Cybersecurity –
An Evolving Law and Policy Issue

KEIO University SFC

Urs Gasser

Berkman Center
Harvard University

December 8, 2011

1

Agenda

I. Examples

II. Government Responses

III. Observations

IV. Looking Ahead

2

I. Examples

3

W32.Stuxnet

Risk Level 2: Low

Summary | Technical Details | Removal

Printer Friendly Page | Rate This Page

Discovered: July 13, 2010
Updated: September 17, 2010 8:53:13 AM
Also Known As: Troj/Stuxnet-A [Sophos], W32/Stuxnet-B [Sophos], W32.Temphid [Symantec], WORM_STUXNET.A [Trend], Win32/Stuxnet.B [Computer Associates], Trojan-Dropper:W32/Stuxnet [F-Secure], Stuxnet [McAfee], W32/Stuxnet.A [Norman], Rootkit.Win32.Stuxnet.b [Kaspersky], Rootkit.Win32.Stuxnet.a [Kaspersky]
Type: Worm
Infection Length: Varies
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP
CVE References: CVE-2010-2568

W32.Stuxnet was first categorized in July of 2010. Originally Symantec named the detection W32.Temphid based upon the information originally received but later renamed it Stuxnet to bring our naming convention in line with other vendors, and therefore virus definitions dated July 19, 2010 or earlier may detect this threat as W32.Temphid.

4

Sony: Personal info compromised on PSN

by Erica Ogg | April 26, 2011 1:07 PM PDT

Follow

comments 261 | Like 2k | Tweet 381 | +1 0 | Share 133 | More +

Sony acknowledged today that the personal information of its PlayStation Network customers has been compromised.

The company posted an update on its blog today warning its more than 70 million customers that their personal information, including customer names, addresses, e-mail addresses, birthdays, PlayStation Network and Qriocity passwords, and user names, as well as online user handles, was obtained illegally by an "unauthorized person." The data was accessed between April 17 and 19, according to Sony.

5

Google reveals Gmail hacking, says likely from China

Recommend 412 people recommend this. Be the first of your friends.

By Sui-Lee Wee and Alexei Oreskovic
BEIJING/SAN FRANCISCO | Thu Jun 2, 2011 8:08am EDT

(Reuters) - Suspected Chinese hackers tried to steal the passwords of hundreds of Google email account holders, including those of senior U.S. government officials, Chinese activists and journalists, the Internet company said.

Tweet 268
Share
Share this
+1 13
Email
Print

Related News

China rejects Google hacking claims
Thu, Jun 2 2011

Reports of Gmail hacking being probed: White House
Wed, Jun 1 2011

Cybersecurity becoming U.S. diplomatic priority
Thu, Jun 2 2011

Gmail hackers had access to accounts for months: expert
Thu, Jun 2 2011

6

Russian websites targeted on election day

Updated December 05, 2011 12:34:46

Websites which revealed violations in Russia's legislative polls were targeted in a mass hacking attack their operators said was aimed at preventing the exposure of mass fraud in the country's parliamentary elections.

RELATED STORY: Blow for Putin in Russian election results

MAP: Russian Federation

7

Characteristics

Great variety of risks related to cybersecurity

All industries affected

Various state and non-state actors involved

Potential for massive economic, societal impact

International and dynamic

8

Focus of Presentation

Private and public responses to cybersecurity risks

Technical, legal, educational, etc. measures

Focus here:
Responses by *governments*
Policy and *legal* responses

9

II.
Government Responses

10

Roles of Government

Owner and operator of systems and networks

User of IT systems

Partner with business, industry, civil society

Funder of R&D

Enactment and enforcement of public policy, law, and regulations

11

Responses

Cybersecurity not a new policy issue

Previously: Security of information systems and networks

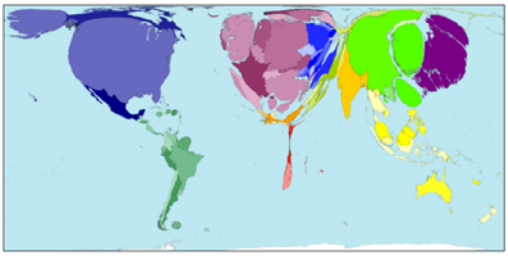
Responses in phases:
Phase I 2002-2009
Phase II 2009- now

From targeted interventions and "culture of security" to holistic cybersecurity strategies

12

Phase I:
2002-2009

< Previous Map | **Internet Users 2002** | Map No. 336 | Open PDF poster | Next Map >



During the 12 years from 1990 to 2002, people using the Internet increased in number by 224 times. By 2002 there were 631 million Internet users worldwide.

The distribution of Internet users worldwide has changed remarkably over just a dozen years. In 1990 Internet users were mainly found in the United States, Western Europe, Australia, Japan and Taiwan. By 2002 people living in Asia Pacific, Southern Asia, South America, China and Eastern Europe were notable Internet users. A not insignificant number of Internet users are also shown to be in Northern Africa, Southeastern Africa and the Middle East.

13

Factors

"Internet as *useful* platform"

E-Commerce

E-Government applications and services

National critical information infrastructures

Privacy

14

Approach

Foster trust online

Security as condition for growth of Internet Economy

Building culture of security

Using various tools, including awareness and education

Developing legal frameworks

15

16

Activities
(Law & Policy)

Legal framework for authentication (digital signature laws)

Laws against Cybercrime

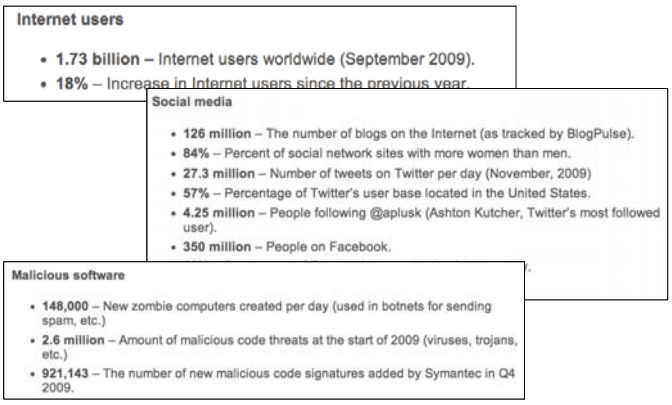
Computer Emergency Response Teams (CERT)

Action plans national critical information infrastructure protection

Updating privacy legislation

17

Phase II:
2009-current



18

Factors

"Internet as *essential* platform"

Infrastructure for all aspects of society

Increased level of cybersecurity risks across all dimensions

Increased vulnerability

Cybersecurity > national interest > national security

19

20

21

Approach

Development and implementation of national cybersecurity strategy

National security issue; military and foreign policy relevance

Agency coordination

Dynamic and proactive security measures (even pre-emptive measures?)

Private-public partnerships

22

Activities
(Law & Policy)

Data security and breach notification laws

Penalties for computer crimes

Critical Infrastructure cybersecurity plans

Stronger government coordination mechanisms

Update legislation

23

Questions

What are the merits and demerits of the 2002 ("protect businesses") vs. the 2009+ ("national security") approaches?

How much emphasis would you put on "policy and law" vs. other approaches?

24

III.
Observations

25

General

Holistic cybersecurity strategies increase number of policy issues

Explosion of policies, laws, and regulations

Sound methodological frame to be developed

Rhetoric of fear

Transparency problem

26

Table of Contents

27

Specific

Justification of regulation
Risk assessment
Trade-offs
Timing
Scope and definitions
Mechanisms
Measures of success
Unintended consequences
Ability to learn

28

VI.
Looking Ahead

29

Questions

How much cybersecurity legislation is needed?

What kind of legislation would you like to see?

What about alternatives to legislation?

30

Possible Take-Aways

Cybersecurity is a fast developing policy area

Concerning trend towards "militarization

Law not particularly well-suited to deal with cybersecurity

Need for realistic risk assessments

More technologists, fewer lawyers

31