Botnet Detection Using Honeypots

Kalaitzidakis Vasileios

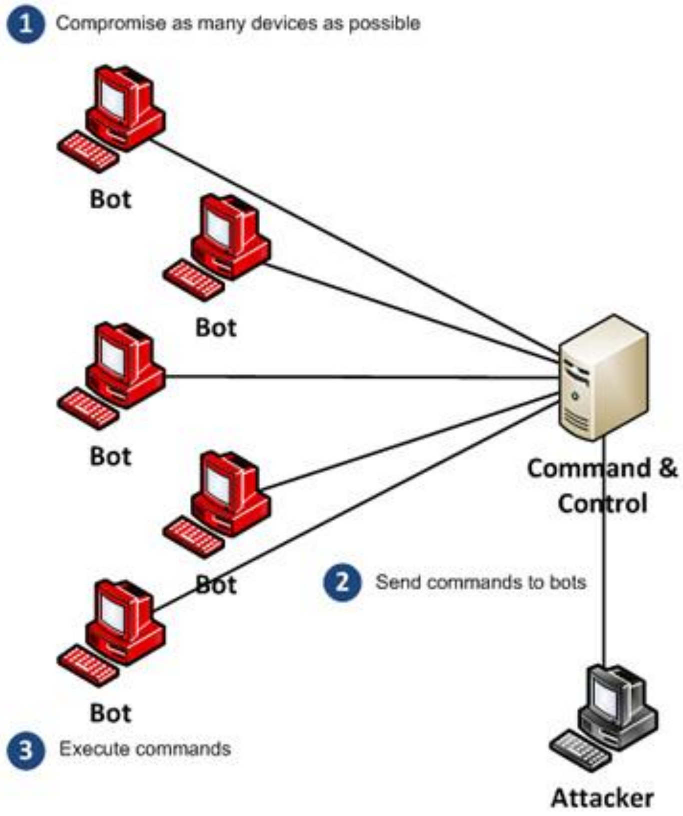
Athens, June 2009

What Is Botnet

- A Botnet is a large number of compromised computers, controlled by one or more Command-and-Control Servers, the Botmasters
- Ro**Bot Net**work also called "zombie army”
- The history of botnets began in 1999:
  - The first IRC Bot, Pretty Park worm, appeared
- Botnets are used for:
  - Distributed DoS Attacks
  - Spam
  - Identity Theft
  - Click Fraud
  - Virus propagation
  - …
- Rising Underground Economy

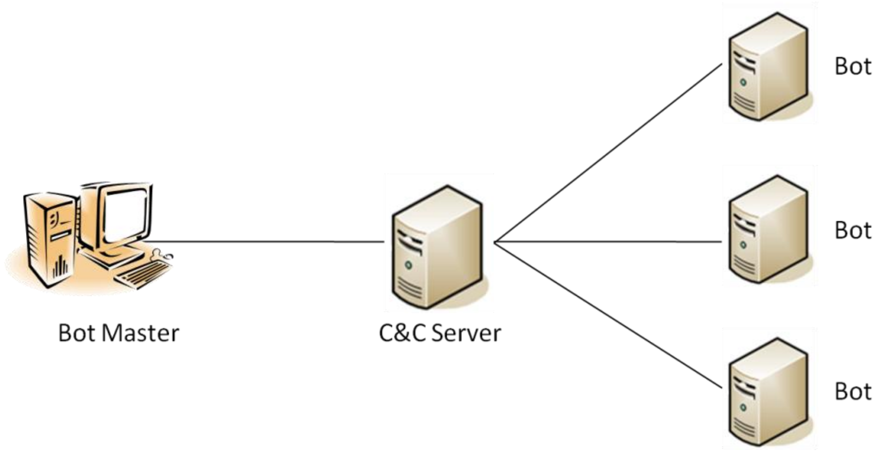
How Do Botnets Work

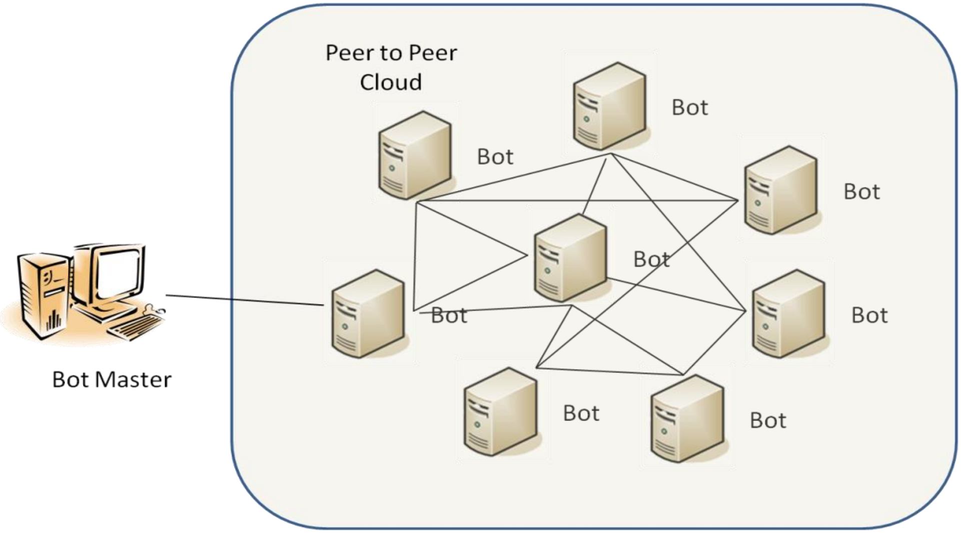
- Installation of malicious software
  - Exploitation
  - Download infected files (P2P, malicious sites, email attachments)
- The infected machine contacts the BotMaster for a mission
- Botmaster sends back mission information
- Bot executes mission and returns results
- Bots can periodically be updated



Botnet Architectures

- Centralized
  - All computers are connected to a single C&C center
  - The most widespread type
  - Easier to deploy
  - Single point of failure
  - IRC, IM
- Decentralized
  - P2P botnet
  - Commands are transferred from bot to bot
  - Botmaster needs access to at least one bot
- Hybrid / Random
  - Theoretical

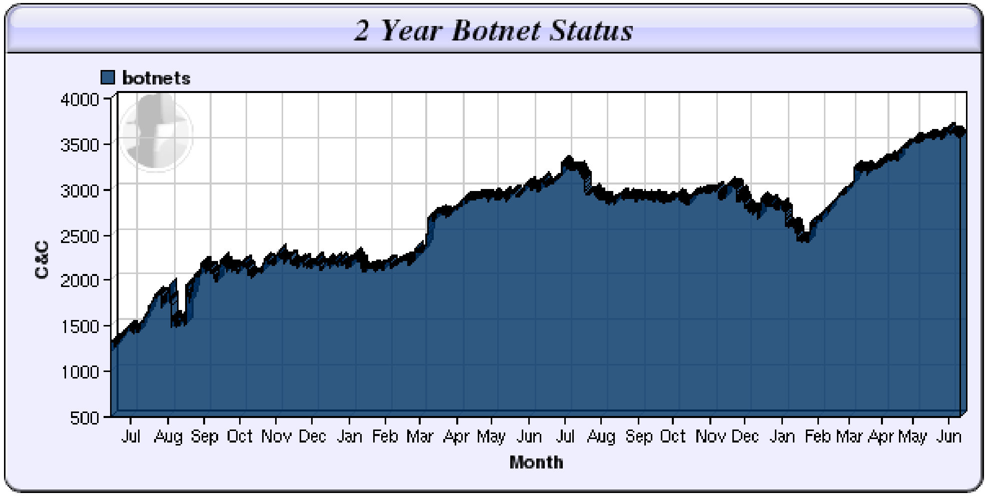


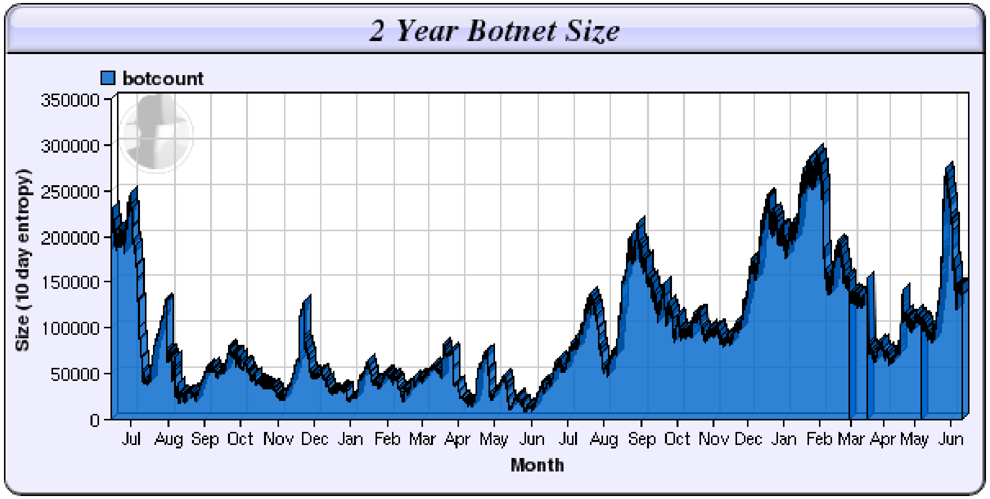


Growing Internet Threat

According to

- Symantec:
  - 1,656,227 new signatures in 2008
  - 165% up from last year
- ShadowServer:
  - Botnets are growing
  - Botnet size is also growing


2 Year Botnet Status


2 Year Botnet Size

Detection Techniques Taxonomy (1)

- Host-based detection
  - Antivirus Programs
  - Log Files Investigation (Administrator should periodically examine Logs)
  - Log Files Correlation (Log files size correlation between different hosts)
  - Monitoring function calls (Keylogging activities, *GetKeyboardState* or *GetAsyncKeyState, WriteFile, outgoing traffic)*
- Network-based detection…
  - IP Headers inspection
    - Monitoring DNS traffic to C&C domains
    - Non-SMTP-server sending emails (spam)
    - High rates of TCP or UDP connections (bots using P2P networks)

Detection Techniques Taxonomy (2)

- …Network-based detection
  - Payload inspection
    - C&C traffic (known commands)
    - Propagation or attacks (exploit code)
  - Signature-based detection (IDSs)
    - Malicious flow patterns
  - Anomaly-based detection
    - Abnormal Behavior (Normal behavior knowledge, Response time, Synchronization)
- Detection Using Honeypots
  - Robots cannot easily identify victims from honeypots
  - Robots have to send noticeable traffic

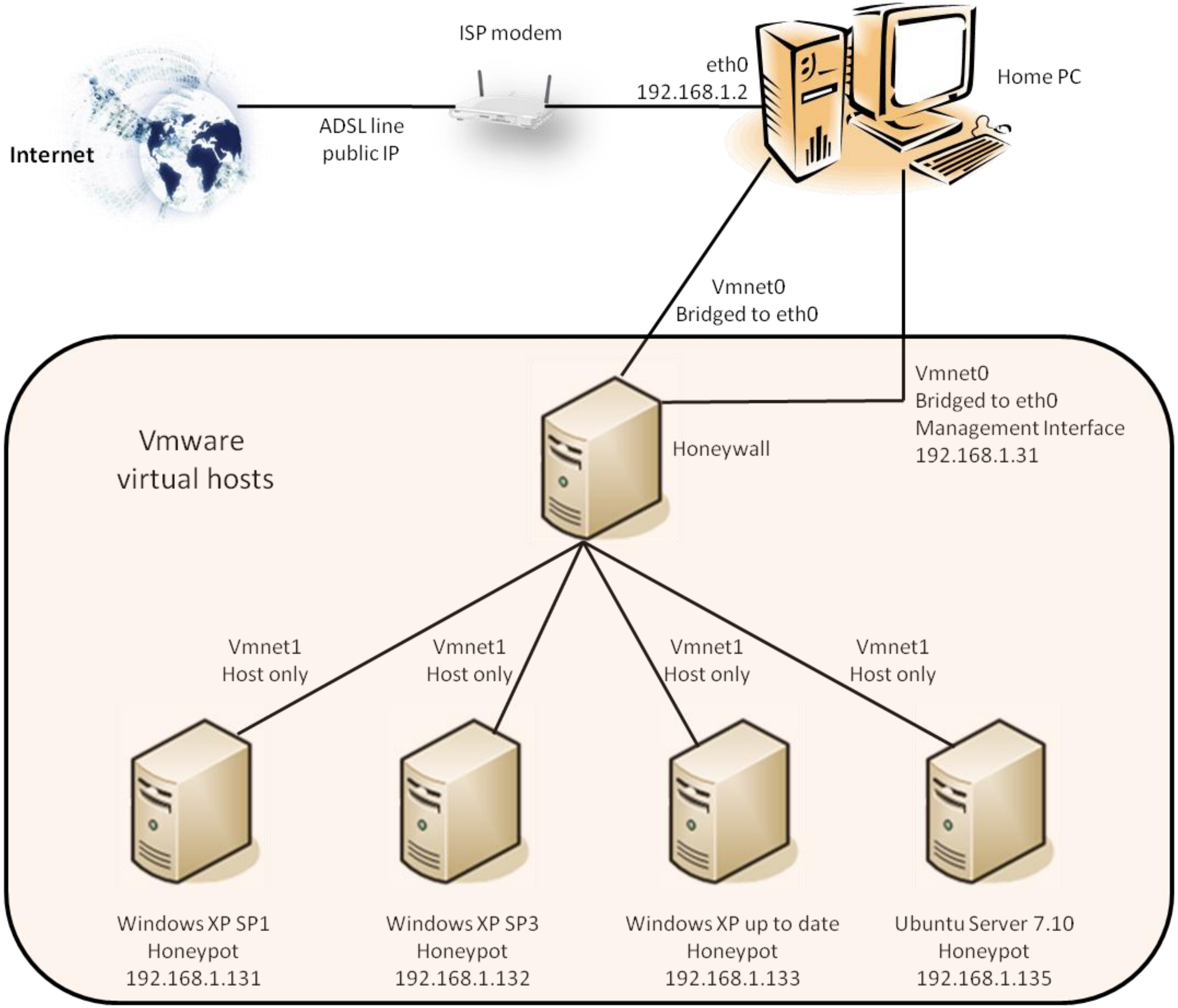
Honeypot Technology

- Honeypot: system used to capture attackers activities
  - Low-Interaction
    - emulate services and systems
    - do not offer full access to the underlying system
    - used in production environments
    - Nepenthes, Honeyd, Honeytrap
  - High-Interaction
    - Real operating system
    - full control over the honeypot
    - used in a research role
    - Honeywall CDROM
- Honeynet: network of two or more honeypots for attackers to interact with

Used Tools

- Honeywall CDROM
  - Honeynet Gateway
    - Fedora Core 6
    - Two layer 2 network interfaces
  - Walleye interface
    - Remote administration and data analysis tool
    - Third network interface
- Sebek
  - Kernel level rootkit
  - Client installed on honeypots
  - Server on Honeywall
  - Monitor system processes
- Honeysnap
  - Basic data analysis tool
  - IRC, HTTP, DNS traffic
- Test Bed – Process Monitor
  - Windows XP System Updated
  - Monitor all system activities (file system, registry, processes, network connections)

The Honeynet Deployment



The Honeypots

- Windows XP Professional SP1
  - Default Windows Services
    - Port 135/tcp, Microsoft Remote Procedure Call
    - Port 139/tcp, NETBIOS Session
    - Port 445/tcp, Microsoft Directory Services
- Windows XP Professional SP3
  - Default Windows Services
  - IIS web server v5.1
  - Microsoft SQL server 2005
  - Windows SMTP server
- Windows XP Professional Up To Date
  - Default Windows Services
- Ubuntu Server 7.10
  - OpenSSH server
  - VSFTPD server
  - Username: user / Password: password

Methodology Of Analysis

- Communication Traffic Data
  - Windows XP SP1 & SP3
    - IRC
    - HTTP
    - DNS
    - SMTP
- Outgoing Attacks
  - Windows XP SP1 & SP3
    - Top Destination Ports
    - IP Addresses
- Incoming Attacks
  - Windows XP Up To Date & Ubuntu Server 7.10
    - Top Destination Ports
    - IP Addresses

Data Analysis - Communication

- IRC
  - Ports 1030, 1099, 1828, 1061,1070
  - Over 30 IRC Channels
    - ##russia##
    - irc.priv8net.com
- HTTP
  - File Downloads
    - "GET http://72.10.169.26/ssvc.exe"
    - "GET http://72.10.169.26/ub.exe"
    - "GET http://rsfq.info/demo.exe“
  - XML communication
- DNS
  - 192.168.1.1 & 194.219.227.2 Servers
  - Queries include mail servers
    - justforclickz.com
    - mail.ru
    - yahoo.com

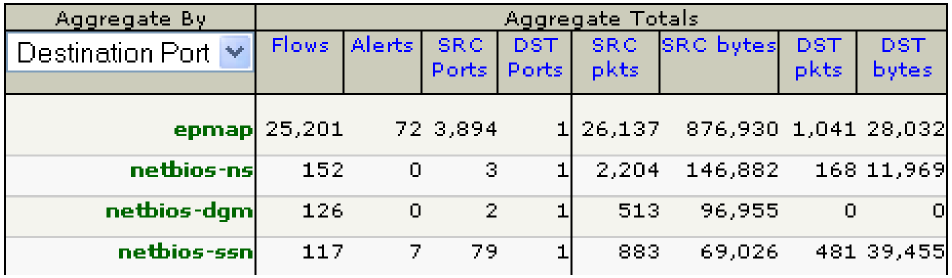
- SMTP

```
220 hotmail.com Kerio MailServer 5.5.0
   ESMTP ready
250 hotmail.com
250 2.1.0 Sender
   <xwfstegxnbo@loughgs.leics.sch.uk> ok
250 2.1.5 Recipient <<nrhy@hotmail.com>
   > ok (local)
354 Enter mail, end with CRLF.CRLF
250 2.0.0
   6f37855f7fcd14d5da0385837a595cab
   Message accepted for delivery
```

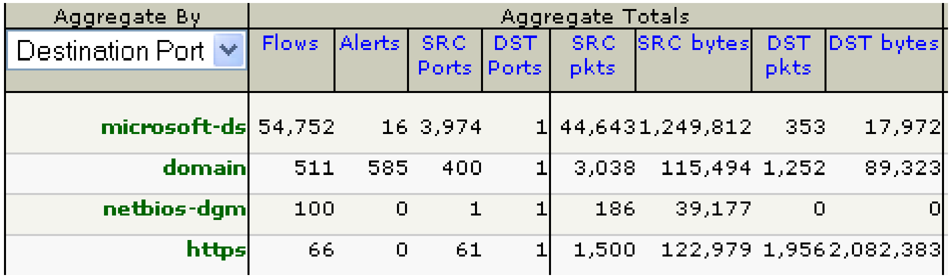
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
 <Results>
  <ip>GET:77.49.137.146,
          POST:77.49.137.146</ip>
  <count>0</count>
  <country>--</country>
  <executed>0</executed>
  <generator>JumboFeed v2.3</generator>
 </Results>
```

Data Analysis – Outgoing Attacks

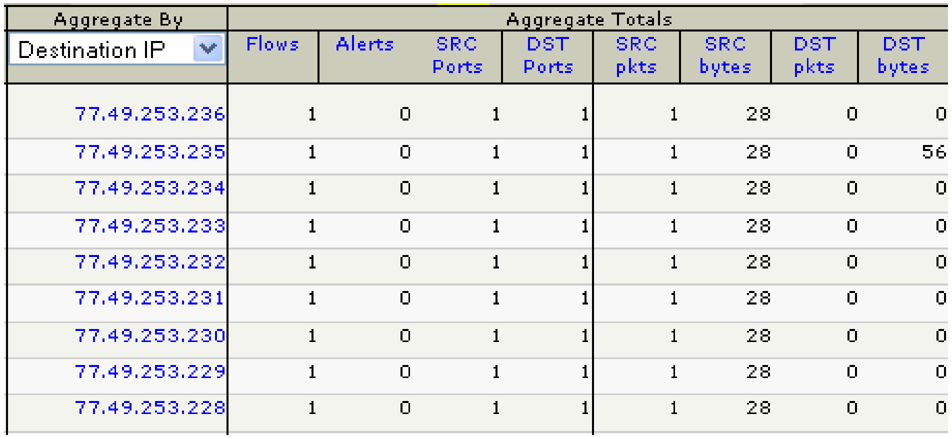
- Top Destination Ports
  - 135 for Windows XP SP1
  - 445 for Windows XP SP3
- Destination Networks
  - ISP’s Network
  - Nat
- Attack Strategies
  - Portsweep at 135,445
- About 20 different processes observed



Aggregate By	Aggregate Totals							
Destination Port	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes
epmap	25,201	72	3,894	1	26,137	876,930	1,041	28,032
netbios-ns	152	0	3	1	2,204	146,882	168	11,969
netbios-dgm	126	0	2	1	513	96,955	0	0
netbios-ssn	117	7	79	1	883	69,026	481	39,455



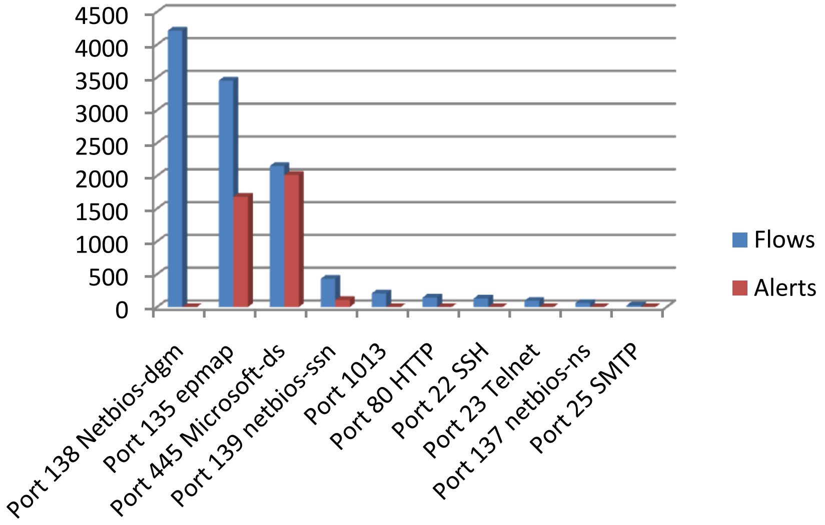
Aggregate By	Aggregate Totals							
Destination Port	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes
microsoft-ds	54,752	16	3,974	1	44,643	1,249,812	353	17,972
domain	511	585	400	1	3,038	115,494	1,252	89,323
netbios-dgm	100	0	1	1	186	39,177	0	0
https	66	0	61	1	1,500	122,979	1,956	2,082,383

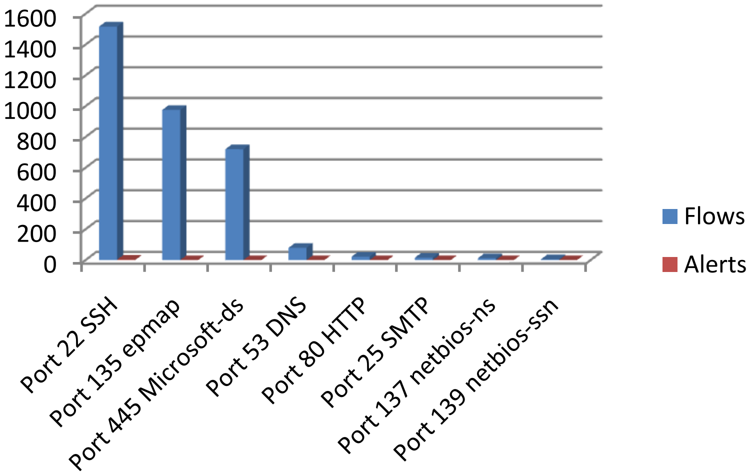


Aggregate By	Aggregate Totals							
Destination IP	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes
77.49.253.236	1	0	1	1	1	28	0	0
77.49.253.235	1	0	1	1	1	28	0	56
77.49.253.234	1	0	1	1	1	28	0	0
77.49.253.233	1	0	1	1	1	28	0	0
77.49.253.232	1	0	1	1	1	28	0	0
77.49.253.231	1	0	1	1	1	28	0	0
77.49.253.230	1	0	1	1	1	28	0	0
77.49.253.229	1	0	1	1	1	28	0	0
77.49.253.228	1	0	1	1	1	28	0	0

Data Analysis – Incoming Attacks

- Top Destination Ports
  - 135, 445,139 for Windows
  - 22 for Ubuntu
- Source IP addresses
  - ISP’s Network
    - 445, 135, 139, 137, 23
  - Global
    - 80, 22, 25
- Attack Strategies
  - Scan and run exploits
    - e.g. 62.1.236.74 → 445, 135, 80
  - Brute force
    - e.g. 61.243.232.120 → 139, 1419 packets
    - e.g. 77.245.148.115 → 22, 5838 packets
- Attack rates
  - 10 -30 per hour for Windows
  - 5-10 per day for Ubuntu





Snort Alerts

- Port 445
  - NETBIOS SMB-DS IPC$ share access
  - NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt
  - NETBIOS SMB-DS srvsvc NetrPathCanonicalize little endian overflow attempt
- Port 135
  - NETBIOS DCERPC NCACN-IP-TCP IActivation remoteactivation little endian overflow attempt
  - NETBIOS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance little endian attempt
- Port 139
  - NETBIOS SMB srvsvc NetrPathCanonicalize WriteAndX unicode little endian overflow attempt
  - NETBIOS SMB repeated logon failure

Main Findings

- Botnets
  - Many active “old-fashioned” botnets, easy to detect
  - Most of bots are single users pcs
- Outgoing Attacks
  - Most of attacks target ports 135 & 445
  - Main attack strategy is port sweep
  - Destinations are ISP’s & Nat networks
- Incoming Attacks
  - Most of attacks target ports 135, 145 ,139, 22
  - Attacks at windows services mostly come from ISP’s network
  - 300 different IPs found within 5 days

Conclusions

- We employed honeynet to study the current attacks employed by botnets
- Our methodology produced clear conclusions
- General
  - A single detection technique is not able to detect all botnets
  - Updating system is a good defense
  - Using honeypot is easy to detect a large number of compromised machines within ISP’s network

Future Work

- Honeynet within ISP's network architecture
  - System consists of a number of honeypots in order to:
    - Capture traffic data
    - Recognize attacks
    - Discover IP addresses of compromised machines
    - Alert users
    - Inform other ISPs using a trust based model

End Of Slides

Thank you!