清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒

——原理、技术和实践

蠕虫

刘功申

上海交通大学网络空间安全学院

2019.03.13

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

本章目标

- 掌握蠕虫的概念
- 掌握蠕虫的发展过程
- 熟悉蠕虫的编制

蠕虫的最大贡献

蠕虫更像是一种传播方式！

蠕虫的基本概念

- 蠕虫（Worm）是恶意代码的一种，它的传播通常不需要所谓的激活。它通过分布式媒介进行图传播。
- 分布式媒介包括：网络、服务、人工等
- 蠕虫强调的是图传播方式（参考本教材第2章的传播模型）。

蠕虫历史

- 蠕虫这个名词的由来是在1982年，Shock和Hupp根据《The Shockwave Rider》一书中的概念提出了一种“蠕虫（Worm）”程序的思想。
- 2003-2005年蠕虫发展的高峰期
- 2010后，蠕虫的传播能力被用在工业控制等新型恶意代码中。
- 2015年后，蠕虫的传播能力被用在勒索软件型恶意代码中。

与传统病毒的联系

- 具有病毒共性：如传播性、隐蔽性、破坏性等
- 独有的性质：不利用文件寄生，对网络造成拒绝服务，以及和黑客技术相结合等

- 蠕虫和传统病毒的区别：

比较项目	传统病毒	蠕虫
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染对象	本地文件	网络计算机

蠕虫的分类

- 一种是面向企业用户和局域网而言，这种病毒利用系统漏洞，主动进行攻击，可以对整个互联网可造成瘫痪性的后果。以“红色代码”、“尼姆达”以及最新的“SQL蠕虫王”为代表。
- 另外一种是针对个人用户的，通过网络（主要是电子邮件、恶意网页形式）迅速传播的蠕虫病毒，以爱虫病毒、求职信病毒为代表。

蠕虫的特征

- 第一，利用漏洞主动进行攻击
- 第二，与黑客技术相结合
- 第三，传染方式多
- 第四，传播速度快
- 第五，清除难度大
- 第六，破坏性强

蠕虫病毒的机理

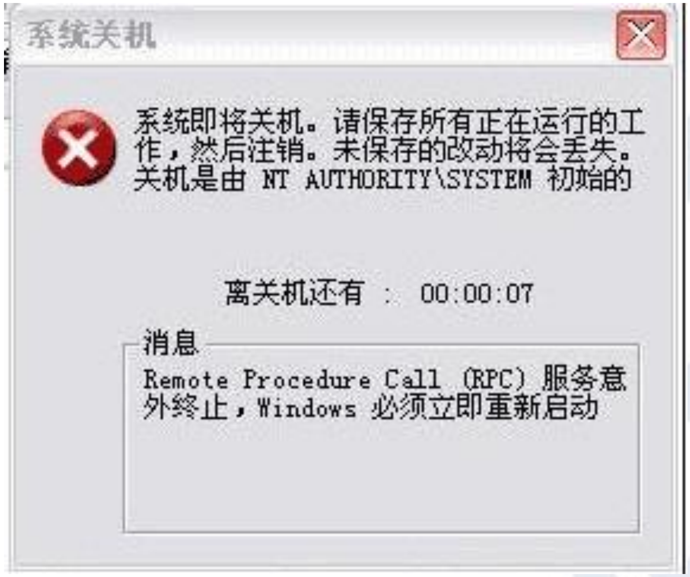
- 蠕虫病毒由两部分组成：一个主程序和另一个是引导程序。
  - 主程序收集与当前机器联网的其他机器的信息。利用漏洞在远程机上建立引导程序。
  - 引导程序把“蠕虫”病毒带入了它所感染的每一台机器中。
- 当前流行的病毒主要采用一些已公开漏洞、脚本、电子邮件等机制进行传播。例如，IRC, RPC 等漏洞。

蠕虫病毒实例 - 基于RPC漏洞蠕虫

- RPC漏洞
  - 远程过程调用 (RPC)是 Windows 操作系统使用的一个协议，提供了一种进程间通信机制
  - RPC 中处理通过 TCP/IP 的消息交换的部分存在一个漏洞。此问题是由错误地处理格式不正确的消息造成的。
  - RPC漏洞影响分布式组件对象模型 (DCOM) 与 RPC 间的一个接口，此接口侦听 TCP/IP 端口 135。
  - Samba等程序存在此类漏洞

基于RPC漏洞蠕虫

- 冲击波病毒
  - 2003年7月16日，微软公司发布了“RPC 接口中的缓冲区溢出”的漏洞补丁，攻击者即制作了一个利用此漏洞的蠕虫



系统关机

系统即将关机。请保存所有正在运行的工作，然后注销。未保存的改动将会丢失。关机是由 NT AUTHORITY\SYSTEM 初始的

离关机还有 ： 00:00:07

消息

Remote Procedure Call (RPC) 服务意外终止，Windows 必须立即重新启动

冲击波的中毒症状

震网病毒

https://www.bilibili.com/video/av5812131/

震网（Stuxnet）是一种Windows平台上的计算机蠕虫，该蠕虫病毒已感染并破坏了伊朗的核设施，使伊朗的布什尔核电站推迟启动。

Stuxnet蠕虫病毒是世界上首个专门针对工业控制系统编写的破坏性病毒，能够利用对windows系统和西门子SIMATIC WinCC系统的7个漏洞进行攻击。特别是针对西门子公司的SIMATIC WinCC监控与数据采集 (SCADA) 系统进行攻击，由于该系统在我国的多个重要行业应用广泛，被用来进行钢铁、电力、能源、化工等重要行业的人机交互与监控。

Outline

- What is Stuxnet?
- How was it detected?
- How does it penetrate a network?
- How does it propagate itself?
- How is it controlled / updated?
- How has it evolved?
- How big is the problem (who is at risk)?

What is Stuxnet?

- Stuxnet is an Advanced Persistent Threat (APT) that was targeted at a specific manufacturing facility. (Named for a string of letters buried in its code)
- It is (was at the time of its discovery) the most complicated virus / worm ever discovered.
- Average viruses are about 10k bytes in size. Stuxnet was 500 KB (and no graphics).
- It is unusual for a virus to contain one zero-day vulnerability. Stuxnet had 4.
- Stuxnet also acted like a rootkit – hiding its actions and its presence.
- It was the first virus to include code to attack Supervisory Control and Data Acquisition (SCADA) systems.

How it was detected

- Discovered by Sergey Ulasen in June, 2010, at the time working for a small Belarus anti-virus company (VirusBlokAda)
- One of their customers in Iran had been experiencing a number of BSOD failures and wanted help finding the cause.
- Research into that problem led to the discovery of the virus.

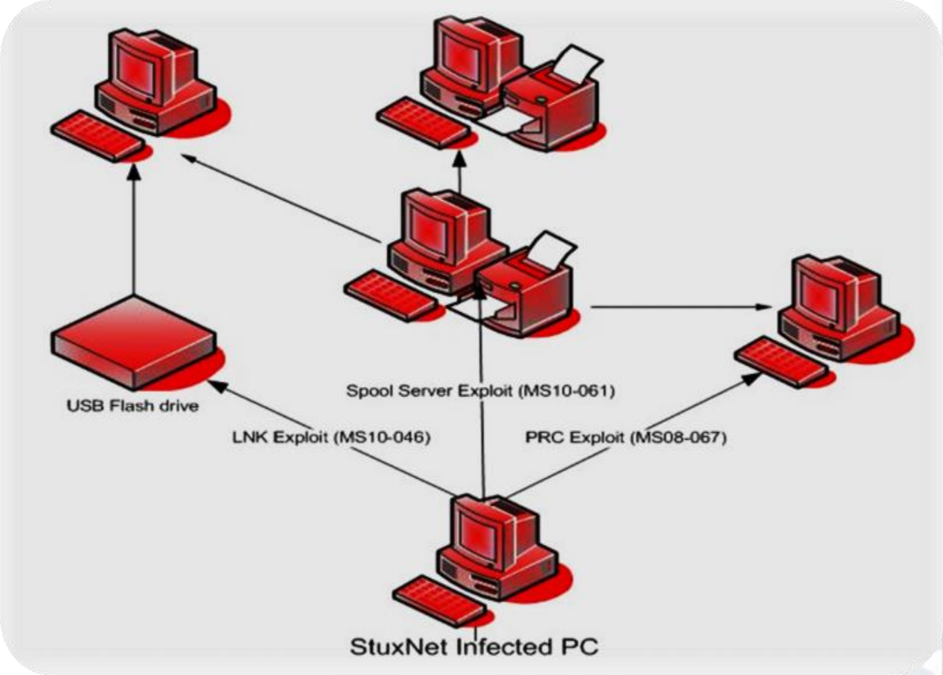
W32.Stuxnet Timeline

November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it’s using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for “Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)” that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.

July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

How does it penetrate a network?

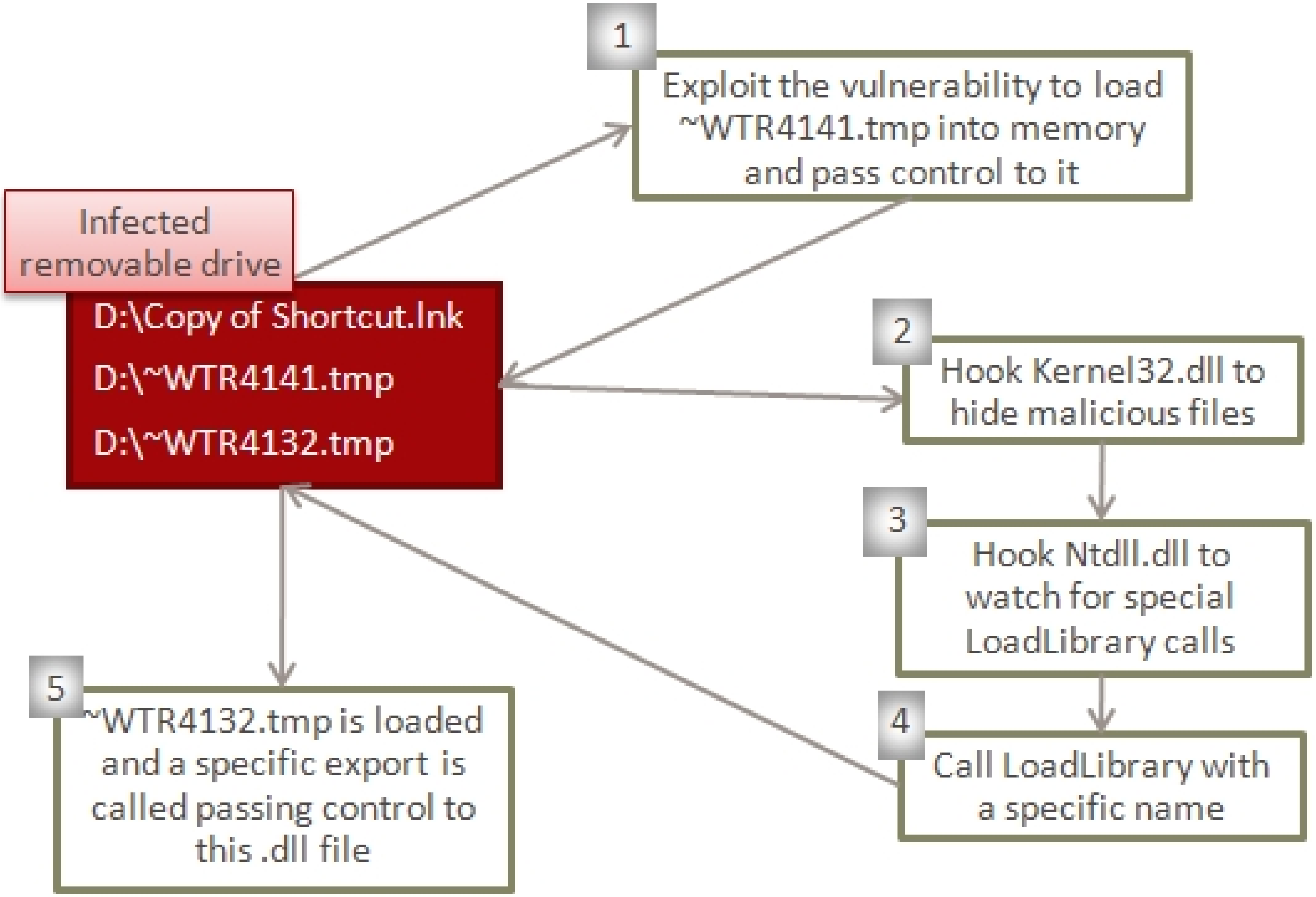
- Target environment was expected to be an air-gapped network (more later).
- Spread through flash drives. *.lnk file on flash drive
- No memory corruption, 100% reliable
- Once virus is uploaded and running, it hides the .lnk and source files.
- Patched in MS10-046



.LNK 0 Day Attack

- Removable drive contains:
  - 2 tmp files: file names variable (∑ mod 10 = 0)
    - ~WT4132.tmp – main DLL ~500KB
    - ~WT4141.tmp – loader for main dll ~25KB
  - 4 .lnk files:
    - Multiple links needed to attack different versions of Windows (W2k, WXP, Serv2003, Vista, W7)
- Removable drive only infects a max of 3 hosts, and then erases itself.
- Host only infects a new removable drive if:
  - Drive is not already infected
  - Infection is less than 21 day sold
  - Drive has more than 5 MB of free space
  - Drive has more than 3 files on it.

.lnk infection strategy



Infected removable drive

D:\Copy of Shortcut.lnk

D:\~WTR4141.tmp

D:\~WTR4132.tmp

1 Exploit the vulnerability to load ~WTR4141.tmp into memory and pass control to it

2 Hook Kernel32.dll to hide malicious files

3 Hook Ntdll.dll to watch for special LoadLibrary calls

4 Call LoadLibrary with a specific name

5 ~WTR4132.tmp is loaded and a specific export is called passing control to this .dll file

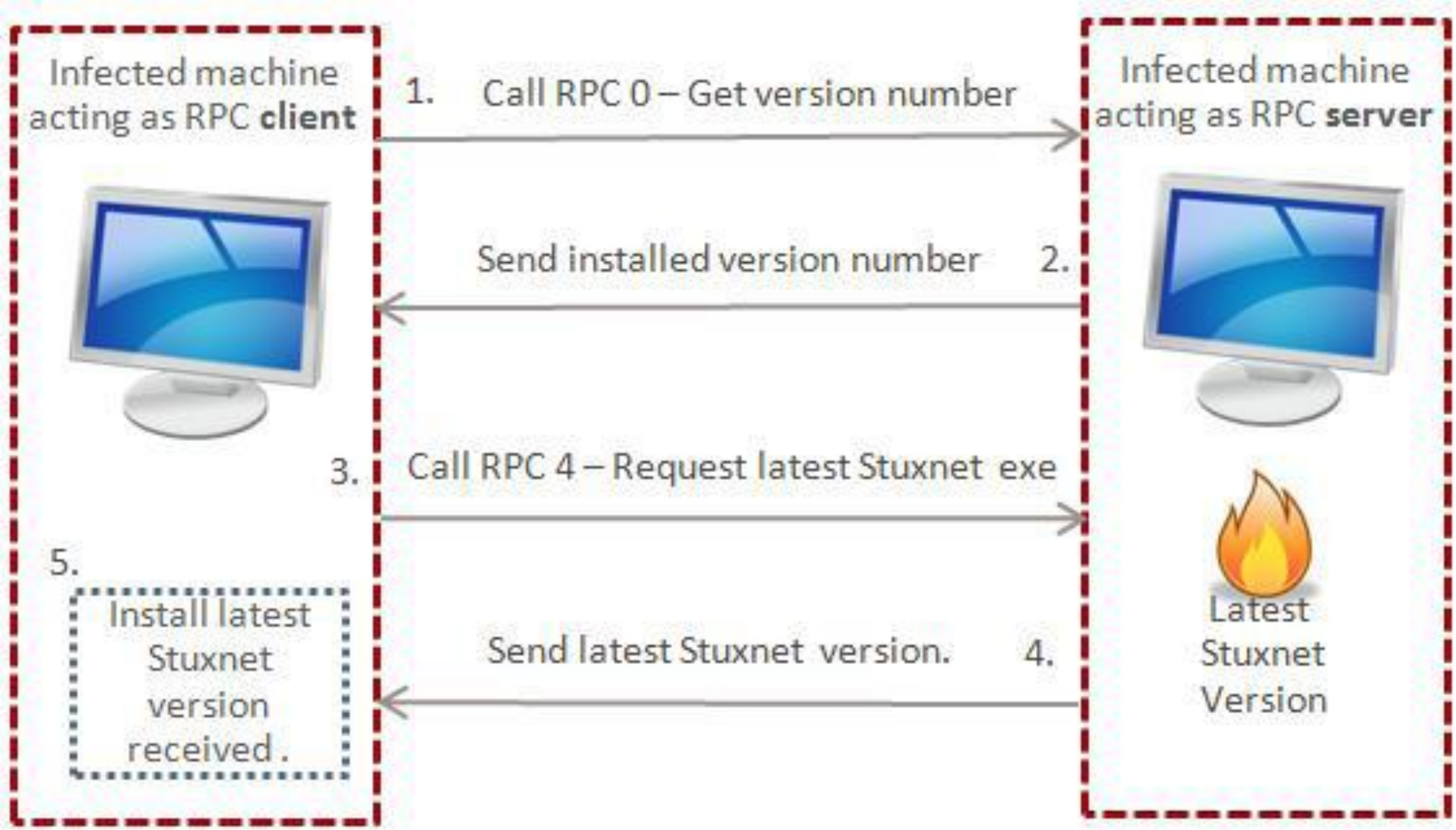
How does it propagate itself? (Overview)

- Carried by flash drive
- Copies to open file shares
- Passed through vulnerable print spooler code (zero-day vulnerability – MS 10-061)
- Passed the RPC vulnerability found in Conficker (MS-08-067)
- Create a vulnerable scheduled task, then modify the task and pad until its CRC32 matches original task. (Will now run under scheduler.) Creates rootkit for Vista+
- Allows users to load different keyboard layouts. Can be loaded from anywhere. Load pointers and then transfer to code. Creates rootkit for Windows XP.

Propagate through P2P

- Use RPC
  - Some of the machines expected to be network isolated, but might have access to infected machines.
- Searches through a set of 5 programs that might be infected (depending on OS version, vulnerabilities, etc.)
- Each infected machine searches for other infected machines (with RPC servers).
  - Query for current virus version. If server has older version, send update.
  - If server has newer version, download update.

P2P update process



Infected machine acting as RPC **client**

Infected machine acting as RPC **server**

1. Call RPC 0 – Get version number

2. Send installed version number

3. Call RPC 4 – Request latest Stuxnet exe

4. Send latest Stuxnet version.

5. Install latest Stuxnet version received.

Latest Stuxnet Version

Siemens Wincc program

- Visualization program to support design and development of supervisory control and data acquisition (SCADA) programs
- Includes database to store projects. Database includes a hardcoded password – backdoor into the system.
- Virus modifies a WinCC view to start virus exe each time view is accessed.
- Virus writes itself into a new table, then creates a stored procedure that extracts and executes code, then deletes stored procedure

Network Shares

- Searches through all user accounts and all shared drives to find access to remote machine.
- If none found, will try Windows Management Instrumentation (WMI) to access shares and download a copy of the virus.

Print Spooler 0-day Attack

- Virus uses a weakness in print spooler on shared machines to propagate an executable file.
- File (%system%\winsta.exe) can be loaded to any machine that uses print spooler.
- Only used if date is before 6/1/2011). Expect the vulnerability to be fixed by then??
- Vulnerability had been published in 2009 edition of Hakin9 magazine – but not patched by Microsoft.
- Patched in MS10-061

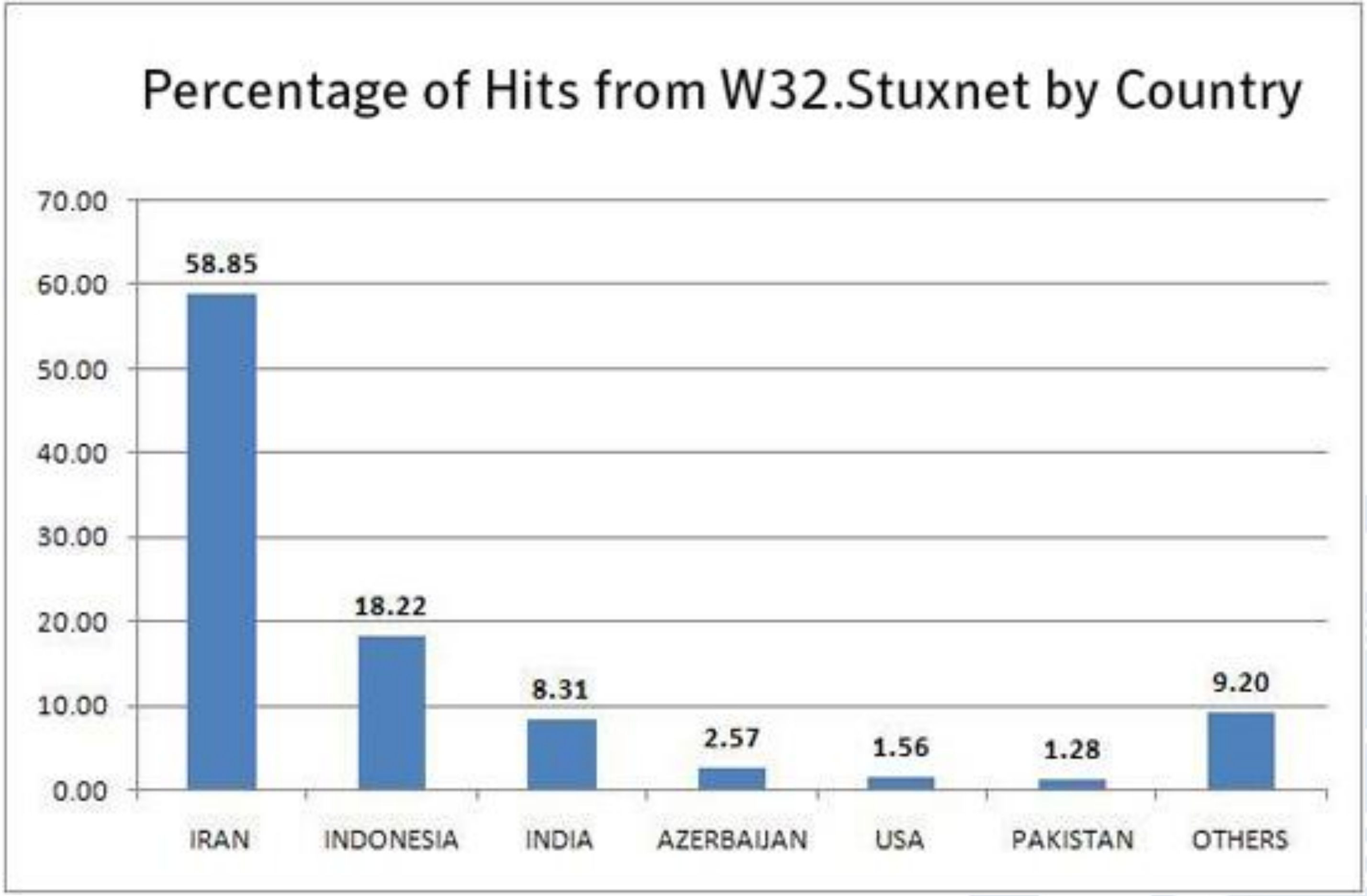
Conficker rpc vulnerability

- Patched as MS08-067
- Patch had been available, but if machines not updated, this vulnerability is easy to exploit.
- Virus verifies that date is before 1/1/2030 ??
- Verifies that antivirus products are dated before 1/1/2009.
- Verifies that kernel32.dll and netapi32.dll timestamps are before 10/12/2008.
- Appears to be testing whether exploit is likely to be detected or not.

Infection Spread

- Virus records infection history – can track ancestors.
- 5 Different organizations targeted (all in Iran)
  - Represents ~12,000 out of ~100,000 hosts
- Primary Infection 1 (version 1.000)– June 22, 2009
  - ~360 infected hosts
- Primary Infection 2 (version 1.100) – March 1, 2010
  - ~8300 infected hosts
- Primary Infection 3 (version 1.101) April 14, 2010
  - ~3300 infected hosts
- August,2010 –stopped recording infected sites from within Iran (link blocked to “sinkhole”).

Infection by country

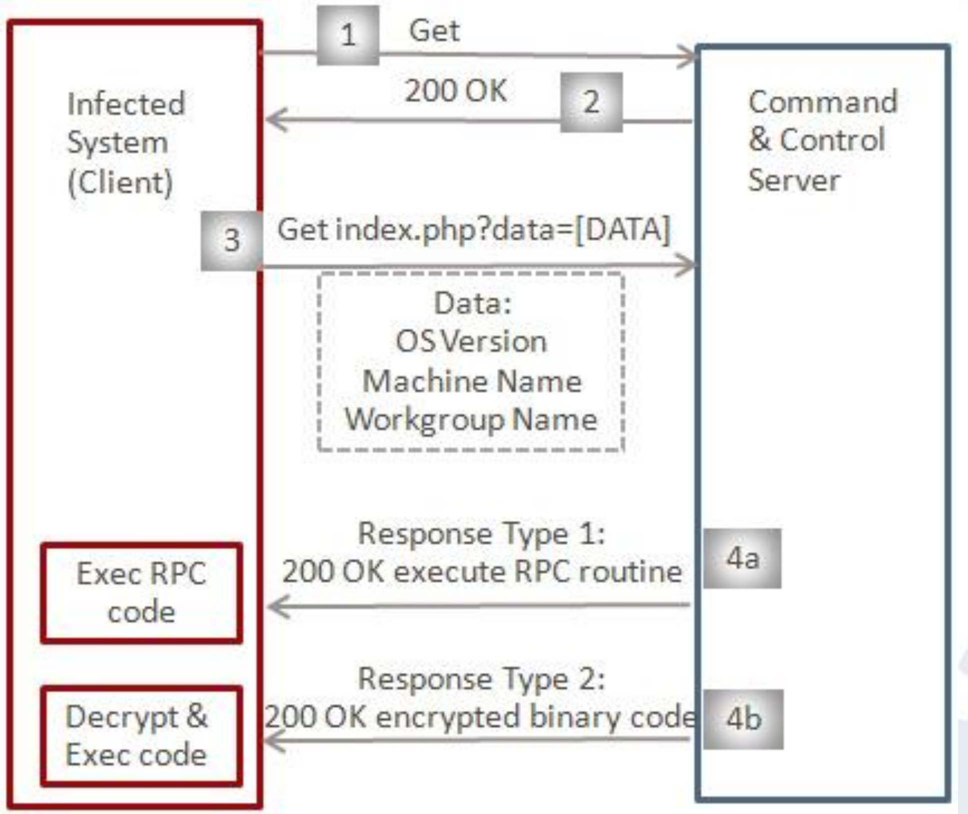


From Symantec (W32.Stuxnet) – updated 2/26/2013

How is it controlled / updated?

- Communicates with servers:
  - Smartclick.org
  - Best-advertising.net
  - Internetadvertising4u.com
  - Ad-marketing.net
- Uses http to communicate with Command and Control (http-c2)
  - Messages sent to server which immediately forwards message to some other (unknown) server.
  - Embeds upload information on infection and download updates to virus through
  - Information passed back in encrypted with AES using 1 of several keys.

How is it controlled / updated?



Infected System (Client)

Command & Control Server

1 Get

2 200 OK

3 Get index.php?data=[DATA]

Data:
OS Version
Machine Name
Workgroup Name

Response Type 1:
200 OK execute RPC routine 4a

Exec RPC code

Response Type 2:
200 OK encrypted binary code 4b

Decrypt & Exec code

1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code

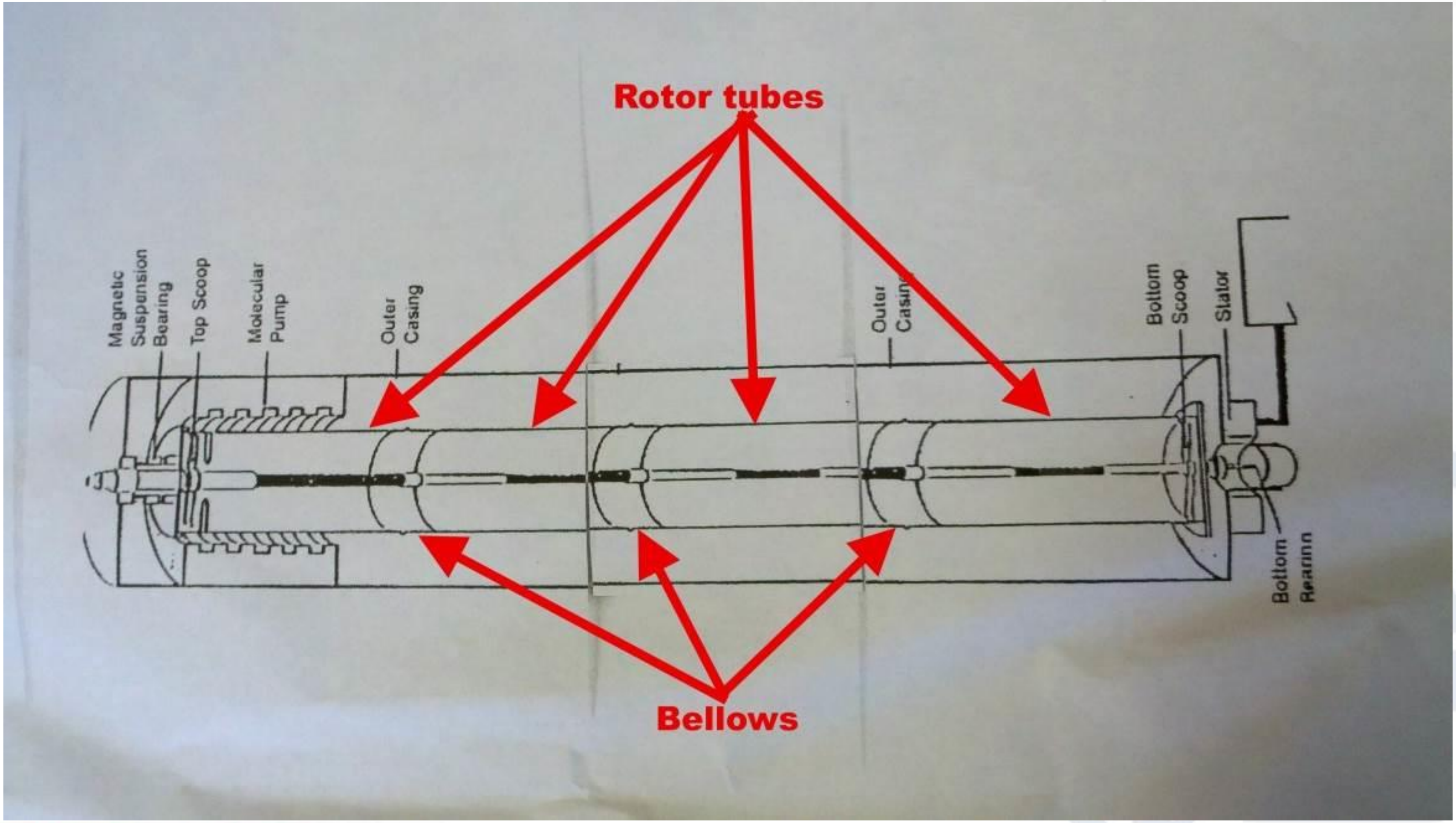
What is the target?

- Very selective propagation. Will only infect 3 machines from a flash drive (probably to limit risk of detection).
- Looks for machines running Siemens Step 7 development software (used to build PLC control programs).
- Virus target is to modify programs used to control Simatic Programmable Logic Controllers (PLCs).

What does Stuxnet look for?

- Then looks for PLC logic running frequency converters. Specifically looking for more than 155 converters running at a frequency between 800 and 1200 Hz.
  - Very few frequency converters in industry run at frequencies above 1000. (Uranium centrifuges are the exception)
  - Iran’s Natanz nuclear facility has (had) 160 frequency converters used to run their centrifuges.

Uranium Enrichment Centrifuge



Iranian Centrifuges

Step 7 project files

- Siemens Step7 development system used to build programs that run industrial controllers.
- Virus modifies exe and dll files in the development environment to allow virus to download files into existing projects.
- Projects are infected if:
  - Project has been accessed within the last 3.5 years
  - Project contains a wincproj folder
  - Project is not an example project (*\step7\examples)

Step 7 project files

- Virus infects *.s7p and *.mcp files
- Creates new *.tmp files that contain the virus.
- Virus can verify virus version and update the infection (through RPC) if needed.

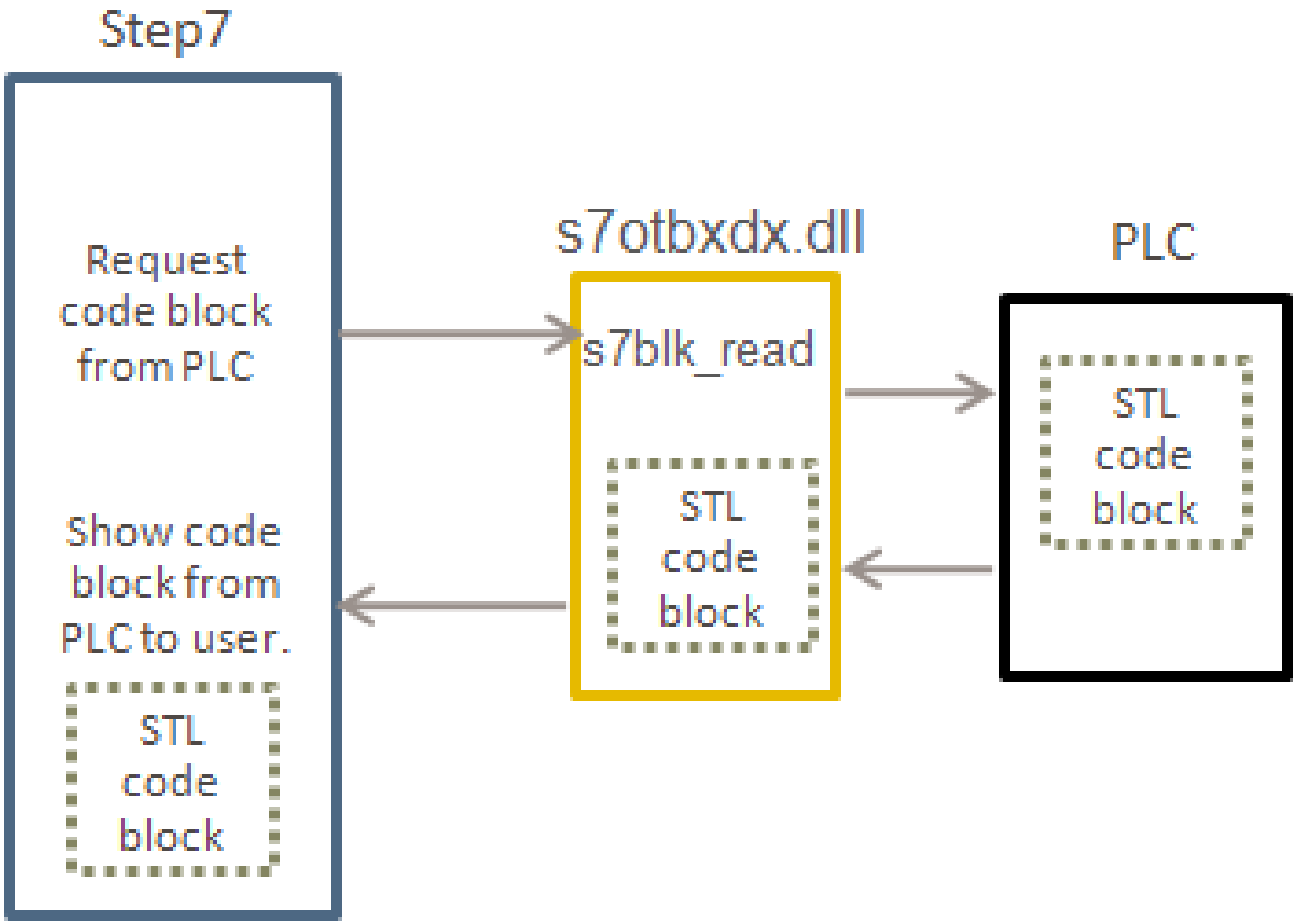
What is Step 7?

- Test and development environment (like Visual Studio)
- Used to develop programs to control programmable Logic Controllers
- Can connect directly to PLCs to:
  - View/modify memory
  - Download programs
  - Debug code
- Once program is downloaded, Step7 can disconnect and PLC will function by itself.

Step 7 Program structure

- **Data Blocks** (DB) contain program-specific data, such as numbers, structures, and so on.
- **System Data Blocks** (SDB) contain information about how the PLC is configured. They are created depending on the number and type of hardware modules that are connected to the PLC.
- **Organization Blocks** (OB) are the entry point of programs. They are executed cyclically by the CPU. In regards to Stuxnet, two notable OBs are:
  - OB1 is the main entry-point of the PLC program. It is executed cyclically, without specific time requirements.
  - OB35 is a standard watchdog Organization Block, executed by the system every 100 ms. This function may contain any logic that needs to monitor critical input in order to respond immediately or perform functions in a time critical manner.
- **Function Blocks** (FC) are standard code blocks. They contain the code to be executed by the PLC. Generally, the OB1 block references at least one FC block.

Step7communications



Replace communications link!

- Stuxnet copies original s7otbxdx.dll to s7otbxsx.dll
- Stuxnet then inserts its own version of s7otbxdx.dll
  - Original library contains 109 different functions (exports)
  - 93 exports unmodified (passed through to original library
  - Remaining 16 exports modified to change commands, hide data, etc.

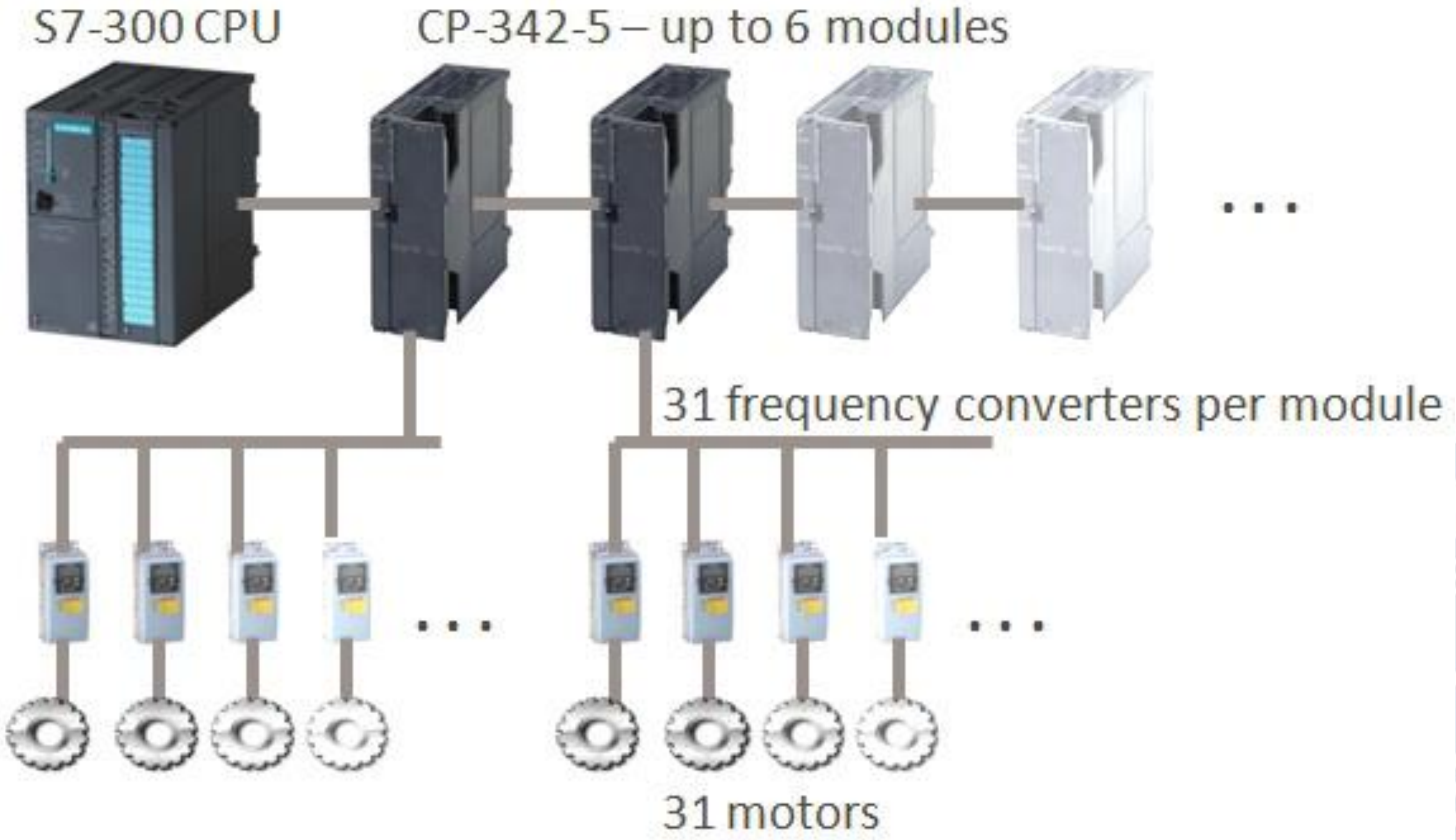
The infection process

- s7otbxdx.dll
  - Starts 2 threads used to infect the logic controllers (PLCs)
  - First thread checks for candidate PLC files every 15 minutes. If it finds a candidate file, it infects it with one of two similar by unique infection sequences (A or B).
  - Second thread monitors the PLCs, looking for a specific System data block (SDB) injected by the first thread. When one of the infected PLCs begins its attack, this second thread contacts all other infected PLCs to coordinate the attack.

The infection Thread

- Check PLC code for PLC type. Looking for 6ES7-315-2
- If found, check SDB for Profibus communications processor CP342-5 (used to control a number of devices, including frequency converters).
- Now, look for at least 33 specific freq. converters
    - Type code 7050H (part # KFC750V3 – frequency converter made by Fararo Paya (Iran)
    - Type code 9500H (Vacon NX frequency converter made by Vacon (Finland).
    - If above detected and #7050H > 9500H, use Sequence A
    - Else if above detected & #9500H > #7050H, use Sequence B

Centrifuge control structure


S7-300 CPU
CP-342-5 – up to 6 modules
. . .
31 frequency converters per module
. . .
. . .
31 motors

The infection Thread

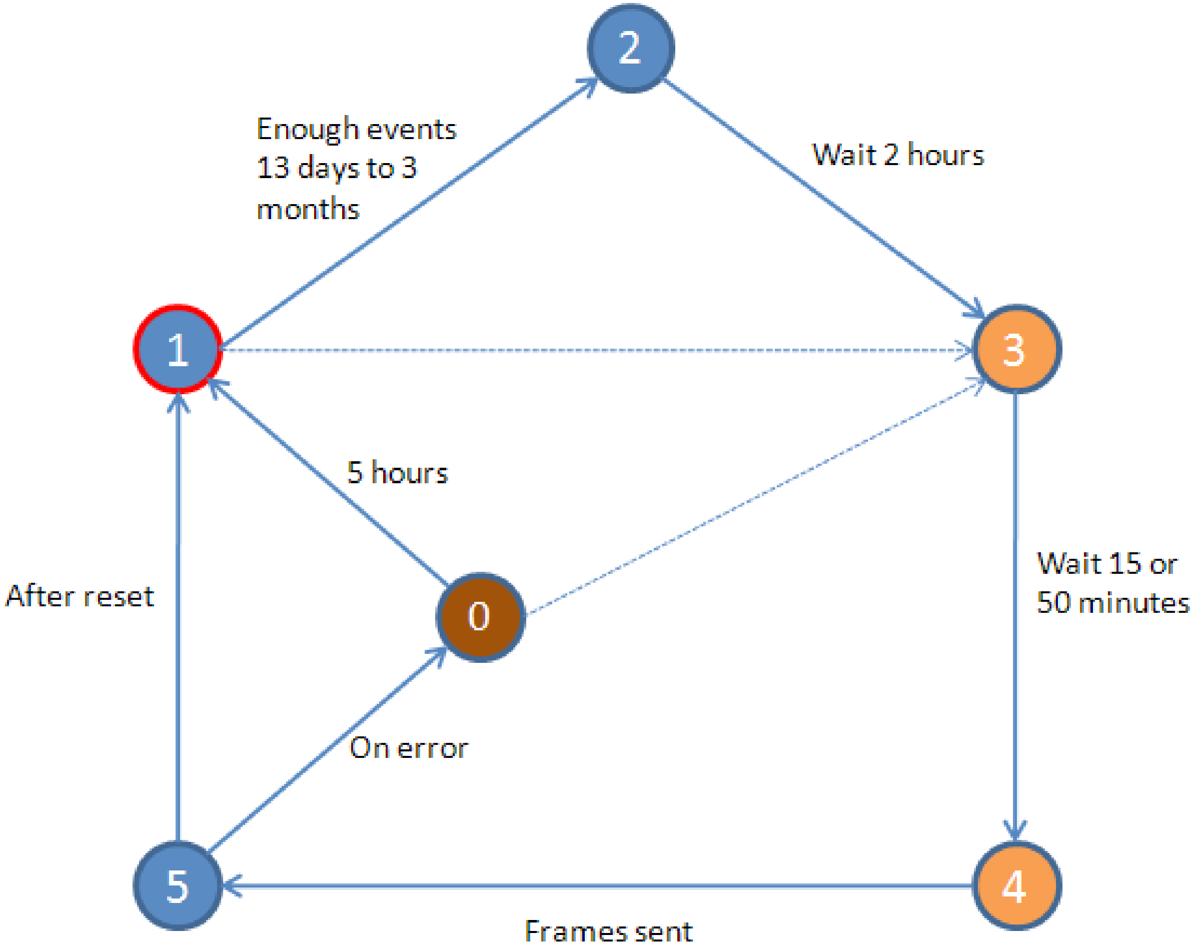
重点大学信息安全专业规划系列教材

恶意代码与计算机病毒

——原理、技术和实践

- OB1 (main entry to PLC program) infection
  - Prepend infection to original code
  - Monitors flow of data between PLC program and controller station.
  - Modifies some instructions sent to PLC
  - Replaces some status data sent from PLC to controller.

Infection state machine



Infection state machine

- Normal State sequence 1-2-3-4-5-1
  - Cycle may be adjusted if other controllers in the set have moved to a higher state.
- State 1
  - Monitor traffic events (typically 60/min – max 186). Count events (cap at 60/min) until ~1.1 million observed (~13 days)
  - Expecting a base frequency of 1064 Hz.
- State 2
  - Seems to be only a delay of 2 hours.
- State 3
  - Sequence 1 – set frequency to 1410 Hz; Wait 15 minutes
  - Sequence 2 – set frequency to 2 Hz; Wait 50 minutes
- State 4
  - Set frequency to 1064 Hz
- State 5
  - Reset event counter and wait for ~2.3 million events (~26.6 days)

Where did it come from (ancestors)

- Stuxnet 0.5
  - Discovered in 2007 (under development in 2005)
  - Propagated only through Step 7 infections
  - Attack strategy to close valves within facility, causing significant damage to equipment.
  - Used a different development framework than later versions of the virus.

How has it evolved?

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task Scheduler Exploit
CVE-2010-2743			X	X	LoadKeyboardLayout Exploit
CVE-2010-2729		X	X	X	Print Spooler RCE
CVE-2008-4250		X	X	X	Windows RPC Server Service
CVE-2012-3015	X	X	X	X	Step 7 insecure Library loading
CVE-2010-2772		X	X	X	WinCC default Password
CVE-2010-2568			X	X	Shortcut .lnk
MS09-025		X			NuUserRegisterClassExWow

What has it become?

- DuQu Trojan
  - Discovered October, 2011
  - Creates files with names prefixed with “-DQ”
  - Identified in 6 different organizations with locations in:
    - Europe (4 countries)
    - Iran
    - Sudan
    - India
    - Vietnam
  - Target seems to be information gathering.
    - Includes general remote access capabilities
    - Gathers passwords
    - Takes screenshots

DuQu

- Has used a 0-day exploit in MS Word to install DuQu, but not clear what other install techniques are used.
- Only a limited number of infections detected.
- Uses several techniques found in Stuxnet
  - Valid certificate to sign drivers
  - HTTP/HTTPS command and control servers
  - Virus removes itself after 36 days

who is at risk?

- Stuxnet
  - If you aren’t a nuclear enrichment facility in Iran, your risk from Stuxnet is very low.
  - Other machines are infected, but no payload is delivered unless very specific conditions are met.
- Stuxnet successors (DuQu, etc.)
  - Use sophisticated attack vectors (expensive), so generally reserved for high-value targets.
  - Lower probability of primary infection, but if utilities are attacked, possibility of secondary effects (lose power to your home, etc.).

综合实验七：基于U盘传播的蠕虫病毒实验

【实验目的】

- 理解U盘蠕虫病毒的传染原理。

【实验环境】

- VMWare Workstation 5.5.3
- Windows XP sp2

基于U盘传播的蠕虫病毒实验

【病毒原理】

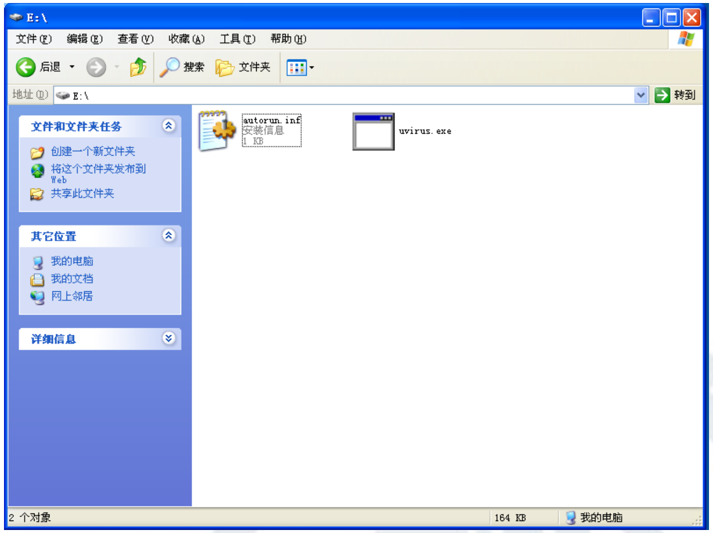
- U盘病毒通常都是通过给u盘创建autorun.inf文件，利用Windows系统的自动播放功能来触发病毒程序，从而达到传染和破坏的目的。
- Autorun.inf文件可以通过以下命令来运行病毒程序
- Open=Virus.exe
- 指定设备启用时运行Virus.exe。
- ShellExecute=Virus.exe
- 设备启用时执行文件Virus.exe。
- Shell\XXX\command=Virus.exe
- 当用户在右键菜单中点击XXX时，运行Virus.exe

实验步骤

1．实验素材：在附书资源目录experiments\wormu下。

2．检查干净的电脑各分区的是否存在autorun.inf和病毒文件virus.exe（需要设置显示隐藏文件和系统文件等选项）。

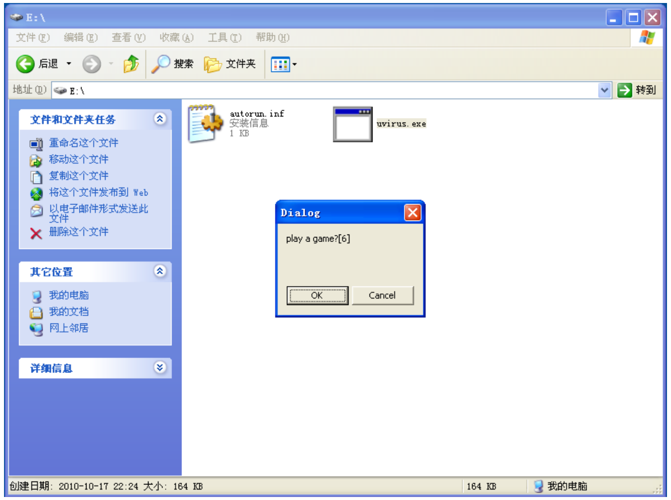
3．插入含有病毒的U盘，U盘的右键菜单出现“auto”后，双击u盘，观察现在各分区的情况（如图）。



4．查看autorun.inf文件内容。其内容如下：

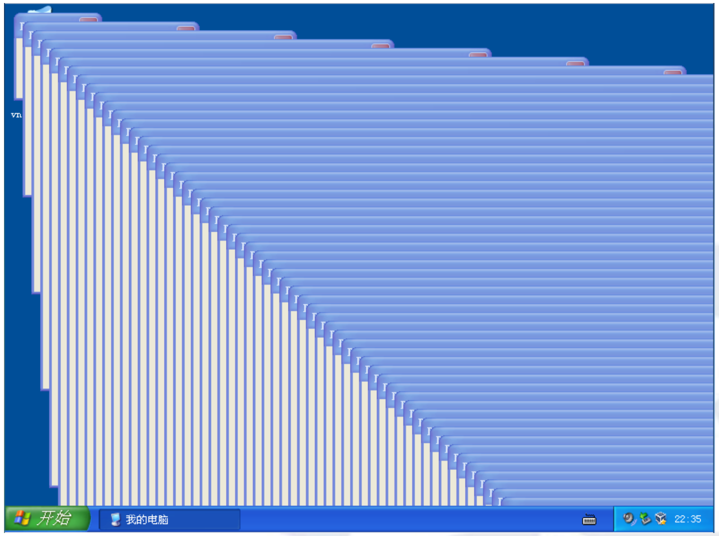
- [AutoRun]
- open=uvirus.exe
- shellexecute=uvirus.exe
- shell\auto\command=uvirus.exe

5．观察病毒触发后的效果。如图所示。



play a game?[6]

创建日期: 2010-10-17 22:24 大小: 164 KB　164 KB　我的电脑



6．插入干净的U盘，观察U盘是否被感染。

【注意事项】

- 实验前，请关闭杀毒软件。否则病毒样本会被自动杀除。
- 请注意操作系统的版本。Win XP Sp2及以下版本都适用。

Any Questions

冲击波实验

【实验环境】

- Host系统：
  - VMWare Workstation 7.0.1
  - Win2000　Advance Server SP1
- 虚拟机中操作系统：
  - 攻击方Linux（Ubuntu8.04）
  - 攻击对象Win2000Advance Server SP1
- 实验素材：experiments目录的RPC目录下。
- 虚拟机映像：vituralmachine目录下的PRCVM。

- 实验准备
  - 环境安装
    - 安装虚拟机VMWare，并在其中分别安装Linux以及WIN2000操作系统。如果直接下载虚拟机映像文件，则可以省去该部分。
  - 源码准备
    - 从电子资源中拷贝病毒程序源码vdcom.c到Linux任意目录中，之后的编译运行等工作都在此目录中进行。　如果直接下载虚拟机映像文件，则源码已经存在于相关目录中。

- 编译源码
  - 使用gcc编译源码：gcc –o rpcattack vdcom.c， 生成文件rpcattack， 如下图所示。并检查文件是否生成。

- 开始冲击波实验
  - 被攻击方：确保目标虚拟机WIN2000打开，并检查c盘根目录下没有多余实验用文件。
  - 攻击方：运行病毒程序，输入/rpcattack
- 请观察现象
  - 参考教材截图