

*“They’re just a bunch of  
script kiddies.”*

*Life, Love, and War in the  
Underground*

Rob Thomas [robt@cymru.com](mailto:robt@cymru.com)

5 November 2003

# all about the leet and the lame

- Introduction
- Culture
- Economy
- Love and war
- Some resulting thoughts and Rob finally shuts up

# Introduction

*what's really going on?*

- Despite a surfeit of security firms and “experts,” things only continue to get worse.
- Why packet? Why hack? *Why me?!*
- Malware analysis doesn't always reveal intent or motives, e.g. the “detritus fallacy.”

# Introduction

*what is a society?*

a voluntary association of individuals for common ends; especially : an organized group working together or periodically meeting because of common interests, beliefs, or profession

*Have the miscreants become a society?*

# Culture

## *language*

- It has a name – Eblish.
- Started with “h4x0r” speak.
- Commonly used in AIM and other chat mediums, e.g. lol, lmao, etc.
- “pls to spak eblish here”
- “im4 g0nn4 p4x0r j00!”
- “stfu and gimme ur shell kthx”

# Culture

## *the true open system*

- Newbies are readily accepted.
- Often must prove clue – albeit low clue – to get “in.”
- One 14 year old miscreant had a 200 bot botnet within six months of entering the underground.

# Culture *sharing*

- 0days often released in the underground, but not released publicly.
- Texts and malware routinely shared.
- Community development efforts are common, e.g. the GT Bot and SD Bot.
- Packet for friends and strangers.

*New members are always welcome!*

# Culture

## *helping*

<A> B care to drop an ip? x.x.185.154

<B> u can't drop that A ?

<A> i can't load any ciscos

<A> B can you drop that ip for me?

<B> ICMP : x.x.185.154 , clocked @ 450KB , 32 / 4,000  
roots engaged. Count:9999 @ 14400B/root

<A> thnx B

<B> n/p

<B> A who is that?

<A> some fag on undernet

# Culture

## *denizens*

- Age range is wide – 12 to 50+ in the miscreant crews.
- A small number of xenophobic crews.
- The range of skills and personalities closely mirrors the White Hat community.

# Culture

## *melting pot*

- No clear border between skillz.
- Hacking, carding, packeting, and coding are now facets of the “gem.”
- Continuing merger of worms, viruses, bots, and trojans – W32.Slanper, SD Bot.
- Most crews include members from all across the globe.

*Politics and religion don't interest or bother the community at large.*

# Economy

## *the barter system*

- The shopping mall includes - shells, cc, cvv, roots, 0days, malware, bots, bot code, DoSnets, domains, webs, bounces, DDoS attacks, ciscos, flowpoints, caymans, pay pal accounts, drops, and...**MONEY**.
- Everything can be traded, and everything has a value.
- Increasingly it's all about HARD CURRENCY.

*The underground economy fuels most of the  
miscreant behavior!*

# Economy

*some trades are very common*

<A> some guy is selling the new aim sploit  
for 300\$

<A> i'll card you a calling card for some  
ciscos b4 i go to sleep

<A> will trade .gov roots for ccs

– Verified that the .gov roots were real. ☹

<A> will pay ccs for paxoring pls msg me!

# Economy

*increasingly the trades are for hard cash*

<A> i need 50 roots k ?

<B> k ill send them after u put \$50 in my  
paypal

<A> \$50 ? u can get a lot more shells or ccs  
instead

<B> ya but I can go to the movies with \$50

# Economy

*increasingly the trades are for hard cash*

- \$40K per month.
- Waking up to \$1200 in a PayPal account.
- Botnet for rent, \$5K per year.
- \$100? Bah! \$500 for the latest 0days!
- Get your daily list of wide open proxies for only \$50 per month!
- The new competitive edge.

# Economy

*the players*

- “Just script kiddies.”
- Organized crime.
- Terrorists?

# Economy

## *resource exhaustion*

- The amount of scanning reduces the number of vulnerable “virgin” hosts for any given vulnerability.
- The value of a 0day continues to increase, but *not* exponentially.
- The value of compromised systems continues to increase.

*The race is on!*

# Economy

*caveat hax0r*

- Why purchase what you can steal?
- Rippers are hated and common.
- Many DDoS attacks are the result of bad business deals.

*Be careful where you drop.*

# Love and war

- Being packeted or hacked is a normal part of life in the underground.
- Packeting is ubiquitous. I logged at least 100 DoS attacks in one 24 hour period. This was only within five crews.
- The ubiquity of packeting makes bouncing imperative. One crew went from 0% bouncing to 80% bouncing (using ciscos) in one month.
- Packeting require botnets and DoSnets. This generates the bulk of the hacking activity.

# Love and war

*what causes packeting?*

<A> C: u cant pax0r

<A> u r lame

<B> lol

<C> stfu

<A> no ur a kid

<A> ur mom can pax0r better than u

<A> and she doesn't charge as much

<B> LOL

<C> now u die

# Love and war

## *who are the targets?*

- ***WE ARE!***
- Bouncing miscreants use our routers. Thus, our routers become the targets.
- Bots and botnets are targets – hacked workstations, hacked servers.
- Our networks and devices originate, receive, or transit the scanning, hacking, and packeting.

*Sometimes the attackers are the targets.*

# Love and war

## *30+ eBGP peers and Own3d*

```
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 02-Feb-02 23:19 by dchih
Image text-base: 0x50010968, data-base: 0x521B2000

ROM: System Bootstrap, Version 11.2(20010625:183716) [bfr_112 181], DEVELOPMENT
SOFTWARE
BOOTLDR: GS Software (GSR-P-M), Version 12.0(19)S2, EARLY DEPLOYMENT RELEASE SOF
TWARE (fc1)

    uptime is 9 weeks, 4 days, 4 hours, 31 minutes
System returned to ROM by error - count interrupt never occurred, PC 0x501BDD88
at 04:06:01 UTC Wed May 8 2002
System restarted at 04:16:40 UTC Wed May 8 2002
System image file is "slot0:gsr-p-mz.120-19.S2.bin"

cisco 12008/GRP (R5000) processor (revision 0x05) with 262144K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on

2 Route Processor Cards
2 Clock Scheduler Cards
3 Switch Fabric Cards
1 8-port OC3 POS controller (8 POS).
2 OC48 POS controllers (2 POS).
1 Three Port Gigabit Ethernet/IEEE 802.3z controller (3 GigabitEthernet).
1 Ethernet/IEEE 802.3 interface(s)
3 GigabitEthernet/IEEE 802.3 interface(s)
10 Packet over SONET network interface(s)
507K bytes of non-volatile configuration memory.

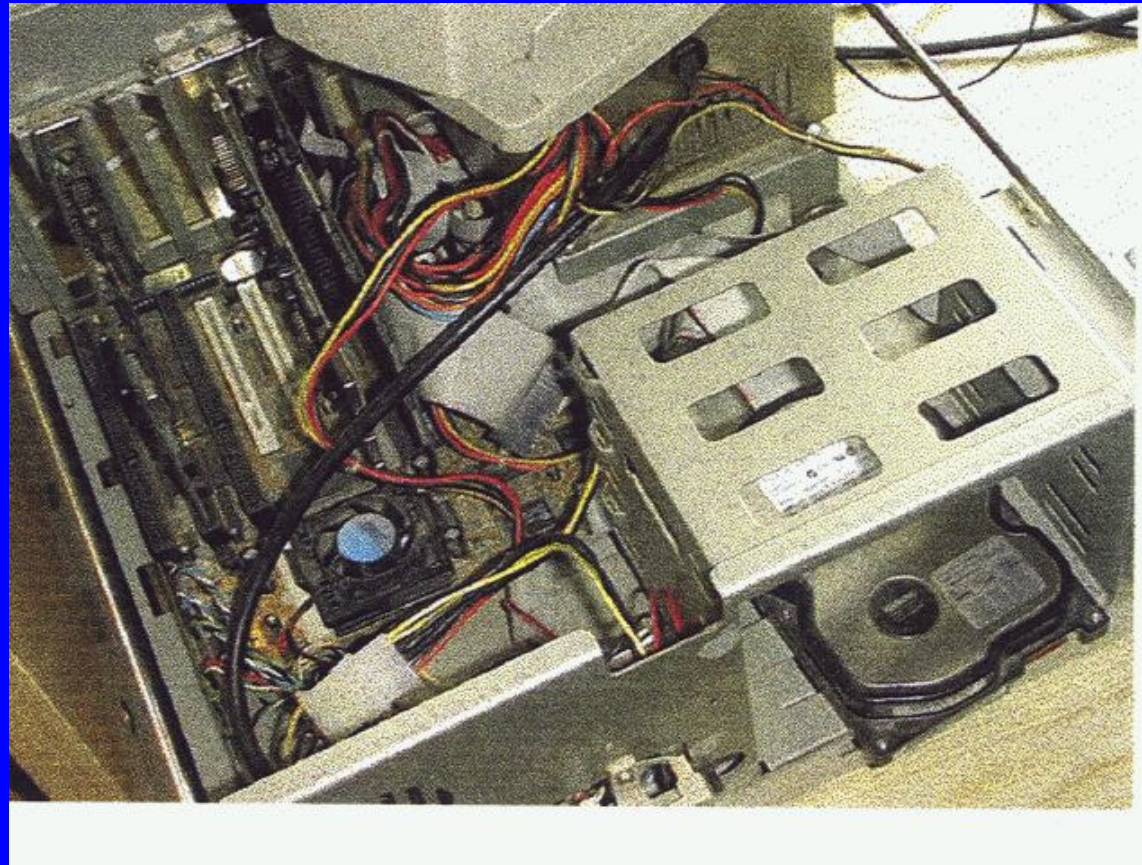
20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

# Love and war

## *the futility model*

- Quad redundant OC-3 links: \$77,500.00/month.
- Redundant firewall cluster with IDS: \$100,000.00.
- Ethical hacking and scanning service: \$1,000.00/IP/month.
- Getting Owned by the machine on the next page...

# Love and war *the futility model*



*...priceless!*

# Love and war

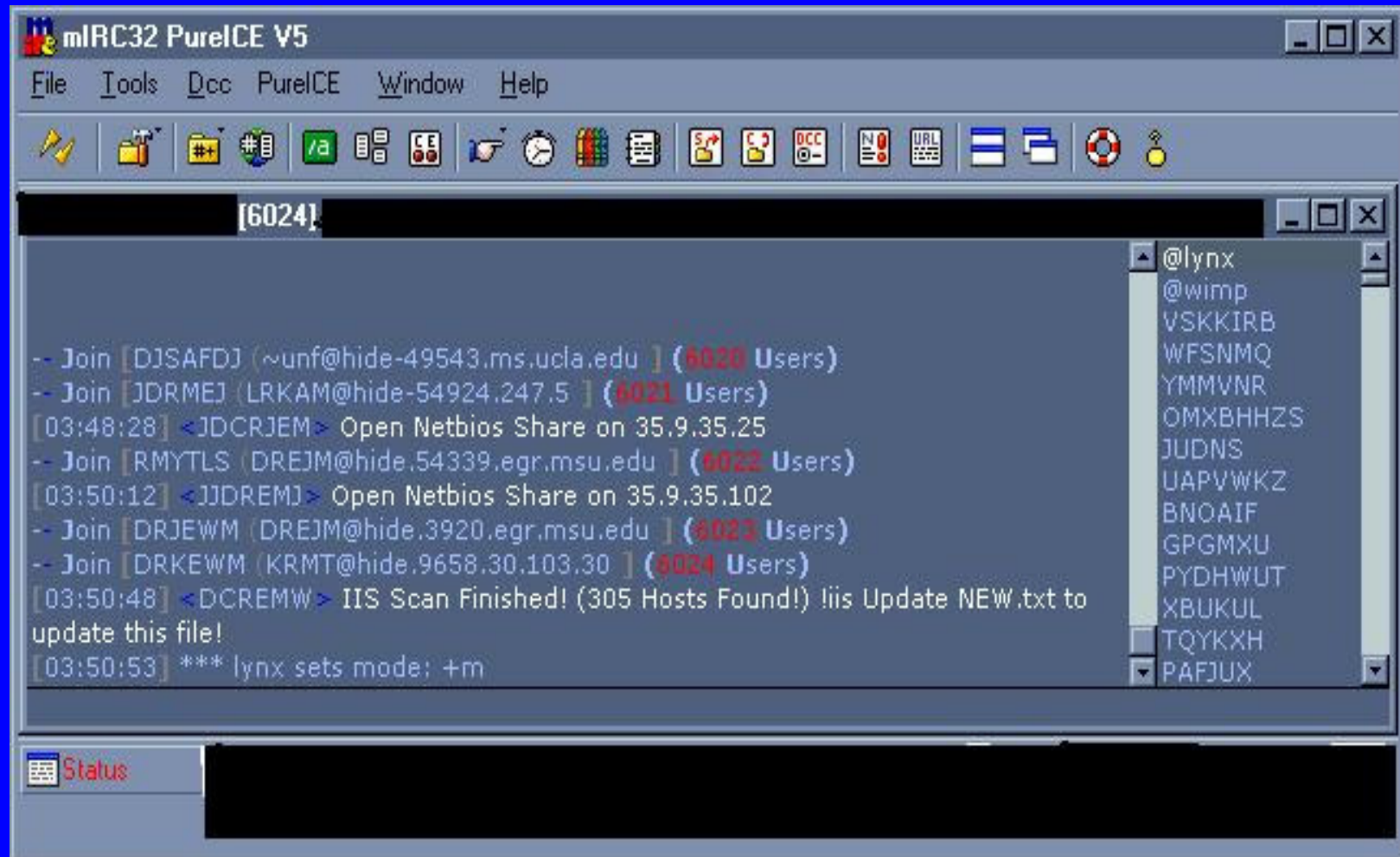
## *bot powa*

- Largest botnet – 140415 bots.
- Largest DDoS attack – 40Gbps aggregated.
- Longest DDoS attack – three years and counting.

*Ouch, ouch, ouch!*

# Love and war

*bots, like rob, never sleep*



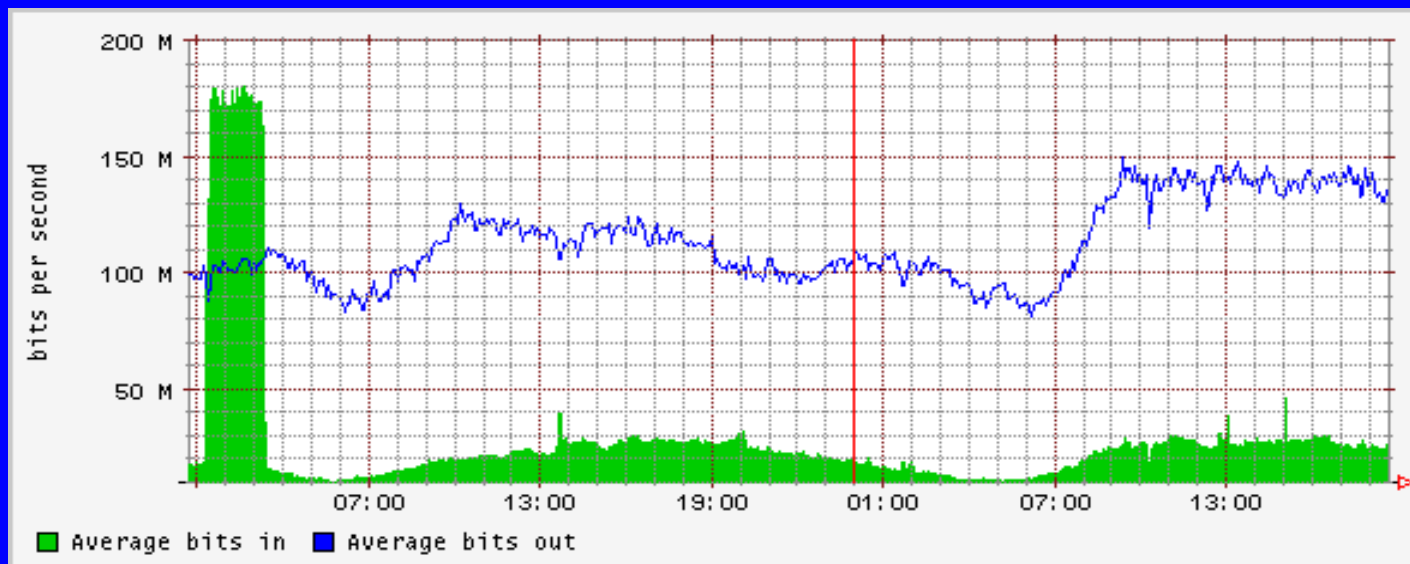
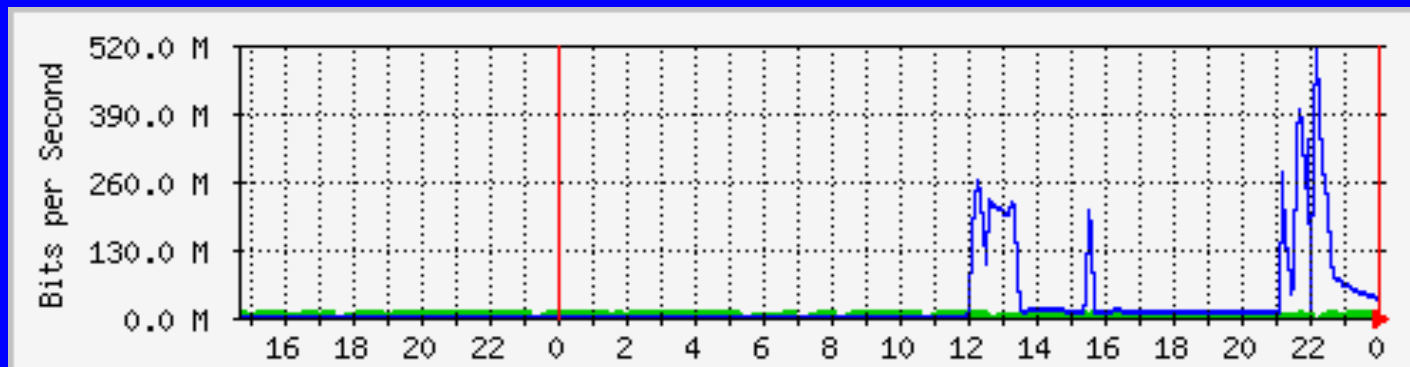
# Love and war

## *the irc attack challenge*

- An IRC server, part of a large public IRC network, target of continuous DDoS attacks.
- Offered an O-line to a miscreant if he could reach 800Mbps in DDoS.
- The miscreant was only able to peak at, and sustain, 792Mbps for a bit under an hour.

***ONLY 792Mbps?!***

# Love and war *feel the burn!*



# Some resulting thoughts...

*We aren't fighting hackers, we are fighting the now outdated philosophy that started the Internet.*

# Some resulting thoughts...

- Internet security is all about “the other guy.”
- The simple things often work quite well.
- Communication and coordination is the key to our success!
- I need more coffee and sleep.

# Thank you!

*Special thanks to CERT Polska!*

robt@cymru.com

www.cymru.com