Enabling Insecurity

Dr. Stacy Prowell

Chief Cyber Security Research Scientist
Oak Ridge National Laboratory

TIMELINE

Before Stuxnet

- 11 April 2008
  - "Cyber" posted a password (2WSXcder) hard coded into the Siemens Step7 system, used for the back-end Simatic WinCC system's SQL database.
  - Siemens: "Don't change it, you'll break stuff."
- 17 November 2008
  - NSTB Report: "Common cyber security vulnerabilities observed in control system assessments by the INL NSTB program."
  - Identifies three vulnerabilities…
- 20 November 2008
  - Zlob trojan uses the .lnk vulnerability in Windows Explorer (autorun.inf)
- April 2009
  - Hackin9 article exposes the Windows print spooler vulnerability

Siemens warns Stuxnet targets of Scada password risk

Summary: *Customers should not change the default passwords in WinCC Scada software, even though the Stuxnet malware is using them to infect systems, Siemens has advised*

Source: ZDNet

Cyber Новый писатель Зарегистрирован: 22.10.2007 Сообщения: 14	Добавлено: Пт Апр 11, 2008 19:27 Заголовок сообщения: login='WinCCConnect' password='2WSXcder' login='WinCCAdmin' password='2WSXcde.'
Вернуться к началу	профиль ЛС email www

Source: http://iadt.siemens.ru/forum/viewtopic.php?p=2974&sid=58cedcf3a0fc7a0b6c61c7bc46530928

Security Dimension	Category	Common Vulnerability
		Control system protocol uses weak integrity checks – 3.4.2.4
	Communication Protocols with Weak or No Authentication	Standard IT protocol encryption can be defeated – 3.4.2.1
		Standard IT protocol uses clear text authentication
		Control system protocol uses weak authentication – 3.4.2.2
	Weak User Authentication	Improper security configuration – 3.4.3.1
		No password required – 3.4.3.2
		Weak passwords – 3.4.3.3
	Least Privileges not Enforced	Unauthorized directory traversal allowed – 3.4.4.1
		Services running with unnecessary privileges – 3.4.4.2

Source: NSTB Report

Aside: Exploits and YouTube

- MS08-067 (RPC vul)
  - Watch at: http://www.youtube.com/watch?v=EM2MBGbI84E
- MS10-046 (.lnk vul)
  - Watch at: http://www.youtube.com/watch?v=r7QIsXvXrIo
- MS10-061 (spooler exploit)
  - Watch at: http://www.youtube.com/watch?v=Fy0S9KMNjnY
- MS10-073 (keyboard layout)
  - Watch at: http://www.youtube.com/watch?v=Hm1PFia7H_Q

Security TechCenter > Security Bulletins > Microsoft Security Bulletin MS08-067

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: Thursday, October 23, 2008

Version: 1.0

Stuxnet in Action

- 4:30pm, 22 June 2009
  - Stuxnet is compiled, and infects the first machine 12 hours later.
  - Does not use Siemens or .lnk vuls.
- Jan 2010
  - Stuxnet is *signed* with a valid RealTek Semiconductor (Taiwan) certificate.
- May 2010
  - Version 2 of Stuxnet, with all exploits and digital signature.

Source: DigitalGlobe

Stuxnet Discovered

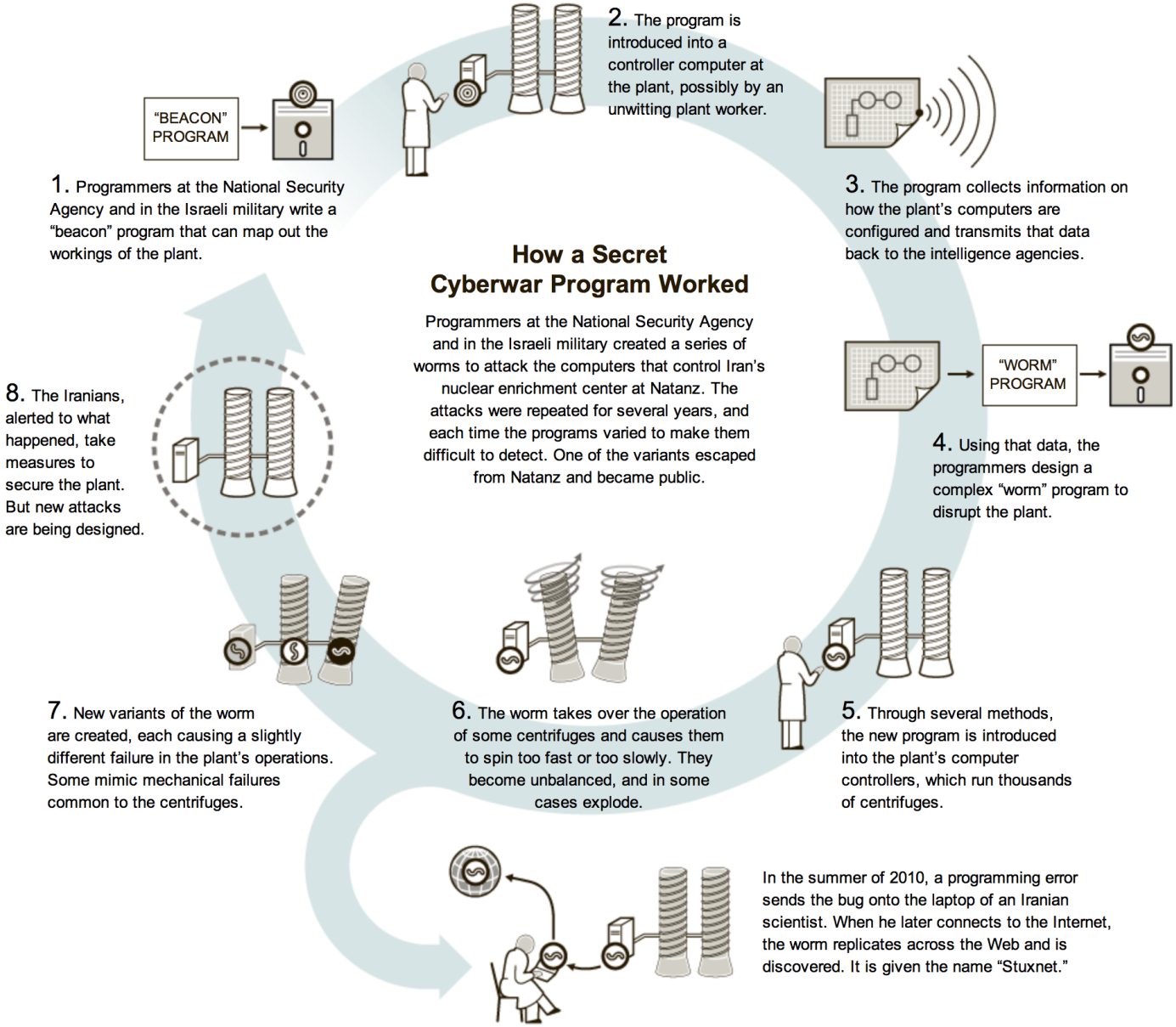
- June 2010
  - VirusBlokAda discovers Stuxnet on machine in Iran.
- 15 July 2010
  - Stuxnet is public knowledge (Brian Krebs).
  - Stuxnet is signed with JMicron's certificate, since RealTek's has expired.
  - A distributed denial of service attack delays news of Stuxnet's discovery.
- August 2010
  - Symantec reveals that Stuxnet injects code into PLC's manufactured by Siemens. They report that Stuxnet is designed for sabotage.
- November 2010
  - Ali Akbar Salehi (MIT Ph.D. 1977), head of Iran's Atomic Energy Organization, reports "Westerners sent a virus to our country's nuclear sites. […] We discovered the virus […] because of our vigilance and prevented the virus from harming [anything]."

Source: English Wikipedia

The End

- 24 June 2012
  - Stuxnet self-destructs.

- John Bumgarner claims to have found evidence of Stuxnet / Duqu active as far back as 2006… and to have connected it with Conficker.



Source: http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html

Cyber Warfare Research Team
Cyber and Information Security Research Group

Others

- 1 September 2011
  - Duqu (~DQ files)

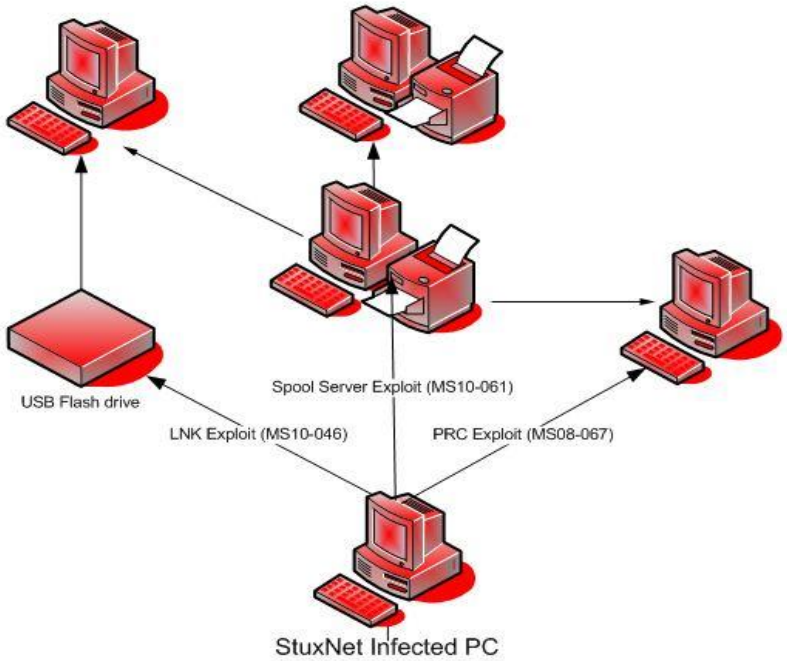
- 28 May 2012
  - Flame / Flamer / Skywiper
  - Most sophisticated malware yet discovered: 20MB
  - Contains a SQL database and a LUA virtual machine for scripting
  - Spreads by: USB, Network
  - Records: Audio, Keyboard, Screenshots, and Skype
  - Does Bluetooth beaconing to download data from nearby devices
  - Exploited a cryptographic weakness (MD5 collision) to sign itself

- 16 August 2012
  - Shamoon / Disttrack erases 30,000 Saudi Aramco workstations.

STUXNET

Why Was Stuxnet Interesting?

1. Used 8 different propagation methods.
2. Includes four zero-day exploits.
3. Used a stolen digital certificate.
4. It crossed the “air gap.”
5. It used replay to fool observers.
6. It used a rootkit to hide on infected computers.
7. Infected Step7 project files.
8. Replaced s7otbxdx.dll to automatically infect / disinfect.
9. Modified PLC code.
10. This is a **template** for future malware.

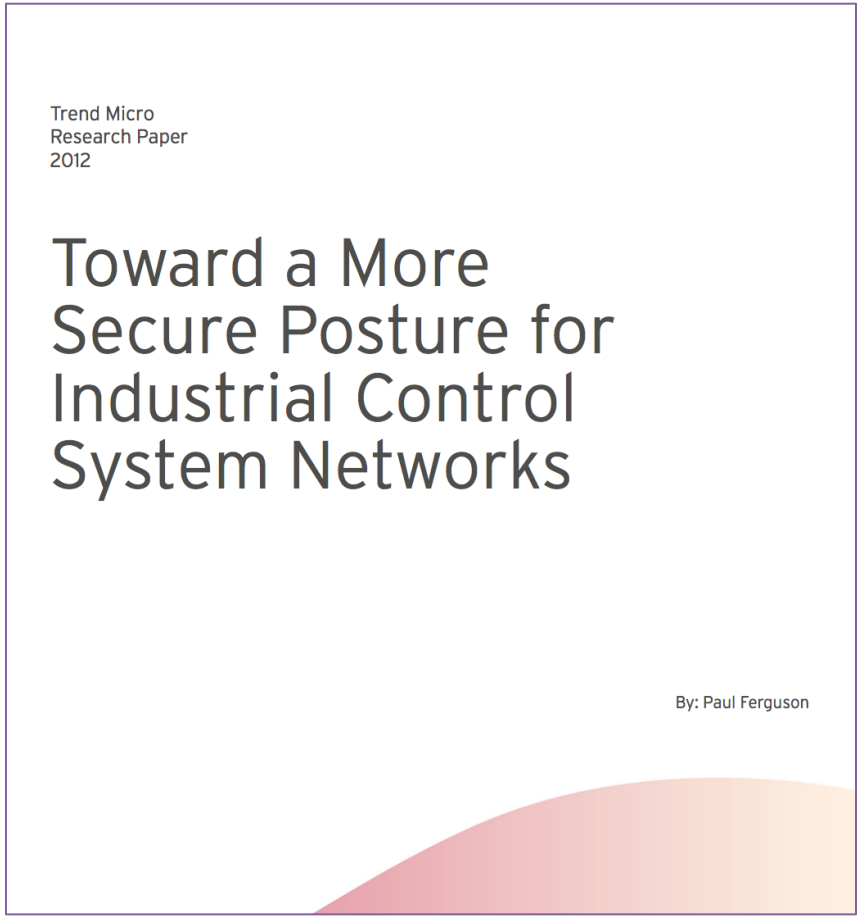


The “Air Gap Principle”

Critical control systems should never, ever interact nor interconnect with Internet systems in any way, shape, or form.

“In practical and operational terms, however, physically separating networks is not functionally nor operationally feasible in the real world.”

- “Toward a more secure posture for industrial control system networks,” Paul Ferguson, Trend Micro


Trend Micro
Research Paper
2012

Toward a More Secure Posture for Industrial Control System Networks

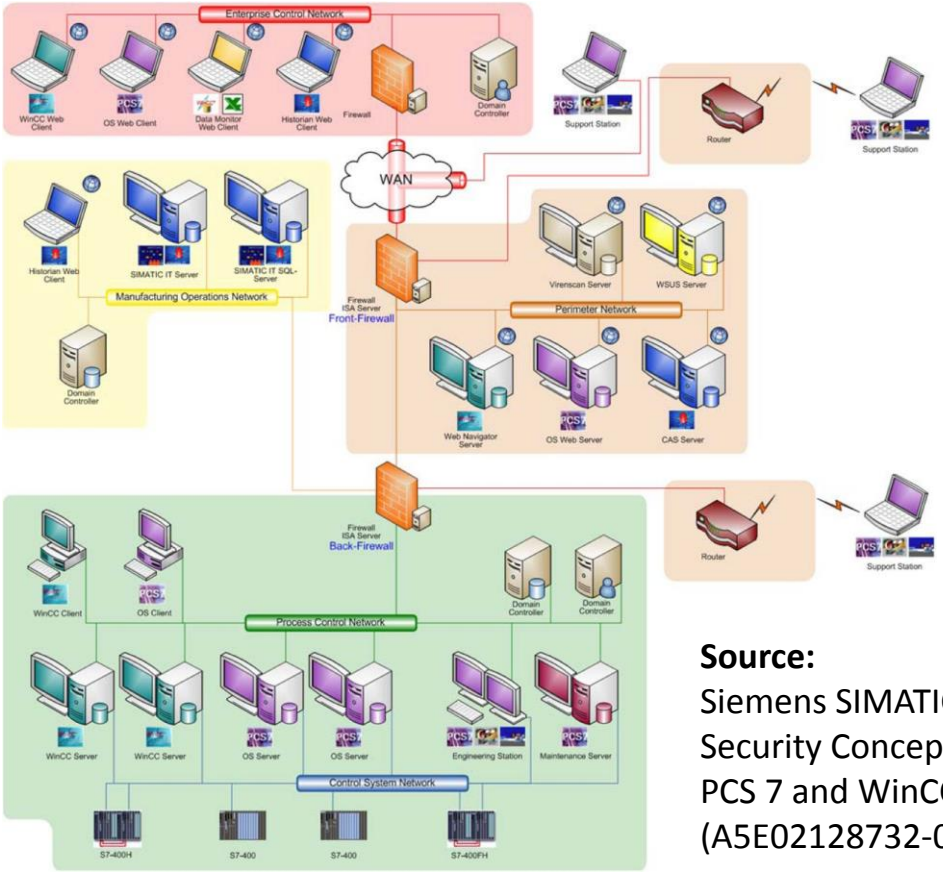
By: Paul Ferguson

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_secure-posture-for-industrial-control-system-networks.pdf

Spot the Air Gap!

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network."

- Sean McGurk, DHS, Testimony to Subcommittee on National Secruity



Source:
Siemens SIMATIC Security Concept PCS 7 and WinCC (A5E02128732-01)

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=26462131&caller=view

Since Stuxnet?

- July 2011
  - Basisk / Basisk hard-coded password in S7-300 (FW 2.3.4) yields a command shell. Now you can dump memory and reprogram. (NSS Labs)
  - Replay: Intercept commands from Step7 and play these commands back to another PLC. Such as STOP. S7-200, S7-300, S7-400, S7-1200…
  - Authentication? Replay. Disable authentication? Replay. Sessions never expire…
  - So… Scan the network for devices with port 102 open

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

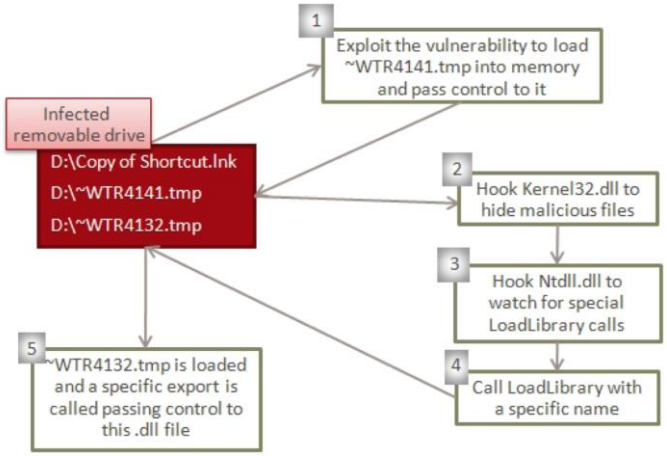
ICS-ALERT-11-204-01A—SIEMENS S7-300 HARDCODED CREDENTIALS

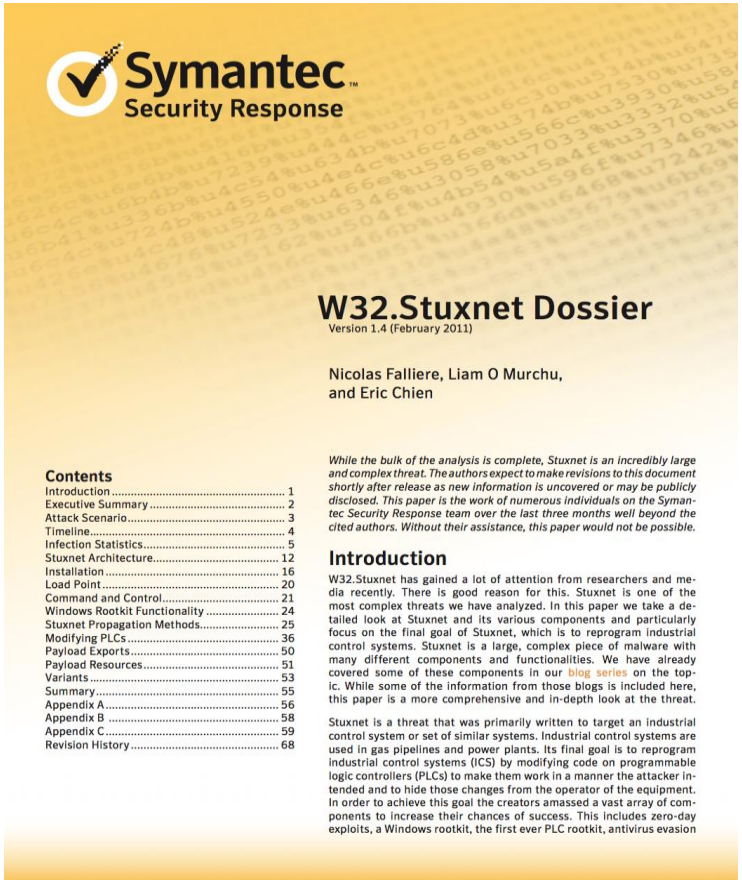
UPDATE A

Lots More

- Symantec report details how Stuxnet works, propagates, installs itself as a stored procedure in WinCC, etc.

Figure 14
USB Execution Flow





Symantec
Security Response

W32.Stuxnet Dossier
Version 1.4 (February 2011)

Nicolas Falliere, Liam O Murchu, and Eric Chien

Contents

Introduction ... 1
Executive Summary ... 2
Attack Scenario ... 3
Timeline ... 4
Infection Statistics ... 5
Stuxnet Architecture ... 12
Installation ... 16
Load Point ... 20
Command and Control ... 21
Windows Rootkit Functionality ... 24
Stuxnet Propagation Methods ... 25
Modifying PLCs ... 36
Payload Exports ... 50
Payload Resources ... 51
Variants ... 53
Summary ... 55
Appendix A ... 56
Appendix B ... 58
Appendix C ... 59
Revision History ... 68

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.

Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our blog series on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion

ACCESS

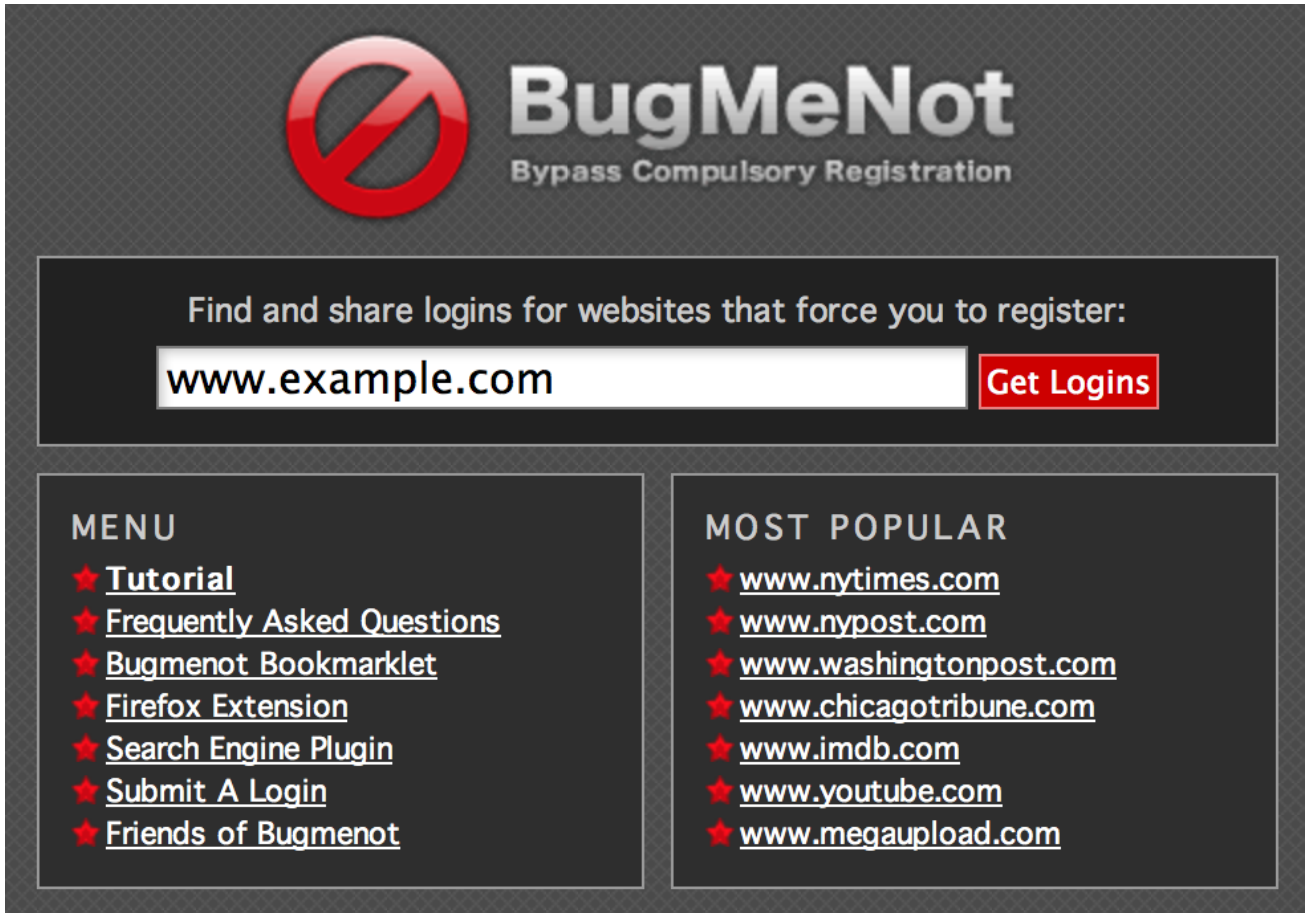
The Web Is Your Frenemy

- Nessus, nmap, and others scan networks for machines, open ports, and known vulnerabilities, so…
  - What if someone ran something like Nessus over the entire Internet?
  - And made those results easily searchable?
- Some people have logins (username and password) for machines and sites, so…
  - What if someone created a place to upload the username / password for any site?
  - And made that database easily searchable?

What's Out There?

https://shodanhq.com

Logins?



http://bugmenot.com

Sure… But that'd never work.

SHODAN "default password"

Home Search Directory

Vote Export Data

Services

FTP	4,997
HTTP	2,808
HTTP Alternate	99
Memcache	4
SSH	1

Top Countries

United States	3,209
Japan	1,866
Germany	1,045
Netherlands	584
Bulgaria	168

Top Cities

Englewood	2,787
Chiba	502
Tokyo	318
Taipei	72
Sofia	69

Top Organizations

Verio Web Hosting	3,274
NTT Communications Cor...	902
NTT Europe Web Hosting...	265
OCN Provided By NTT-Co...	87
Ziggo	72

Login Form

User Name:

Password:

Login

Cisco IOS

Corporation

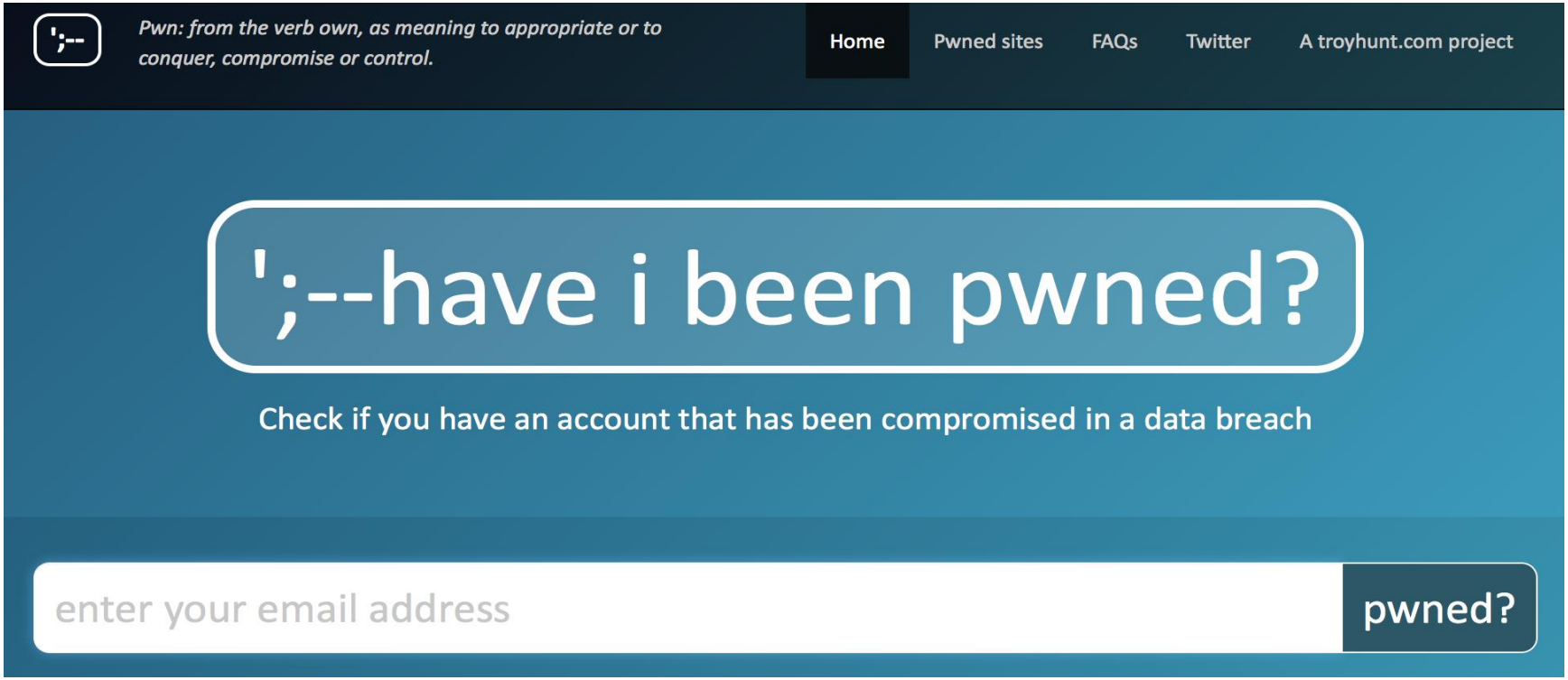
Added on 15.01.2013

Pasadena

Details

HTTP/1.0 200 OK
Date: Tue, 15 Jan 2013 09:00:48 GMT
Server: **cisco-IOS**
Connection: close
Content-Length: 1431
Content-Type: text/html
Expires: Tue, 15 Jan 2013 09:00:48 GMT
Last-Modified: Tue, 15 Jan 2013 09:00:48 GMT
Cache-Control: no-store, no-cache, must-revalidate
Accept-Ranges: none

So… Have they got you?



http://haveibeenpwned.com/

Maybe.

Your email, username, and password have been compromised at least 1 time(s).

The most recent recorded occurrence is November 4, 2013. You should change all your passwords as soon as possible. Ensure that each password is at least 10 characters in length and is a combination of random upper and lower case letters, numbers, and symbols. Do not re-use the same password across multiple sites!

Want us to keep an eye out for your email address?

We can let you know if we come across your email in any new breaches!

https://shouldichangemypassword.com/

VULNERABILITY

The Life of a Vulnerability

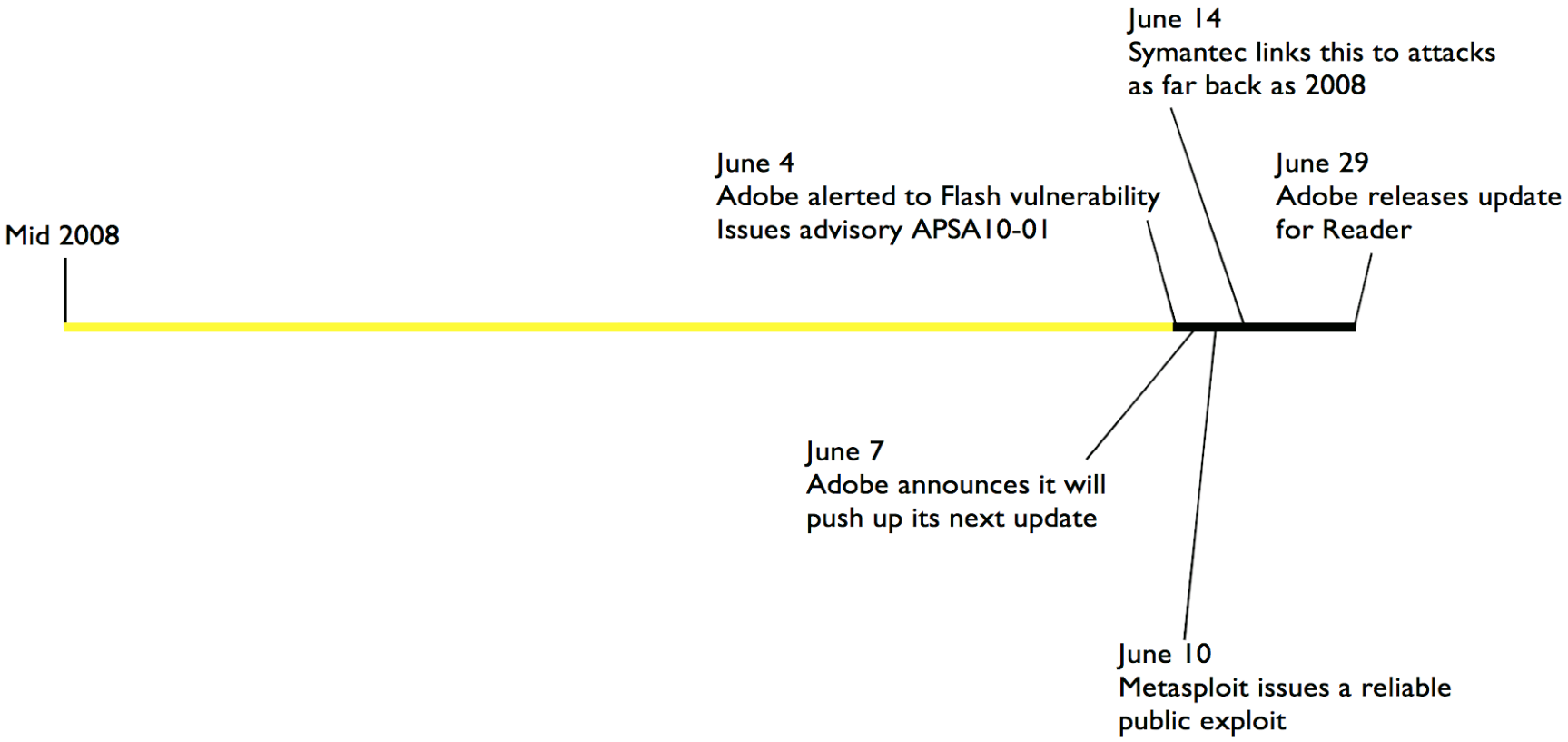
June 14
Symantec links this to attacks
as far back as 2008

June 4
Adobe alerted to Flash vulnerability
Issues advisory APSA10-01

June 7
Adobe announces it will
push up its next update

June 10
Metasploit issues a reliable
public exploit

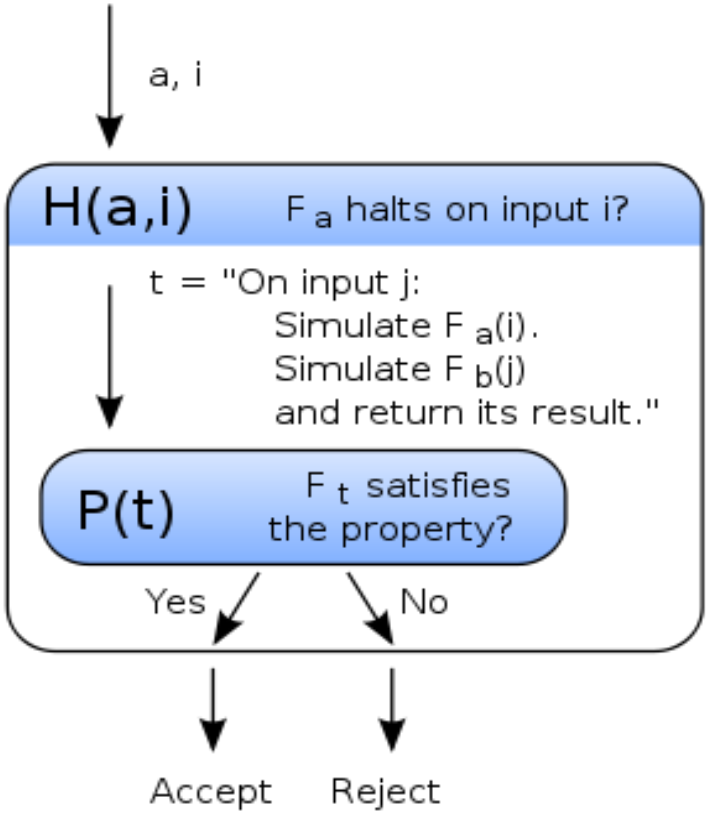
The Life of a Vulnerability



MALWARE

Malware

- *Any non-trivial property of programs is undecidable*. [Rice's Theorem]
  - The halting problem
  - The malware detection problem
- A perfect antimalware program cannot be constructed…



Behavior

- …But you can observe behavior.
  - *Time* consumed by processes on a machine.
  - *Power* transients on a machine.
- Malware actually does make your computer run slower… and in very specific ways.
  - Hide process, kernel module, tinker with clock, hide files, record keystrokes, observe packets…

Problems Have (Not) Been Solved

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-13-016-02—OFFLINE BRUTE-FORCE PASSWORD TOOL TARGETING SIEMENS S7

January 16, 2013

ALERT

RISK

Risk

$$R = T \times V \times C$$

Risk

Threat

Person | Circumstance | Event

Vulnerability

Weakness | Bug | Backdoor

Consequence

Loss | Damage

Source: Sean McGruk, "Industrial Control System Security," Presentation, 2008. http://tinyurl.com/23etw3x

Risk

$$R = \boxed{T} \times V \times C$$

Reduce the **threat**

- Hackers | Insiders | States | Terrorists
- Intelligence

Risk

$$R = T \times \boxed{V} \times C$$

Reduce the **vulnerability**

- Weaknesses | Bugs | Backdoors
- Formal / rigorous analysis
- Secure coding techniques
- Supply chain risk management

Risk

$$R = T \times V \times \boxed{C}$$

Reduce the **consequences**

- Loss | Damage
- Resiliency | Survivability
- Rely on the physics of the system

Stacy Prowell

voice: +1 (865) 241-8874 • fax: +1 (865) 576-5943
prowellsj@ornl.gov

THANK YOU!