ARBOR NETWORKS

Botnet Tracking:
Tools, Techniques, and Lessons Learned

Dr. Jose Nazario

Security to the Core. Performance to the Edge.™

About Arbor Networks

- **Founded in 2000**
- **~150 employees worldwide**

- **Peakflow product lines**
  - Peakflow SP for service providers
  - Peakflow X for enterprises
- **Anomaly detection products**
  - Primarily NetFlow-based data collection

- **The global DDoS response leader**

Botnets

- **Pressing problem for network operators**
- **ISPs - number 1 pressing issue**
- **Enterprises**
  - Unknown threat scale
  - Big concern to many

Bots in the Malware Taxonomy

- **Bots exhibit worm characteristics**
  - Use network exploits to propagate
- **Bots exhibit backdoor characteristics**
  - Start up a network listener service, inbound connections
    - FTP server, web server, etc
  - Connect outbound to receive connections
- **Bots utilize rootkits**
  - Rootkits hide their presence
- **Bots have spyware components**
  - Keystroke loggers for information theft

- **Bots are extensible and may download additional software**
- **A botnet herder may load adware and/or spyware on a compromised system**

Botnets in the Internet Underground

- **Bots are distributed computing and resources**
- **Help build a buffer between criminals and victims**
- **Botnets have aggregate storage and bandwidth**
- **Excellent for illicit activities**
  - Spam (increasingly pump and dump)
  - DDoS
  - Warez, stolen media

Know Your Goals

- **Malware Collection**
  - Popular with AV, security companies
- **Attack Traceback**
  - Our primary goal
- **Attack Profiling and Assessment**
  - Small, specialized field

Botnet Tracking Requirements

- **Origins**
  - Can't do this from your desktop!
- **Targets**
  - Botnet server, passwords, bot characteristics, etc
- **Malware**
  - Have to know what a bot would do
- **Client**
  - Have to have a botnet client to participate

Secondary Requirements

- **Distant origins**
  - Don’t want it to tie back to you
- **Multiple origins**
  - Don’t want to be too obvious
- **Familiarity with attacker underground**
  - Exploits, vulnerabilities, underground economy
- **Language skills**
  - Be able to read and write foreign languages

How to Actively Monitor Botnets

Sacrificial Lambs

- **One binary at a time**
  - Repeat for every new bot
- **High risk of participating in an attack**
- **Lower risk of looking "out of place"**

Custom Clients

- **Multiple nets at once**
- **Easy to customize**
- **May look "different" (and hence suspicious)**

This is what we'll use

Botnet Tracking Client Requirements

- Secure
- Scalable
- Flexible
- Easy to retarget
- Records everything it sees
- Stealthy

Project Bladerunner

- **Botnet infiltration**
  - Active monitoring
  - Multiple networks at once
- **Uses Python and irclib module**
- **Also wrote a Kaiten tracking tool**
  - Kaiten affects Linux systems
- **Focused only on IRC-based botnets**

About Bladerunner

- Mimics a basic bot
- Understands "login", "join"
- Chooses to be quiet rather than misspeak

- Logs everything

Why a Custom Bot?

- Time consuming to defang a bot
- Only needed very basic functionality
- Knew code very well
- Little risks (DDoS, installations, etc)

- Bladerunner was about 300 LoC

Which Botnets?

- **Need to know host, nickname format, and passwords**
  - Blacklists, AV writeups insufficient
- **Captured malware**
  - In house analysis
- **Norman Sandbox digest**
  - Back when it was free
- **Link sharing**
  - Strong research community

Botnets and DDoS

- **About half of all botnets we tracked performed DDoS attacks**
  - Most attacks are not against a significant target
  - Most attacks are not crippling to the endpoint
- **Did observe a set of high profile attacks in the spring of 2006**
  - Against a series of anti-spam and anti-DDoS companies
- **DDoS nets use different bots than spyware or adware bots**
  - Not all bots have DDoS capabilities
  - Type of bot used can often indicate intent of herder

Botnet Tracking as DDoS Traceback

- **Looked at DosTracker archive**
  - Arbor project to analyze global DDoS provalence
  - Over 20,000 DDoS attacks measured between Sept 2006 and January 2007
- **Looked at Shadowserver botnet tracking logs of DDoS attacks**
  - Over 21,000 attacks in this timeframe
  - Over 400 unique IRC servers
- **Attack intersection results**
  - 2% of all DDoS attacks measured by Arbor had clear botnet cause
  - 13% of all DDoS attacks recorded by botnet tracking showed up in Arbor monitors

Our Current Position in Botnet Response

- **(Community position)**
- **Collection**
  - Nepenthes or other honeypots
- **Communication**
  - Whitestar list, DA, NSP-SEC, Shadowserver, etc
- **Analysis**
  - Sandboxing (Norman dominates)
- **Tracking**
  - Shadowserver, some private tracking

Where the Botherders Are

- **Source code is widely available**
  - GPL licensed, using CVS!
  - GUI-based configuration, no coding skills needed
  - Bug fixing
    - Compare SpyBot in 2004 and 2006
    - Lots of little bugs fixed: string bounds checks, etc
- **Multiple types of bots**
  - SpyBot, SDBot, Reptile, Agobot, Rbot, RxBot, Kaiten, etc …
  - Lots of overlapping capabilities, not all support DDoS
  - Which codebase you use depends on your intentions
- **Proliferation of spyware, adware provides money**

Where the Botherders Aren't

- **IRC**
  - Too many snoops on IRC
  - Too easy to break into
  - Lots its "elite" factor some time ago
  - Growing number of HTTP, IM, and other bots
- **Web Forums (eg Ryan 1918)**
  - They know these are monitored

We've Peaked!

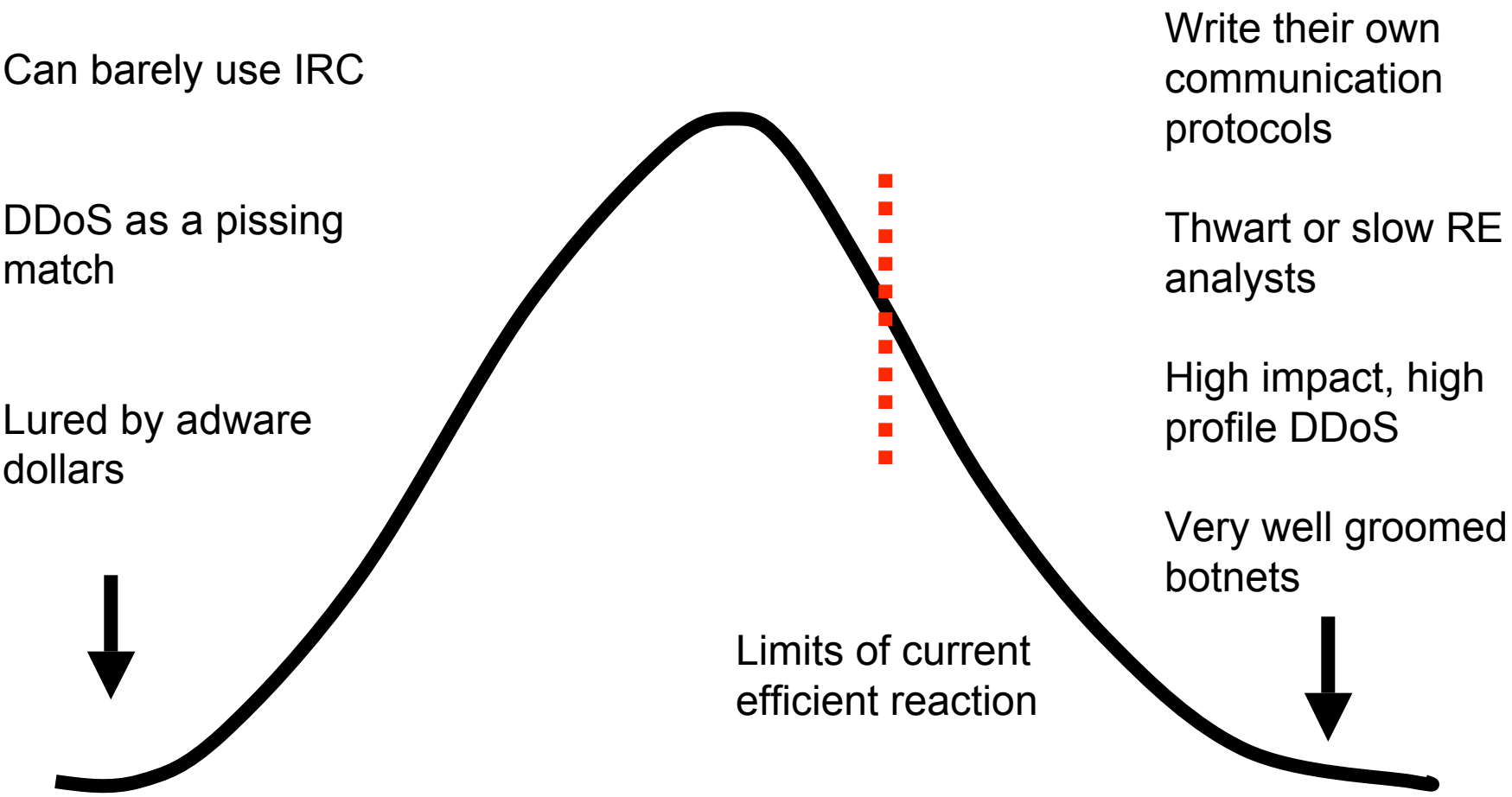
- **This combination reached its peak in early 2006**
- **Good guys**
  - Lots of basic RE analysts
  - Armed with tools like sandboxes
  - Lots of collection networks (ie Nepenthes)
  - Rapidly caught, analyzed, and tracked botnets
- **Bad guys**
  - Explosion in bots and botnets launched
  - Only a few botnet groups were actively thwarting attacks
  - HTTP and P2P bots were not very popular yet (still IRC heavy)
  - Lots of botnets were very visible

- **This confluence meant we peaked**

The Revolt by Botnet Operators

- **More and more bots are defeating the basic techniques**
- **Sandboxes are being defeated**
  - Increased use of debugger checks
  - Delays in revealing useful information
  - Poisoning data
  - Inject fake bots to detect people who mine Norman for data
- **Honeypots and honeynets**
  - Detected or ignored
- **IRC tools**
  - Fingerprinted and blocked, or simply ignored
- **It's all downhill from here!**

The Botnet Herder Ability Curve



Non-Technical Challenges

- **Acting on the data**
  - Takedown, blackhole, etc
  - Becoming facilitated with commercial solutions
- **Speed - getting usable data quickly**
  - Trustworthiness of the data is key
- **Reaction**
  - This is a reactive cycle
  - Need proactive mechanisms

Getting Botnets Taken Down

- **Getting the information in the right hands**
  - Thousands of botnets a week, only so much operators can do
  - Cannot blindly block
- **Focus is on active, high profile DDoS networks**
- **Coordination is a pain in the neck**
  - DNS registrar
  - DNS server network(s)
  - C&C host network(s)
- **Botnet operators can easily stay a few steps ahead**
- **Complement is egress filtering for victims**

Technical Challenges

- **Encrypted communications channels**
- **Defeating rapid analysis techniques**
- **New or custom command languages**
  - HTTP, peer to peer

Encrypted Channels

- **Encryption**
  - Windows “Somelender” bots - homegrown Caesar cipher

```
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG
## :=GoU6jyt7xCuvfRamp+NOAeNFFF/q/h9EHT/H6DV5fxcD7RoX9Pt5a/o2AST9N+j4Y4jf
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG ## :=rvyJWDmfvujXJ4XDKp5
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG ## :=+rhlS+/trmwFfUNtERLa
```

Decrypts to:

```
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG ## :40% ddos tcp
65.77.140.140 6667 900 -s -f -i -2
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG ## :* kill dos
(66.186.35.22:8080) :ckodg!j@tyrant PRIVMSG ## :* kill ddos
```

Fallout from Encrypted Commands

- **Very time consuming**
- **Two options**
  - Mimic bot
    - Must reverse encryption algorithm
    - Must implement
  - Honeypot the bot and monitor it
    - Doesn't scale well
- **This dramatically slows down botnet tracking**

Defeating AV Detection

- **Polymorphism is rare**
  - Achieve polymorphism by simply repackaging bots
  - New or modified packer
  - Fresh compile
  - Bingo, AV fails to detect

- **The bot is just a tool to load the real payload on the box**
  - Spyware, adware, spam tools, etc …
  - The bot code itself can be thrown away once it's gotten the second stage payload on board

Analysis Slowdown

- **Increased use of obfuscated, anti-reversing binaries**
  - Anti VMWare, debugger, sandbox mechanisms available as drop in modules
    - Increasingly popular in 2006
  - Abuse well-known holes in these tools, bot stops working in their presence
  - Thwarts automated analysis, requires a trained human

Anti Analysis Techniques

- **Increased use of rapid analysis thwarting tools**
  - eg Debugger detection
  - Poisoned "wells" (honeypots)
- **Detection and disabling of sandbox tools**
  - Detect VMWare
  - Detect Norman
  - Result: no results
- **Solution: put a human in the loop**

Defeating Sandboxes and Honeypots

```
/* Check if running inside VMWare */
int IsVMWare()
{
        int version=VMGetVersion();
        if(version)
                return TRUE;
        else
                return FALSE;
}

/* Fool ProcDump with increasing size */
void FoolProcDump()
{
        __asm {
                mov eax, fs:[0x30]
                mov eax, [eax+0xC]
                mov eax, [eax+0xC]
                add dword ptr [eax+0x20], 0x2000        // increase size variable
        }
}

/* Screw with Connectix VirtualPC */
#define vpcscreen __asm _emit 0x0F __asm _emit 0x3F __asm _emit 0x01 __asm _emit 0x0C
#define vpcadditions __asm _emit 0x0F __asm _emit 0x3F __asm _emit 0x05 __asm _emit 0x01
```

Defeating Sandboxes

```
Norman Scanner Engine 5.83. 10
Sandbox 05.83, dated  1/01-2006

Your message ID (for later reference): 20060217-1786

7a9aee7b604acdbffa8c891b40845ec5 : Not detected by sandbox (Signat
 [ General information ]
    * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMA
ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
    * Anti debug/emulation code present.
    * File length:       214528 bytes.


(C) 2004-2006 Norman ASA. All Rights Reserved.

The material presented is distributed by Norman ASA as an informat
```

HTTP Bots

- **Two main mechanisms**
  - Phone home (register, poll for commands)
  - Register, await an inbound connection
- **Communication is over HTTP, using URLs**
- **Korgo, Padobot, Bzub, Nuclear Grabber**
- **Example registration URL**
  - `http://XXXXXXXX/index.php?`

```
id=jqkooamqechepsegsa
&scn=0
&inf=0
&ver=19
&cnt=GBR
```

HTTP Bot Implications

- **Harder to spot**
  - No long lived connection
- **Have to know what to look for in URL logs**
  - Hiding in the maelstrom
- **Still uses a central command point**
  - Easy to block
- **Not too hard to lurk**
  - Poll server, understand replies

Peer to Peer Bots

- **Storm Worm (CME-711, January 2007)**
  - UDP-based eDonkey protocol
  - Used to send spam
- **Nugache (Spring, 2006)**
  - Encrypted TCP, custom command protocol
  - No clear use for this network yet
  - Network is still alive
- **Effectiveness: 100,000+ nodes, sustained network**

Peer to Peer Bot Implications

- **Resilient network**
  - No central point to shut down
  - No central point to block
- **Difficult traceback**
  - Network manager can enter network from anywhere

- **Anyone can join network**
- **Reverse protocol, join and lurk**

Changes in Botnet Handlers' Intents

- **Previously**
  - Getting the bot on there was the end goal
  - Keeping the bot on there was important

- **Now**
  - The bot is just to bootstrap new code on there
  - The bigger that window of opportunity is, the better
  - Evade AV detection by staying ahead
  - First seen on a wide scale with Zotob

Success on Their End

- Increased spam volumes
- All attributable to deployed botnets

- High impact DDoS events against high profile crimefighters, antispam groups

- Inter-spam gang fighting

- With success like this, don't expect a slowdown

The Botnet Arms Race

Bad Guys	*Good Guys*
• More bot families	• Behavioral analysis
• More bots	• Sandboxes
• Packers and obfuscators	• Process dump tools
• More botherders	• More analysts
• Leaving IRC behind	• Sacrificial lambs
• Encryption	• Reversing

Then ↓ Now

Scalable ↓ Not

Conclusions

- **Botnets have been a sustained growth industry**
- **Botnet herders have increasingly ditched their "minders" (the good guys)**
- **Botnets are increasingly used for high profile problems and crime**

- **We must work hard to adapt to these new realities and increase our monitoring**
  - Collaboration will be crucial

An Untenable Position

Reactive

Proactive

How do we get from here …..

To here? We must.