21