

The New Front Line

An observation of cyber threats in the 21st century

Jonathan Francis Roscoe

<jjr6@aber.ac.uk>



November 4t 2010

Outline

Introduction

Malice in Wonderland

Cyber Warriors

Worms

Denial of Service Attacks

The Estonian Cyberassault

Stuxnet

Defensive Measures

The Future

Conclusions

The New Front Line: Estonia under cyberassault

- IEEE Security & Privacy *July/August 2007 (vol. 5 no. 4)*
- Overviews a Distributed Denial of Service attack on Estonia, hypothesises perpetrators, mechanisms and even cost
- Michael Lesk of Rutgers University

Wrote a number of Unix utilities - lex, uucp and the predecessor to stdio Involved with a number of information systems Apparently only recent contributions

Malice in Wonderland

There are a variety of software threats for machines connected to a network.

- Worms
- Viruses
- Trojans
- Rootkits
- Other malware

But threats may come from software not created with malicious intent..

Cyber Warriors - Who

- Academics
- Malicious programmers & "Script Kiddies"
- Spammers
- Disgruntled employees
- Hacktivists
- Military groups

Cyber Warfare - Why

The why depends on the who..

- Research
- Mischief
- Corporate espionage
- Money
- Political statements
- Terrorism

Worms

A computer program that *self-replicates over a computer network*.

- 1988 - The Morris Worm - intended to gauge the size of the Internet
- 1999 - ILOVEYOU - simple VBS script that used Outlook to propagate
- 2003 - SQL Slammer - slowed general Internet traffic, targetted a buffer overflow in MS SQL
- 2010 - Stuxnet - attacks a specific industrial PLC system from Siemens

Worms - How

- Install
 - Backdoor
 - Ideally unnoticed
- Propagate
 - Counterfeit/bogus software
 - Software exploits
 - Email attachments

Botnets

- A collection of infected hosts running autonomous software that can respond to commands
- Worms designed to contact and respond to an owner
- Geographically dispersed
- Used for Denial of Service attacks, Spamming, Proxying, Dialing
- Software is easy to obtain and modify
- Often "war" between owners for control of susceptible machines
- Up to a quarter of personal computers may be a part of a botnet (BBC)

Botnets

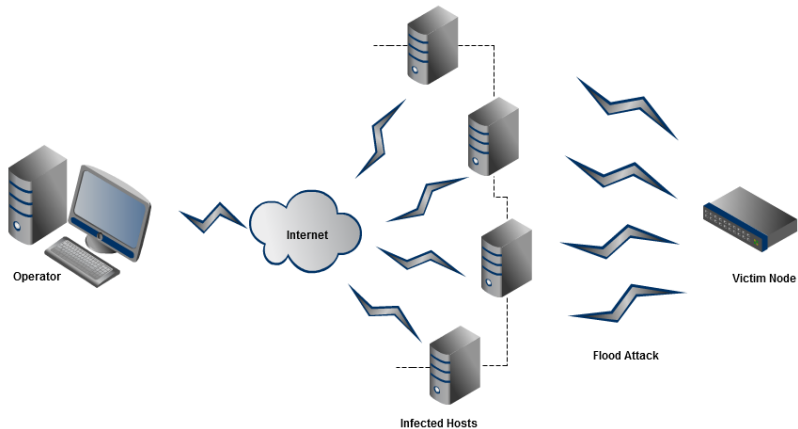
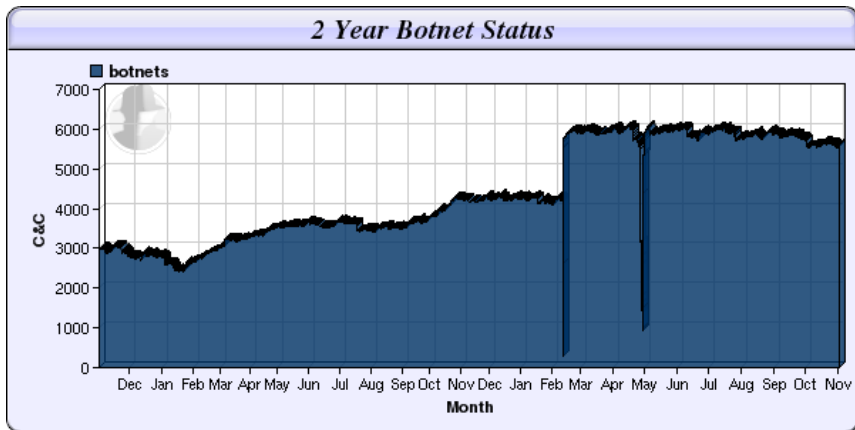


Illustration of a Distributed Denial of Service attack performed with a botnet.

Botnets









A graph counting all the known command and control networks by the Shadowserver Foundation

Denial of Service

An extremely common form of general attack. Often use botnets.

- Type
 - Distributed
 - Flood - ICMP, SYN, Smurf
 - Teardrop
 - Peer-to-peer & multicast
 - Application flood
 - Phlashing
- Motive
 - Personal
 - Business
 - Political and Tactical

Denial of Service Attacks

Attack Subclass	Number of Attacks	Percentage
TCP SYN	377	 31.4%
Total Traffic	366	 30.5%
Protocol	63	 5.2%
DNS	59	 4.9%
Bandwidth	57	 4.8%
TCP NULL	21	1.8%
TCP RST	18	1.5%
other	239	 19.9%

Summary of DoS attack methods, from <http://atlas.arbor.net/summary/dos>

The Estonian Cyberassault

- Strong technological society
- Followed protests in which one person was killed and several injured
- Attack not large, but target was small
- Estonia closed itself off from the wider Internet
- General consensus is that it was not a military attack, due to the style

Stuxnet

An unusually sophisticated worm.

- Utilises zero-day exploits in Windows
- Fraudulent authentication certificates
- Seeks out Programmable Logic Controllers (specifically Siemens) - industrial controllers for electromechanical devices
- Speculation that it was targeted at nuclear assets
- Majority of infection in Iran (Symantec)
- Uses fingerprinting, apparently to target a specific system
- Designed to cause catastrophic physical failure
- “..mischief or financial reward wasn't its purpose, it was aimed right at the heart of a critical infrastructure.” - Lumension IT Security

Defensive Measures

- Common sense & Awareness
 - Software updates
 - Physical access
 - Data authentication
- Using open source platforms
- Antivirus
- Firewalls & Routers
- Intrusion Detection Systems (IDS)

The Future

- Attacks can be economically and tactically significant to an entire nation.. and the world?..
- Attacks will get more specific - there are many kinds of embedded system and many of them are turning into fully-fledged computers
- Continuingly increasing awareness and security will force novel methods of attack

Conclusions

- Undeniable military and political motivations
- Power is in the hand of individuals
- There is money to be made
- There's as much potential for abuse and misuse as for growth and advancement

Resources

- Bob Gourley - Open Source Software and Cyber Defense
- <http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>
- <http://www.direct.gov.uk/nationalsecuritystrategy>
- <http://tools.ietf.org/rfc/rfc4732.txt>
- <http://schneier.com/blog/archives/2010/10/stuxnet.html>
- <http://www.avast.com/virus-monitor>
- <http://atlas.arbor.net/summary/dos>
- <http://news.bbc.co.uk/1/hi/business/6298641.stm>
- <http://www.bbc.co.uk/news/technology-11388018>
- <http://www.governmentsecurity.org/>
- <http://www.shadowserver.org/>
- <http://news.bbc.co.uk/1/hi/8489265.stm>