Digging Up Worms, Herding BotNets

Daniel Medina
Academic Information Systems
Columbia University

Introduction

26 April – 30 April, 2004

Scan and 'sploit via tcp 80, 135, 445, 1025, 2745, 3127, 5000, 6129...

Phatbot variant – malicious bot software, not mindless worm!

- Encrypted, distributed communications back to C&C
- POST to www.stanford.edu, www.rit.edu, nitro.ucsc.edu, others
- Special attention to .edu hosts

```
prints netinfo when the bot is .edu          irc.getedu
makes the .edu bots join channel you want    irc.getedu.join
exec command if bot is an edu                logic.ifedu
```

Overview

Network Overview

Detection

Reporting

Network Overview

Internet2-connected

OC3, to be upgraded this summer

NYSERNet member

Multiple Commodity Providers

ASN: Autonomous System Number, aggregates your subnets

OC3 to Broadwing (AS 6395)

T3 to Qwest (AS 209): upstate campuses and backup link

100 Mbps RCN private peering (AS 6079)

5 /16s networks (aka Class Bs, ~64K addresses), plus some others

Network Overview

ResNet

RHNO (undergraduate dorms), ~5000 students

AptNet (university housing: profs, grad, staff), ~2500 students

Not segregated by any policy

Same Internet connection as the rest of campus

No login, No registration

Been discussed, but our logging is good

Detection

NetFlow

Flow records exported by routers – Ciscos, Junipers, others

"flow":

Protocol

Source IP address and Source Port

Destination IP Address and Destination Port

Start and End time

Aggregated Packet and Byte counts per flow

Detection

`FLOW` (actual flow dump from binary data)

```
router:          10.0.0.6
src IP:          192.168.59.218
dst IP:          172.16.0.28
src port:        53
dst port:        53
pkts:            2
bytes:           237
IP nexthop:      10.0.5.6
start time:      Fri Mar 15 00:52:04 2004
end time:        Fri Mar 15 00:52:15 2004
protocol:        17
tos:             0x0
src AS:          0
dst AS:          4538
TCP flags:       0x0
```

Useful abstraction of traffic

Detection

Hardware

Early 2002: 500 Mhz

Fall 2002: Xeon 2.5 Ghz

Fall 2003: Dual Xeon 3 Ghz

Records

No students, ~500K flows / 5-minute sample

Students, ~1M flows / 5-minute sample

Outbreak, much higher

Detection

Flowscan

Released by Dave Plonka, U. Wisconson

For each flow record, call external modules

CU Modules:

Top-N and Grapher

Bandwidth usage tracking

Find infected hosts

http://www.columbia.edu/acis/networks/advanced/CUFlow/

Detection

Find infected hosts

flows / second / host

Simple signatures: protocol # (udp, tcp, etc), port, byte size

```
$SIGNATURE{17}{1434}{404} = "SQL Slammer";
$SIGNATURE{6}{135}{0} = "MS RPC";
```

Locate C&C (Command and Control) nodes

Host A is scanning for 3127/tcp and talking to C on 7000/tcp

Host B is scanning for 3127/tcp and talking to C on 7000/tcp

Host C is probably C&C – who else talking to it?

Detection

List infected hosts

2004-03-18 01:19:43

Src Addr	Incident	Count	Src MAC	Hostname
160.39.201.174	445/tcp	26924	00000088391F	dyn-carl-201-174.dyn.columbia.edu
160.39.201.174	6667/tcp	3	00000088391F	dyn-carl-201-174.dyn.columbia.edu
160.39.202.41	445/tcp	12282	000046CD8D2E	dyn-carl-202-41.dyn.columbia.edu
160.39.202.41	6667/tcp	1	000046CD8D2E	dyn-carl-202-41.dyn.columbia.edu

Security / Support services quarantine identified infected hosts
User receives notice of incident via web, directions for cleanup

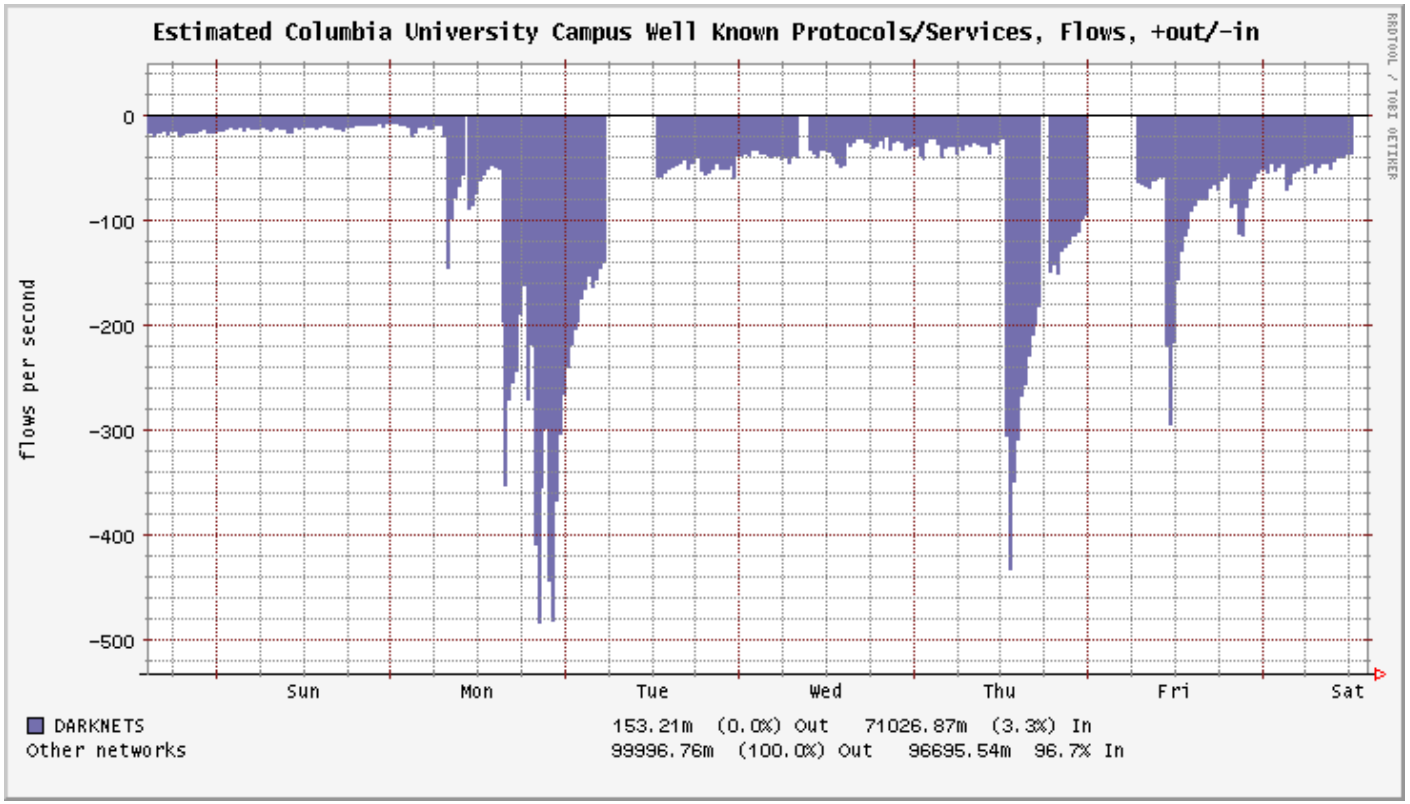
Detection

Strange destinations

- Hosts talking to “dark” networks
  - 209.2.224.0/20 valid, announced destination of ~4K addresses
  - Not connected
  - (CAIDA at UCSD uses /8 for “network telescope”)
- Bogons
  - Non-announced, non-allocated (non-permitted) destinations
  - Includes RFC1918 addresses

Detection

Darknet monitoring



Detection

DNS Logs

```
logging
{
    channel query_logs
    {
    file "/var/log/named_queries";
    severity debug;
    print-time yes;
    };
    category queries { query_logs; };
};
```

What were infected hosts trying to resolve – C&C nodes

```
client 10.0.202.5#1028: query: ph4t.b0t.central.org IN A
client 10.0.209.132#1028: query: ph4t.b0t.central.org IN A
```

Reporting

Send some mail

- Automated reporting?
  - Contact `abuse@` before WHOIS contact
  - Alter contact as requested
  - Silence reporting if requested
  - Don't let signatures go stale
- Give the required details
  - Timestamp + Timezone (UTC preferred)
  - Give methodologies or helpful links when possible
  - Send text-based logs

Reporting

Cymru WHOIS

```
$ whois -h whois.cymru.com 129.236.0.1
ASN      | IP                | Name
14       | 129.236.0.1       | COLUMB Columbia University
```

Translate IP to ASN

```
$ whois -h upstream-whois.cymru.com 129.236.0.1
PEER_AS | IP                | Name
209     | 129.236.0.1       | QWEST-4 Qwest
6395    | 129.236.0.1       | BCS-93 Broadwing Communication
```

Talk to upstream when primary ignores you

Team Cymru has lots of other good stuff

Reporting

Operational forums

ISP/NSP operators

Regional Internet2 operators

Reporting agencies

REN-ISAC

Homeland Security NIPC, chartered ISAC for Internet2

CERT

Communications

INOC-DBA – VOIP call-by-ASN: 14*DAN

Reporting

Finding your own reports

MyNetWatchman –

http://www.mynetwatchman.com/ListIncidentbyASSummary.asp?AS=14

Responding to reports

Who wants `abuse@` ?

What does our network look like normally?

Who gets to look at the data we find?

Small incidents sometimes become big – feds can take an interest

Questions?

Time?

Credits

Contact

Daniel Medina – medina@columbia.edu
http://www.columbia.edu/~medina/
Here all weekend, just find me!
Looking to chat about
networking, e-mail, security, disaster preparedness, etc

Thanks to...

Folks who have answered questions for me:
Dave Plonka (U. Wisconson)
Rob Thomas (Team Cymru)
Bill Owens (NYSERNet)
Doug Pearson (REN-ISAC)
Phil Rodrigues (NYU)

More Information – NetFlow

http://www.columbia.edu/~medina/
Links to this presentation and other documentation
http://www.cisco.com/go/netflow
Cisco NetFlow starting site
http://www.linuxgeek.org/netflow-howto.php
Getting things set up
http://net.doit.wisc.edu/~plonka/FlowScan/
FlowScan, Perl package and tools
http://www.columbia.edu/acis/networks/advanced/CUFlow/
Top-N reporting and Grapher modules
http://www.columbia.edu/acis/networks/advanced/FlowMonitor/
Bandwidth quota system
Send me some mail!
medina@columbia.edu

Other information...

http://www.internet2.edu

Internet2 offers many useful forums (security, VOIP, etc)

http://www.ren-isac.net

Research and Educations ISAC

http://www.mynetwatchman.com

Logs from distributed firewalls

http://www.cymru.com/

Team Cymru – building darknets, WHOIS server, and more

http://www.pch.net/inoc-dba

Call-by-ASN SIP proxy server

http://www.caida.org

CAIDA, home of the network telescope