Kim Jong-il and me:

How to build a cyber army to attack the U.S.

Charlie Miller

Independent Security Evaluators

cmiller@securityevaluators.com

Overview

- About me
- Some background material
- Key strategies
- Cyberwar potential attacks
- Cyberarmy tasks
- Possible defenses
- Layout of army
- Timeline of preparation and attack
- Conclusions and lessons learned

About this talk

- Originally given at Conference for Cyber Conflict, at the NATO Cooperative Cyber Defense Centre of Excellence
- The audience was some technical, some policy types
- This version is a little more technical (and hopefully funny)

Who I am

- PhD in Mathematics, University of Notre Dame
- 1 year, Security Architect, a Financial Services firm
- 5 years, NSA Global Network Exploitation Analyst
- 4 years, consultant for Independent Security Evaluators
  - Application and network penetration testing
  - Project planning and scoping
- First remote exploits against iPhone, G1 Android phone
- 3 time winner Pwn2Own competition

My career as a govie

- Bullets from my NSA approved resume
  - Computer Network Exploitation
    - Performed computer network scanning and reconnaissance
    - Executed numerous computer network exploitations against foreign targets
  - Network Intrusion Analysis
    - Designed and developed network intrusion detection tools to find and stop exploitation of NIPRNET hosts, as well as locate already compromised hosts

Why I gave this talk

- Those in charge of “cyber” policy don’t understand technical details
  - Sometimes the details matter
  - Clarke’s “Cyberwar” was clearly written by someone who knows nothing about the technological details
- To help those capable of making decisions concerning cyberwar to discern fact from fiction

Basics

For comparison

- US Annual military spending: $708 Billion
- US Cyber Command: $105 Million
- North Korea military spending: $5 Billion
  - North Korean cyber warfare spending: $56 Million
- Iran cyber warfare spending: $76 Million
- *My hypothetical cyber army is a bargain at $49 Million!*

Aspects of Cyberwarfare

- Collect intelligence
- Control systems
- Deny or disable systems
- Cause harm on the level of “kinetic” attacks

Some statistics

- # IP addresses: ~3.7 bil
- # personal computers: ~2 bil
- # iphones worldwide: ~41 mil
- Botnets size:
  - Zeus: 3.6 mil (.1% of personal computers)
  - Koobface: 2.9 mil
  - TidServ: 1.5 mil
  - Conficker: 10 mil+

Botnet

- A distributed set of software programs which run autonomously and automatically
- Group can be controlled to perform tasks
- Individual software running on each system is called a bot

Remote access tool

- Abbreviated RAT
- Program which allows remote control of a device/computer
- Allows attacker to search/monitor host, search/monitor local network, attack other hosts, etc
- Should be hard to detect

0-day, the known unknowns

- A vulnerability or exploit that exists in software for which there is no available patch or fix
- Oftentimes, the existence of this exploit is unknown by the community at large, even the vendor
- Difficult to defend against the attack you don’t know about

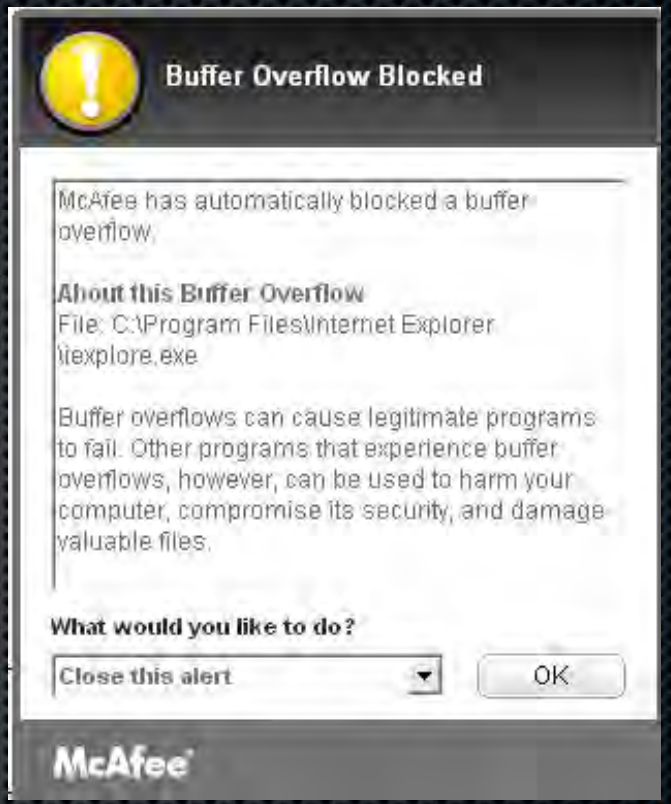
0-days exist

- I found a bug in Samba in Aug 2005. Sold in Aug 2006, Fixed in May 2007
- Adobe JBIG2 vulnerability. Discovered in 2008, Sold in Jan 2009, Discussed in Feb 2009, Patch March 2009
- Found a bug preparing for Pwn2Own 2008. Used it in Pwn2Own 2009. Fixed 2 months later

0-day lifespan

- Average lifespan of zero-day bugs is 348 days
- The shortest-lived bugs have been made public within 99 days
- The longest lifespan was 1080 days
  - nearly three years.
- From: Justine Aitel, CEO Immunity (from 2007)

0-day detection



- Possible but extremely difficult
- Tend to lead to false positives
- Can be circumvented if defenses are known

Overall Strategies

- Dominate cyberspace
- Infiltrate key systems in advance
- Rely on research and intelligence gathering
- Use known exploits when possible, 0-days when necessary

Hack the Planet

- “Dominate cyberspace”, i.e. control as many devices around the world as possible
- In a cyberwar, portions of the Internet will be degraded. Controlling lots of devices increases ability to still act
- Makes attribution easier for your side, harder for opponent
- Sometimes you find yourself inside hard targets by luck
- Many basic attacks work by using many hosts and are more effective with more hosts

Advance Planning

- Attacking well secured networks requires research and planning, it cannot be done overnight
- Many offensive capabilities (communication, scanning, etc) are easily detected if performed quickly, not if performed slowly
- Can be prepared to disable/destroy key systems when needed

Research and Intelligence

- How are key financial and SCADA systems and networks constructed?
- What hardware/software do core Internet routers, DNS servers utilize?
- What defenses and monitoring systems are in place?

To 0-day or not

- Sometimes, especially during early stages, it makes sense to look like an average attacker
  - Use known vulnerabilities, known tools
  - Harder to attribute to military
  - inexpensive if caught
- 0-day exploits and custom tools are harder to detect, but if found, are expensive and time consuming to replace

Other strategies to consider

- Clarke’s logic bombs
- Stealing from/paying cyber criminals for access
- Insider backdoors, i.e. employees at MS, Cisco, etc

Potential Cyberwar Attacks

Potential Cyberwar Attacks

- Shut down the Internet
- Take financial markets offline, corrupt or destroy financial data
- Disrupt shipping, air transportation
- Blackouts
- Disable communication within military
- Disable cell phone networks

Cyberarmy tasks

Cyberarmy tasks

- Communication redundancy
- Distributed Denial of Service
- Hard targets
- Core infrastructure
- Attacking air gapped networks

Communication redundancy

- Operators will be geographically distributed
  - Offices throughout the world
  - Multiple offices in target country
- Direct, redundant communication possible to command
  - Modems over phone lines, satellite phones
  - Even without the Internet, attacks against the Internet can be commanded and controlled

DDOS

- Flood target with too much traffic
- Deny DNS, bandwidth to server, server(s) themselves
- Need to control (and coordinate) a large number of hosts to perform this attack
  - BTW, North Korea functions just fine if the Internet goes away

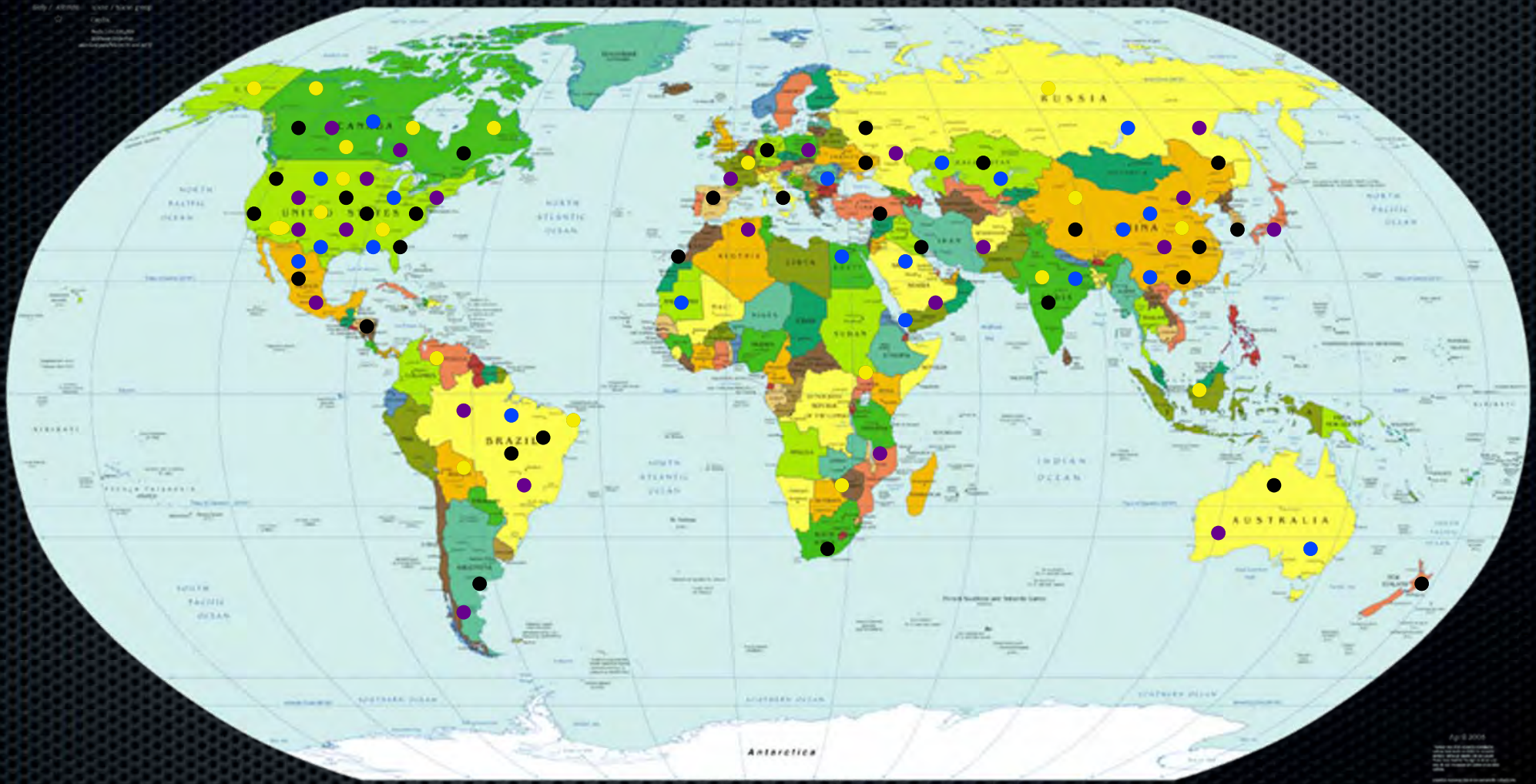
Collecting hosts

- Assume ownership of existing botnets
- Use client side vulnerabilities
  - Browsers, Flash, Reader, Java, etc
- Make some effort to clean up existing malware, patch systems
  - Other botnet masters may try to take your bots
- Use only known vulnerabilities
  - Don’t waste the 0-days, unless you have extras

The N. Korean Botnets

- Want to avoid “string which unravels all”
- Develop a large number of different varieties of bot software
- Avoid central control
- Bots should be geographically diverse
  - Saturated in target country
  - Regionally diverse in target country
- at least 100x bigger than largest botnet seen

Multiple botnets with diversity



Hard Targets

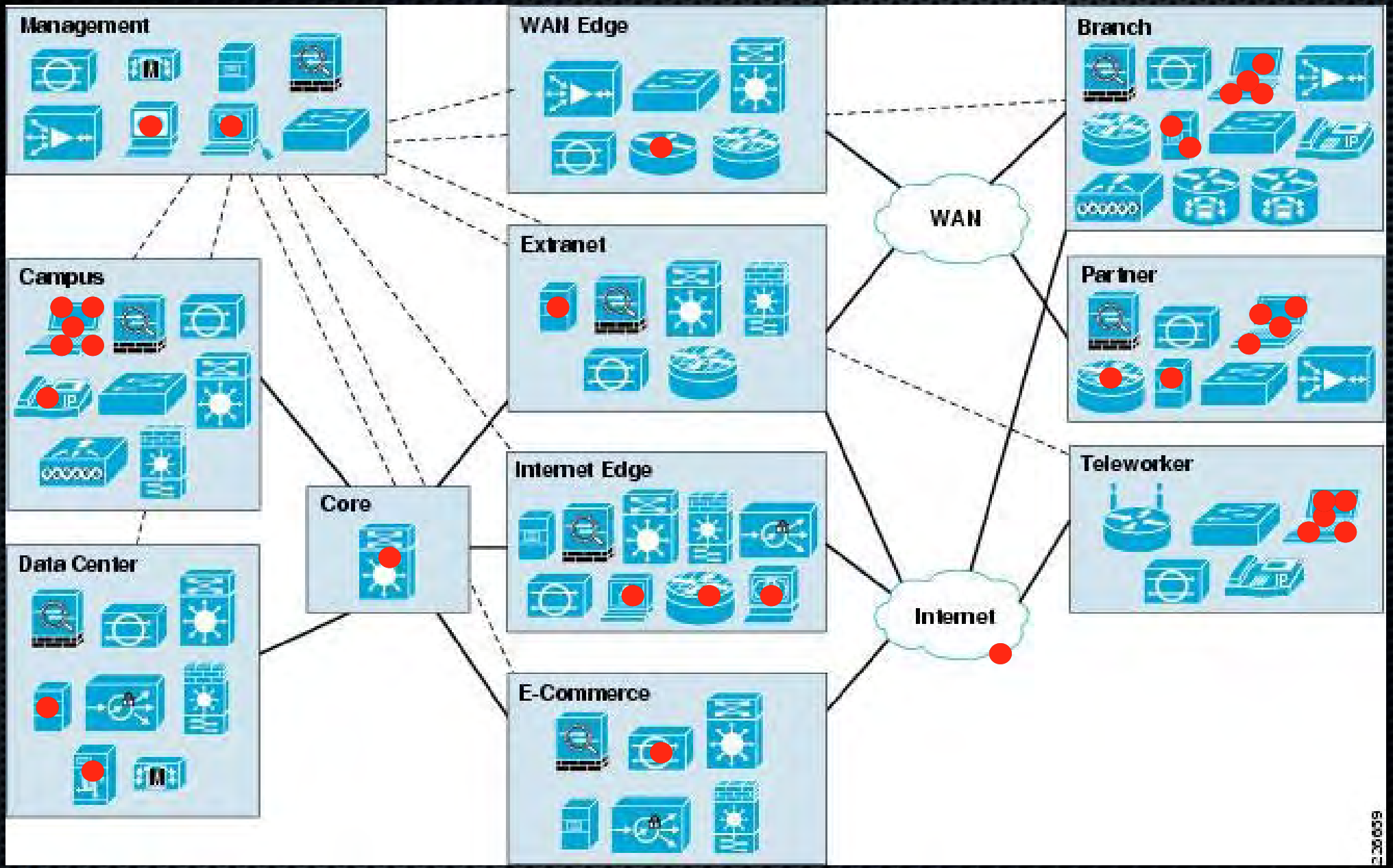
- “Hard” targets
  - Large corporations
  - Banking and Financial Services
  - Air traffic controls
  - NIPRNET
- Employ multiple security mechanisms, many distinct security regions in network, dedicated security teams
- Botnet size figures suggest there are no “hard” targets!

Attacking Hard Targets

- Need a dedicated, patient attack. Pentesting 101
- Step 1: get a foothold
  - Research target network and users
  - Can track victims with GSM information (SOURCE Boston talk)
  - Examine social networks of users
  - Get inside help, infiltrate or buy access
  - Send targets emails with malware/links to 0-day exploits
  - Maybe you already control some trusted nodes via the botnet

More Hard Targets

- Spread
  - Record keystrokes, sniff packets, map network, analyze intranet services
- Slowly take over the entire local network
  - Learn how they make changes, what intranet sites they use, monitor emails, crack all passwords
  - Use client side attacks, observe VPN, SSH usage
  - Install RATs on systems, different RATs for different hard targets
- Become so-called “Advanced Persistent Threat”


Management
WAN Edge
Branch
WAN
Extranet
Campus
Partner
Core
Internet Edge
Teleworker
Data Center
Internet
E-Commerce
229039

Core Infrastructure

- Targets: Core routers, DNS servers
- Attacks
  - DDOS
  - Poisoning routing tables
  - Gain access via “hard target” approach
  - DOS attacks against vulnerabilities in routers, servers
    - Cisco IOS, JunOS, BIND, MS DNS

Air gapped systems

- The most secure systems are “air gapped” from the Internet (or at least are supposed to be)
  - DOD TS//SI network
  - Electric power grid
  - Air traffic control?
- These can still be remotely attacked, but difficult
  - JWICS was compromised by USB

Un-airgapping

- The easiest solution is to put these networks back on the Internet
- Have an operative stick a 3g modem and a RAT on a computer/device on the network
  - ...or add a whole new device to network
  - Or a satellite phone
  - Or a modem over existing phone lines
    - if tempest shielding is a problem

Cyberwar defenses

Cyberwar Defenses

- Target country can take defensive actions during or in advance to a cyber attack
  - Segregation (i.e. disconnect from the Internet)
  - Deploy large scale IDS/IPS systems
  - Akami-like DOS protection of critical systems
  - Airgap sensitive networks

Segregation

- Target country can isolate itself from the Internet to protect itself from foreign attack
- Country may install aggressive filters on foreign inbound traffic
- By positioning botnet hosts and making operations in-country, the attack can still occur

Filtering

- Target country may use filtering on Internet traffic
  - IDS, IPS, etc
- All botnet clients and their communications are custom written, so no signatures will exist
- All RATs and their communications are custom written, so no signatures will exist
- Redundancy of bots and RATS ensure if one is detected, attack can continue from remaining ones

Akami-like defenses

- Akami works by mirroring and caching content in multiple, physically diverse locations
- Akami delivers content close to the requester
- Target may use Akami itself, or develop similar approach to try to stop DDOS attack against critical infrastructure
- Our botnet is physically diverse so will have many nodes close to each Akami server
- Our botnet should be large enough to overwhelm even distributed service

Airgapped systems

- Target country may physically separate critical infrastructure (utilities, financial networks, military systems)
- Some systems cannot be airgapped (e-commerce)
- In advance, we try to un-airgap the systems we target

The Cyberarmy

- Job roles
- Numbers and cost per role
- Equipment
- Total cost

Job roles

- Vulnerability Analysts
- Exploit developers
- Bot collectors
- Bot maintainers
- Operators
- Remote personnel
- Developers
- Testers
- Technical consultants
- Sysadmins
- Managers

Vulnerability analysts

- Bug hunters, find vulnerabilities in software via fuzzing and static analysis
- Need to be world class, hard to “grow” this talent
- Try to hire up all the best people
- Find bugs in client side applications (browsers) as well as servers (DNS, HTTP) and networking equipment, smart phones
- Find bugs in kernels for sandbox escape and privilege escalation
  - As needed, exploitable or DOS bugs

Exploit developers

- Turn vulnerabilities into highly reliable exploits
  - For both 0-day and known vulnerabilities
- This used to be easy, but now takes a tremendous amount of skill
- Will need to be able to write exploits for various platforms: Windows, Mac OS X, Linux
- Will need to be able to defeat latest anti-exploitation measures, ALSR, DEP, sandboxing

Bot collectors

- Responsible for using client side exploits to take over and install bots on as many computers and devices as possible
- Mostly use exploits based on known exploits, some 0-day usage
- Deliver exploits via spam, advertising banners, malware
- Maintain and monitor exploit servers

Bot maintainers

- Collection of bot machines will constantly be changing
  - Some will die, be reinstalled, etc
  - Others will be added
- Monitor size and health of botnets, as well as geographic diversity inside and outside target country
- Test botnets
- Make efforts to maintain bots by keeping the systems on which they reside patched, removing other malware, if possible

Operators

- Actively exploiting hard targets (elite pen testers)
- Advanced usage of exploits, mostly 0-day
- Need to understand entire target network and be able to passively and actively scan and enumerate network
- Install RATs, monitor keystrokes and communications to expand reach in network

Remote personnel

- Responsible for setting up operations around the world
- Getting jobs, access to airgapped systems
- Installing, monitoring, and testing un-airgapping devices

Developers

- Need to develop a variety of bots with differing communication methods
- Need to develop a variety of RATs
- Develop tools to aid other personnel
- Requires user and kernel level development on a variety of platforms

Testers

- Test exploits, RATs, and bots for functionality, reliability
- Run all tools/exploits against a variety of anti-virus, IDS, IPS, to ensure stealth

Technical consultants

- These are experts in various domain specific and obscure hardware and software systems
  - SCADA engineers
  - Medical device experts
  - Aviation scheduling experts
  - etc

Sysadmins

- Keep systems running, updated
- Install software, clients and target software
- Manage test networks and systems

Number and Cost per role

- Vulnerability Analysts
- Exploit developers
- Bot collectors
- Bot maintainers
- Operators
- Remote personnel
- Developers
- Testers
- Technical consultants
- Sysadmins
- Managers

Some info about costs

- I only factor in hardware, software, and personnel salaries
- I do not include
  - Building rent, utilities, travel
  - support staff: Electricians, janitors, guards...
  - “Spys”
  - Intelligence analysts
  - Health insurance, retirements, other benefits

Some risk in this job

- I pay slightly inflated salaries to compensate for this risk
- Could start many small companies (or contract out to existing companies) such than no one group knew what was going on
  - Plus this is better opsec, if all the sudden all known security researchers disappeared, people would get worried!

Vulnerability analysts

- Level 1: 10
  - Well known, world class experts
  - $250,000/yr
- Level 2: 10
  - College level CS majors
  - $40,000/yr
- Total: $2,900,000

Exploit developers

- Level 1: 10
  - World class experts: devise generic ways to beat anti-exploitation, write exploits
  - $250k
- Level 2: 40
  - Prolific Metasploit contributors: write exploits
  - $100k
- Level 3: 20
  - College level CS majors
  - $40k
- Total: $7,300,000

Bot collectors

- Level 1: 50
  - BS or Masters in CS
  - $75k
- Level 2: 10
  - College level CS majors
  - $40k
- Total: $4,150,000

Bot maintainers

- Level 1: 200
  - BS in CS
  - $60k
- Level 2: 20
  - CS majors
  - $45k
- Total: $12,900,000

Operators

- Level 1: 50
  - Experienced, skilled penetration testers
  - $100k
- Level 2: 10
  - CS Majors
  - $40k
- Total: $5,400,000

Remote personnel

- Level 1: 10
  - Experienced spys
  - Pay comes from spy agency
- Level 2: 10
  - CS Majors
  - $40k
- Total: $400,000

Developers

- Level 1: 10
  - Experienced Kernel developers
  - $125k
- Level 2: 20
  - BS in CS
  - $60k
- Level 3: 10
  - CS Majors
  - $40k
- Total: $2,850,000

Testers

- Level 1: 10
  - BS in CS
  - $60k
- Level 2: 5
  - CS Majors
  - $40k
- Total: $800,000

Others

- Technical consultants
  - 20 at 100k fee
  - $2mil
- Sysadmins
  - 10 at 50k
  - $500,000
- Managers
  - 1 for every 10 people, 1 for every 10 mangers
  - 52 managers (@100k), 5 senior managers (@200k)
  - $6.2mil

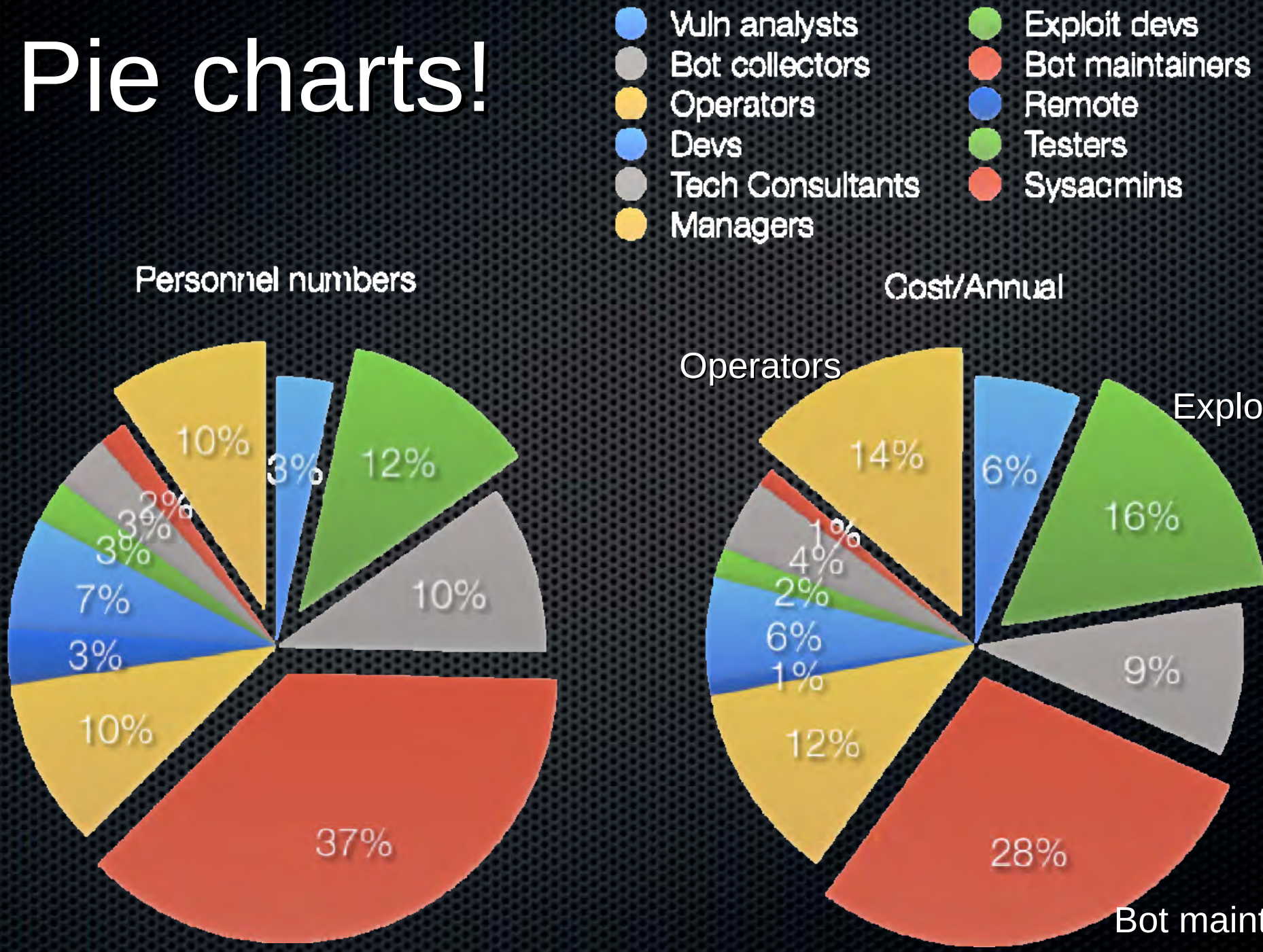
Equipment

- Hardware
  - Average of 2 computers per person
  - Exploitation/Testing lab with 50 computers, variety of routers and network equipment, smartphones, etc
- Software
  - MSDN subscription, IDA Pro, Hex Rays, Canvas, Core Impact, 010 editor, Bin Navi, etc
- Remote exploitation servers
  - Eh, we'll just use some owned boxes

The army

- 592 people
- $45.9 mil in annual salary
  - Average annual salary $77,534
- $3 mil in equipment

Pie charts!


Vuln analysts
Bot collectors
Operators
Devs
Tech Consultants
Managers
Exploit devs
Bot maintainers
Remote
Testers
Sysacmins
Personnel numbers
10%
3%
12%
2%
3%
3%
7%
10%
3%
10%
37%
Cost/Annual
Operators
Exploit dev
14%
6%
16%
1%
4%
2%
6%
1%
9%
12%
28%
Bot maintiners

A 2 year projection

First 3 months

- Remote personnel set up stations
- Remote personnel try to get jobs in financial industry, airlines, and electrical/nuclear industries, join military
- Vulnerability analysts start looking for bugs
- Exploit developers write and polish (known) browser exploits for bot collection
- Developers write bot software, RATS
- Hard targets identified and researched

Months 3-6

- A couple of exploitable 0-days and some DOS bugs are discovered
- Exploit developers begin writing 0-day exploits
- Bot collection begins
- Hard targets research continues, social networks joined, emails exchanged, “trust” established

Months 6-9

- With 0-days in hand, hard target beach heads are established
- Bot collection and clean-up continues
  - 500k hosts compromised (a small botnet by cybercriminal standards)
- Remote stations operational, communication redundant
- Developers writing additional bots and tools

After 1 year

- Control over some systems in hard targets
- System of bots continues to grow
  - 5 million hosts (large botnet by cybercriminal standards)
- 0-day exploits available for many browser/OS combinations, some smartphones
- Inside access to critical military, financial, and utilities achievied

1 year 6 months

- Most hard targets thoroughly compromised
  - It would be hard to ever lose control over these networks, even if detected
- System of bots continues to grow
  - 100 million hosts
- 0-day exploits available for all browser/OS combinations, DOS conditions known for BIND, many Cisco IOS configurations
- Control of many airgapped systems

2 years

- All hard targets thoroughly compromised
- System of bots continues to grow
  - 500 million hosts (20% personal computers), many smart phones
- Airgapped and critical systems thoroughly controlled

Attack!

- Financial data altered
- Military and government networks debilitated
- Utilities affected, blackouts ensue
- Ticket booking and air traffic control systems offline
- DOS launched against root DNS servers
- BGP routes altered
- Phone system jammed with calls from owned smartphones
- North Korea wins!

Conclusions

Lessons learned

- With some dedication, patience, and skilled attackers there is not much defense that is possible
  - It’s an offensive game, although perhaps I’m biased
- Its more about people than equipment (94% of my cost is for salaries)
- Taking down the target’s Internet without taking down your own would be harder but possible (not a problem here)

Lessons learned (cont)

- A lot of talk concerning software and hardware backdoors in the media
  - North Korea can’t easily do this, and this attack suffers from being hard to carry out and largely unnecessary
- Cyberwar is still aided by humans being located around the world and performing covert actions
  - Can’t have all the cyber warriors in a bunker at Fort Meade

What about defense?

- Defender can use the buildup period to try to detect and eliminate cyberwar presense
- Best defense is to eliminate vulnerabilities in software
  - Best way to do that is to hold software vendors liable for the damage caused by the vulnerabilities in their software
  - Currently there is no financial incentive for companies to produce vulnerability free software
  - Building in security costs them money and doesn’t provide them anything in return

Thanks to

- Early draft readers
  - Dino Dai Zovi
  - Dave Aitel
  - Jose Nazario
  - Dion Blazakis
  - Dan Caselden
- Twitter people who gave comments

Questions?

- Contact me at cmiller@securityevaluators.com