PaIRS
Point of contact And Incident Response System

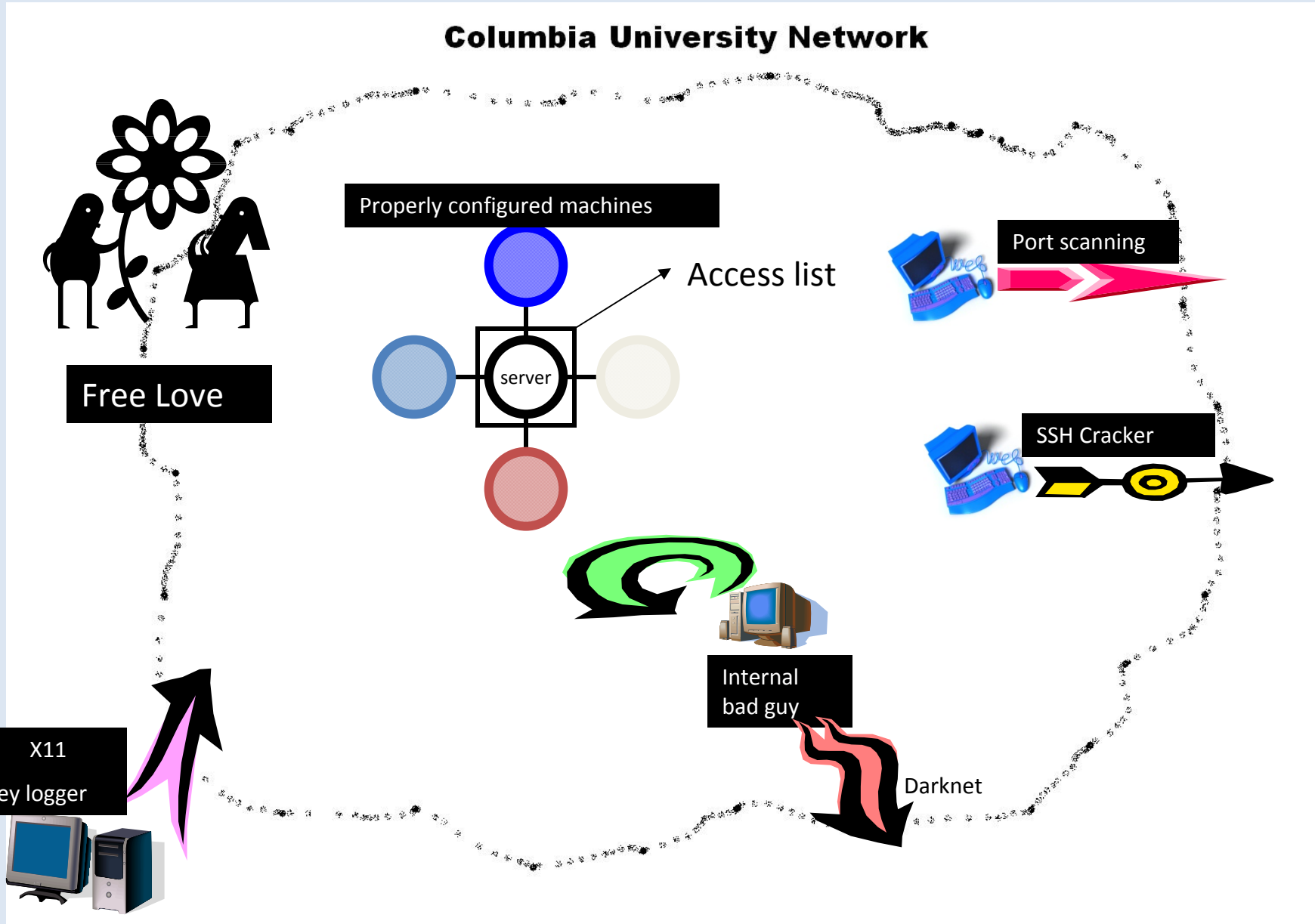
Security Camp

Boston University Summer 2009

Joel Rosenblatt, Manager Computer & Network Security, CISO

Columbia Network Environment

- Large research university
- Decentralized management structure
- Over 65,000 network nodes
- Over 35,000 MAC addresses active on average
- Decentralized computer support
- No sniffing traffic or scanning machines allowed
- “Free Love” IP address assignments
- No university wide, corporate like, firewalls
- Approximately 80,000 active email addresses



The Columbia Model - assumptions

- There is no such thing as perfect security
- There are more bad guys outside the University than inside
- Telling people what they can't do at Columbia is hard
- We have a big network pipe and lots of fast hardware
- We own the campus network
- Security in layers works
- We believe in privacy

The Columbia Model - Philosophy

- A security system that can protect the rest of the world from Columbia University will also protect Columbia from the rest of the world
- We may have some control over the attackers; the machines on our campus

What is PAIRS

PaIRS consists of two separate parts

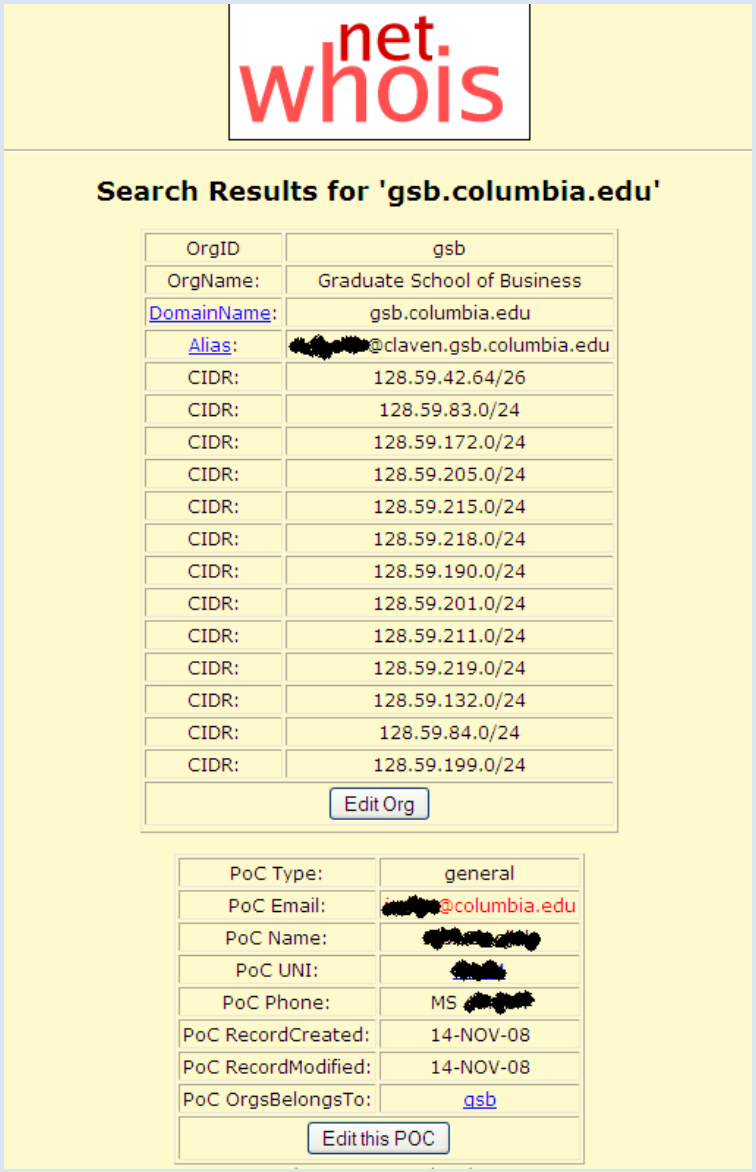
- Point of contact
  - A database that contains the person or persons responsible for a range of IP addresses or domain in the columbia.edu realm
- Incident Response System
  - A system that monitors all data flows to and from the Internet and processes them looking for patterns that represent incoming or outgoing attacks

POC Management

- IPs are either managed by departments or Free Love
- Contacts can be associated with multiple departments
- Contact information is compared against LDAP nightly – a title or dept change generates alert
- Departments can have central contact email plus a list of contacts
- Departments are defined by a list of CIDR blocks or domain

POC database

Sample POC record



net. whois

Search Results for 'gsb.columbia.edu'

OrgID	gsb
OrgName:	Graduate School of Business
DomainName:	gsb.columbia.edu
Alias:	[redacted]@claven.gsb.columbia.edu
CIDR:	128.59.42.64/26
CIDR:	128.59.83.0/24
CIDR:	128.59.172.0/24
CIDR:	128.59.205.0/24
CIDR:	128.59.215.0/24
CIDR:	128.59.218.0/24
CIDR:	128.59.190.0/24
CIDR:	128.59.201.0/24
CIDR:	128.59.211.0/24
CIDR:	128.59.219.0/24
CIDR:	128.59.132.0/24
CIDR:	128.59.84.0/24
CIDR:	128.59.199.0/24
Edit Org	

PoC Type:	general
PoC Email:	[redacted]@columbia.edu
PoC Name:	[redacted]
PoC UNI:	[redacted]
PoC Phone:	MS [redacted]
PoC RecordCreated:	14-NOV-08
PoC RecordModified:	14-NOV-08
PoC OrgsBelongsTo:	gsb
Edit this POC	

Incident Response System

- Based totally on Netflow – we do not look at packet content by policy
- Bayesian in nature
  - **Bayesian inference** is statistical inference in which evidence or observations are used to update or to newly infer the probability that a hypothesis may be true. Wikipedia
- Each flow is attributed to a IP address and then scored based on various behavior attributes
- Report Tolerance: 3 Capture Tolerance: 10
  Current Equation: y = A + (C * (D + log base B x))

	A	B	C	D	Short	Long	Direction
10000/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 10000	This machine is attempting to make connections to remote systems on TCP port 10000, which is indicative of an attempted exploit in Veritas Backup Server.	ACTIVE
RFC1918	0	5	2	0	Machine is attempting to connect to a range of non-routable IP addresses as defined in RFC 1918	This machine is making numerous requests to Univeristy routers to connect to non-routable IP addresses. This behavior is seen in worms attempting to infect an internal network once the perimeter has been breached.	ACTIVE
Dumbot	0	3	3	1	Machine is attempting to make contact with a command and control node that has been disabled by its ISP	This machine is attempting to connect to a known command and control node that has been disabled by its ISP via DNS. This means that not only is the machine infected by a bot, but is most likely very vulnerable in terms of being infected by another.	ACTIVE
139/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 139	This machine is attempting to connect to remote systems on TCP port 139, which is indicative of a worm attempting to exploit various file sharing and NetBIOS vulnerabilities in Microsoft Windows.	ACTIVE
5000/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 5000	This machine has made multiple attempts to an external machine on TCP port 5000. This is indicative of the presence of several different Trojans and could indicate an attempt to exploit a Microsoft Universal Plug and Play vulnerability.	ACTIVE
Welchia Ping	0	5	3	0	Machine is attempting to locate vulnerable machines in the manner of the Welchia worms	This machine is attempting to assess whether or not other machines can be infected by it using very specific ICMP packets best known for their use by several Welchia worm variants.	ACTIVE
SQL Slammer	0	5	3	0	Machine is attempting to spread the SQL Slammer worm	This machine is apparently infected by the SQL Slammer worm or a close variant, as it is attempting to infect other machines with this worm. This traffic will be seen on UDP port 1434.	ACTIVE
42/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 42	This machine is attempting to contact remote systems on TCP port 42, which is indicative of an attempted exploit of the Association Context Vulnerability in the Microsoft WINS service.	ACTIVE
C&C	0	2	5	1	Machine is connecting to a command and control node and may be under remote control	This machine has been connecting to a known command and control node. A command and control node is a server which runs special chat software for infected machines to connect to to receive commands and return information. Common commands include attacking other machines, attempting to infect others, sending spam, retrieving stored passwords and license keys, and recording keystrokes.	ACTIVE
CUDARKNET	0	5	3	0	Machine appears to be scanning for other vulnerable systems on the University network	This machine has attempted multiple connections to IP addresses that are assigned to the University but are intentionally kept out of use. Typical connections of this type are scans for Windows vulnerabilities in the case of network worms and brute force password attempts, or dictionary attacks, on SSH, telnet, or FTP servers.	ACTIVE
21/tcp	0	5	3	0	Machine is attempting to connect to other systems on port 21	This machine has made multiple attempts to an external machine on port 21, typically reserved for FTP service. The pattern of attempts indicate an attempt to perform a brute force or dictionary password attack against an FTP server. If you have no knowledge of this activity, this indicates a botted machine accepting remote control.	ACTIVE
22/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 22	This machine has made multiple attempts to an external machine on TCP port 22, typically reserved for SSH service. The pattern of attempts indicate an attempt to perform a brute force or dictionary password attack against an SSH server. If you have no knowledge of this activity, this indicates a botted machine accepting remote control.	ACTIVE
23/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 23	This machine has made multiple attempts to an external machine on TCP port 23, typically reserved for insecure telnet service. The pattern of attempts indicate an attempt to perform a brute force or dictionary password attack against a telnet server. If you have no knowledge of this activity, this indicates a botted machine accepting remote control.	ACTIVE
6667/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 6667	This machine is attempting to connect to remote systems on TCP port 6667, a port typically reserved for connections to Internet Relay Chat servers. This is suspicious due to the enourmous number of bots that make use of IRC to issue commands and receive reports from infected machines.	ACTIVE

SNMP scan	0	5	3	0	SNMP Scanning port 161, possibly caused by misconfigured printer software. See long explanation.	This machine has been observed SNMP scanning machines on the network on UDP port 161. This may be the result of misconfigured printer software (usually HP) or may be caused by a trojan scanner. Please check your software configuration and reconfigure if that is the problem. Otherwise treat this as a compromised system.	ACTIVE
1433/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 1433	This machine is attempting to connect to other systems on TCP port 1433, which is indicative of an attempted exploit of a vulnerability in Microsoft SQL Server.	ACTIVE
SSHScan	15	10	0	0	Machine is attempting to break in to a Columbia IT server via SSH	This machine has been observed making numerous attempts to guess passwords on a server maintained by Columbia University IT via SSH, SCP, or SFTP. Attempting to break into a Columbia system is a serious policy violation. If you have not done so, this machine has been hijacked by a malicious user.	ACTIVE
C&CHosted	25	10	0	0	Machine is a command and control node and is being used to control infected machines	This machine is being used maliciously as a command and control node for a bot network. This machine is responsible for sending instructions to countless infected machines and receiving data from them. This puts the user of this machine in serious danger of privacy compromise or legal liability.	ACTIVE
SNMP Attack	10	10	0	0	Machine is attempting to gain unauthorized access to a CU switch or router	This machine has been observed making numerous attempts to break in to a router or switch maintained by Columbia University IT. Attempting to break into a Columbia system is a serious policy violation. If you have not done so, this machine has been hijacked by a malicious user.	ACTIVE
6000/tcp	0	5	3	0	Machine is scanning for unprotected X-Windows servers	This machine has been observed looking for systems with running X-Windows servers that have not been secured and opening null sessions for the purpose of key logging	ACTIVE
8/tcp	0	5	3	0	This machine has been observed connecting to an encrypted botnet control port	This machine has been observed connecting to an encrypted botnet control port.	ACTIVE
31337/udp	0	5	3	0	This machine is scanning for Back Orifice	This machine is scanning for Back Orifice	ACTIVE
5900/tcp	0	5	3	0	This machine is scanning for unpatched RealVNC machines	This machine is scanning for unpatched RealVNC machines	ACTIVE
10080/tcp	0	5	3	0	This machine appears to be scanning for MyDoom Variants	This machine appears to be scanning for MyDoom Variants	ACTIVE
Spamlist	5	10	0	0	IP address is listed in a spammer blocklist.	This machine's IP address is listed in a spammer blocklist such as Spamhaus or the CBL.	ACTIVE
32768/tcp	0	5	3	0	This machine is scanning for systems compromised with HackersParadise.	This machine is scanning for systems compromised with HackersParadise.	ACTIVE
31337/tcp	0	5	3	0	This machine is scanning for BackOrifice	This machine is scanning for BackOrifice	ACTIVE
25/tcp	-3	5	3	0	This machine is sending so much mail that it appears to be spamming.	This machine seems to be sending too much mail traffic to an external relay. It appears to be spamming.	ACTIVE
2967/tcp	0	5	3	0	This machine is scanning for machines listening on the default Symantec Anti-Virus CE port	This machine is scanning for machines listening on the default Symantec Anti-Virus CE port	ACTIVE
5060/udp	3	10	0	0	This machine is scanning for SIP connections.	This machine is scanning for SIP connections.	ACTIVE
5060/tcp	3	10	0	0	This machine is scanning for SIP connections.	This machine is scanning for SIP connections.	ACTIVE
CNCreport	10	10	0	0	This machine was reported to be connecting to a known command and control host	This machine was reported to be connecting to a known command and control host, and is likely under remote control.	ACTIVE
baddns	10	10	0	0	This machine is connecting to malicious DNS services	This machine is connecting to malicious DNS services which suggest infection by DNSchanger or a related Trojan.	ACTIVE
7871/udp	0	5	3	0	The Storm Worm variant creates a peer-to-peer network that operates on port 7871/UDP. This machine is looking for peers.	The Storm Worm variant creates a peer-to-peer network that operates on port 7871/UDP,	ACTIVE
BackScatter	0	5	3	0	Connections being sent to command and control node with a request to terminate the connection	This machine is attempting connection to a known command and control node. However, it seems that this traffic consists entirely of replies to likely spoofed attacks on the node itself.	ACTIVE
3306/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 3306	Machine is attempting to connect to other systems on TCP port 3306, indicative of an attack on a MySQL server.	ACTIVE
143/tcp	0	5	3	0	This machine is scanning for IMAP servers.	This machine is scanning for IMAP servers.	ACTIVE
stormworm	0	5	3	0	Stormworm	Test patern for Stormworm connection port	ACTIVE
p2pBot47	3	10	0	0	47 Octet UDP Transmission	This host has been sending 47 Octet UDP 1 or 2 packet transmissions from the same source port.	ACTIVE
DroppedCNC	3	10	0	0	Machine attempted to connect to a C&C node but our routers dropped the traffic.	This machine is attempting connection to a known command and control node. However, the traffic was dropped by our routers. This could indicate that the traffic is spoofed.	ACTIVE
StormHTTP	10	10	0	0	Machine appears to be a Stormworm node hosting web content or a Skype supernode - turn off Skype when not active.	This machine not only appears to be a member of a Stormworm network based on p2p traffic, but also appears to be serving a great deal of HTTP content, indicating that it is hosting an eCard site.	ACTIVE
111/tcp	0	5	3	0	Port 111 is a security vulnerability for UNIX systems.	Port 111 is a security vulnerability for UNIX systems due to the number of vulnerabilities discovered for the portmapper and related RPC services.	ACTIVE

5168/udp	0	5	3	0	Machine scanning for systems running Trend Micro products	Machine scanning for systems running Trend Micro products	ACTIVE
5168/tcp	0	5	3	0	Machine scanning for systems running Trend Micro products	Machine scanning for systems running Trend Micro products	ACTIVE
2968/tcp	0	5	3	0	This machine is scanning for machines running rtvscan NLM on Netware servers	This machine is scanning for machines running rtvscan NLM on Netware servers.	ACTIVE
111/udp	0	5	3	0	Port 111 is a security vulnerability for UNIX systems.	Port 111 is a security vulnerability for UNIX systems due to the number of vulnerabilities discovered for the portmapper and related RPC services.	ACTIVE
3389/tcp	0	5	3	0	Brute force scan for Windows RDP	Brute force scan for Windows RDP	ACTIVE
1080/tcp	0	5	3	0	Scanning for SOCKS proxy server	Scanning for SOCKS proxy server	ACTIVE
1025/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 1025	This machine is attempting contact to remote systems on TCP port 1025, which is indicative of an attempted exploit of a Microsoft Windows RPC malformed message buffer overflow.	ACTIVE
1025/udp	0	5	3	0	Machine is attempting to connect to other systems on UDP port 1025	This machine is attempting contact to remote systems on UDP port 1025, which is indicative of an attempted exploit of a Microsoft Windows RPC malformed message buffer overflow.	INACTIVE
135/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 135	This machine has made multiple attempts to an external machine on TCP port 135, which indicates an attempt to exploit a vulnerability in Microsoft Windows. This machine is probably infected by one or more worms.	ACTIVE
1026/udp	0	5	3	0	Machine is attempting to connect to other systems on UDP port 1026	This machine is attempting contact to remote systems on UDP port 1026, which is indicative of an attempted exploit of a Microsoft Windows RPC malformed message buffer overflow.	INACTIVE
1027/udp	0	5	3	0	Machine is attempting to connect to other systems on UDP port 1027	This machine is attempting contact to remote systems on UDP port 1027, which is indicative of an attempted exploit of a Microsoft Windows RPC malformed message buffer overflow.	INACTIVE
445/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 445	This machine is connecting to remote systems on TCP port 445, which indicates an attempted exploit of one of many Microsoft Windows vulnerabilities, notably the LSASS vulnerability that was exploited by the Sasser worm and variants.	ACTIVE
4000/udp	0	5	3	0	Machine is attempting to connect to other systems on UDP port 4000	This machine is attempting to connect to remote systems on UDP port 4000, which is the default communications port for several Trojans as well as botnets employing ICQ for communication.	ACTIVE
4899/tcp	0	5	3	0	Machine is attempting to connect to other systems on TCP port 4899	This machine has been attempting to connect to remote systems on TCP port 4899, which is indicative of an attempt to exploit a vulnerability in radmin server installations.	ACTIVE

IRS – Netflow

- We have 1 machine dedicated to Neflow collection
  - /usr/bin/flow-capture -w /cflow/flows -V 5 -E900G -n 287 -N0 -p $PIDFILE 0/0/$PORTNUMBER
  - Each flow file contains 5 minutes worth of flows – Data is stored on a NetApp, shared via NFS
- We have 2 machines (with 2 more “on demand”) to process the flow data – each machine can process 4 files in parallel
- A 65M flow file can be processed in about 4 minutes
- With full student loads, we see 100M+ files, with processing time of 6-7 minutes
- With our current configuration, we can handle 400M+ files
- Incidents are moved to our incident database, correlation is done by IP address

Incident Database

IP Address	MAC Address	Hostname	Timestamp	Incident	Count
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:40:00 flows	DroppedCNC	3
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:40:00 flows	DroppedCNC	10
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:35:00 flows	DroppedCNC	15
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:35:00 flows	DroppedCNC	9
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:30:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:30:00 flows	DroppedCNC	10
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:25:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:25:00 flows	DroppedCNC	10
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:20:00 flows	DroppedCNC	15
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:20:00 flows	DroppedCNC	9
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:15:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:15:00 flows	DroppedCNC	10
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:10:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:10:00 flows	DroppedCNC	10
160.39.46.14	00235A687C2A	dyn-160-39-46-14.dyn.columbia.edu	2009-08-17 15:07:46 flows	p2pBot47	2684
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:05:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:05:00 flows	DroppedCNC	9
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 15:00:00 flows	DroppedCNC	15
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 15:00:00 flows	DroppedCNC	10
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 14:55:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 14:55:00 flows	DroppedCNC	10
160.39.98.162		mil-98-162.barnard.columbia.edu	2009-08-17 14:51:05 flows	p2pBot47	12140
128.59.42.156	08CFCAB7A867	dyn-128-59-42-156.dyn.columbia.edu	2009-08-17 14:50:00 flows	DroppedCNC	14
128.59.149.248	00123FB5E359	dyn-128-59-149-248.dyn.columbia.edu	2009-08-17 14:50:00 flows	DroppedCNC	9

Hourly Database processing

- Once an hour, the information in the database is processed
- The data for each IP address is correlated and scored
- Machines with a score of 10 and above are processed, below 3 are dropped and between 3 and 9.999 are carried over
- A hourly report is generated, with an email containing watched machines

Hourly report

```
CUIT Dynamic

?
qf=incident page
ip=209.2.215.209
hw=0019D267D690

dyn 209 2 215 209.dyn.columbia.edu

10 aug 2009 00:45:00 | 10 aug 2009 00:50:00 | DroppedCNC 2 10

DroppedCNC: Machine attempted to connect to a C&C node but our routers dropped the traffic.
SCORE: 3.00
Score does not meet capture threshold, machine will continue to be monitored

?
qf=incident page
ip=128.59.149.180
hw=00123F79D3BD

dyn-128-59-149-180.dyn.columbia.edu

10 aug 2009 03:55:00 | 10 aug 2009 00:50:00 | DroppedCNC 60 579

DroppedCNC: Machine attempted to connect to a C&C node but our routers dropped the traffic.
SCORE: 3.00
Score does not meet capture threshold, machine will continue to be monitored

?
qf=incident page
ip=160.39.220.178
hw=0000F07CE0F3

dyn-160-39-220-178.dyn.columbia.edu

10 aug 2009 04:05:26 | 10 aug 2009 05:00:03 | p2pBot47 2 43903

p2pBot47: 47 Octet UDP Transmission
SCORE: 3.00
Score does not meet capture threshold, machine will continue to be monitored

?
qf=incident page
ip=128.59.165.39
hw=0013722FAB0C

dyn-lab-165-39.dyn.columbia.edu

10 aug 2009 04:01:37 | 10 aug 2009 04:01:37 | p2pBot47 1 3325

p2pBot47: 47 Octet UDP Transmission
SCORE: 3.00
Score does not meet capture threshold, machine will continue to be monitored

?
qf=incident page
ip=128.59.149.248
hw=00123FB5E359

dyn-128-59-149-248.dyn.columbia.edu

10 aug 2009 03:55:00 | 10 aug 2009 00:50:00 | DroppedCNC 60 577

DroppedCNC: Machine attempted to connect to a C&C node but our routers dropped the traffic.
SCORE: 3.00
Score does not meet capture threshold, machine will continue to be monitored
```

Hourly report - continued

Dialup/VPN Hosts - 0 Distinct Users

CUIT Hosts already captured - 1 Botted Host

?
Ticket: HD0000000770422
Not yet captured or hardcoded, last IP: 160.39.52.86 at 18-aug-2009 08:52:13
ip=160.39.52.86
hw=002369607648

dyn-160-39-52-86.dyn.columbia.edu

18-aug-2009 07:55:00 | 18-aug-2009 08:45:00 | 25/tcp 9 5756

Downstream Gateways - 0 Botted Hosts

Potentially Botted Hosts on Ignore List - 0 Botted Hosts

Ignored Machines

128.59.172.243 (wofi.gsb.columbia.edu) Reason: Wireless Network Gateway for GSB Added: 11-oct-2005 14:58:28
128.59.211.2 (wofi2.gsb.columbia.edu) Reason: Wireless Network Gateway for GSB Added: 11-oct-2005 14:59:14
128.59.144.64 (crystal.bio.columbia.edu) Reason: Gateway for lab managed by Daisy Added: 11-oct-2005 15:00:39
129.236.10.20 (chaos.ldgo.columbia.edu) Reason: DNS Server for ldgo Added: 24-oct-2005 12:01:20
128.59.172.32 (fluffy.gsb.columbia.edu) Reason: InfraKeeper scans GSB for outages Added: 16-dec-2005 15:43:28

Watched machine email

This is an automatically generated message from the PAIRS system.
The following host(s) have not scored high enough to warrant
automatic processing. Please take a look.

?
qf=Incident page
ip=160.39.62.232
hw=00A0D131801E

dyn-160-39-62-232.dyn.columbia.edu

09-aug-2009 14:47:46 | 09-aug-2009 14:47:46 | p2pBot47 1 8119

p2pBot47: 47 Octet UDP Transmission

SCORE: 3.00

?
qf=Incident page
or=Barnard College
em=atadmin@barnard.edu, sysadmin@barnard.edu
ip=160.39.111.126

r600-111-126.barnard.columbia.edu

09-aug-2009 12:20:00 | 09-aug-2009 14:50:00 | DroppedCNC 31 293

DroppedCNC: Machine attempted to connect to a C&C node but our routers dropped the traffic.
SCORE: 3.00

Compromised machine processing

- IP addresses come in two flavors, Managed and Unmanaged (Free Love)
- Managed addresses are easy
  - Look up address in POC database
  - Send email to group that manages address
- Unmanaged IP addresses are Captured

Email sent to POC

Teacher's College - 1 Botted Host

?
qf=Incident page
ip=160.39.72.213

dyn-160-39-72-213.tc.columbia.edu

18-aug-2009 09:15:00 | 18-aug-2009 09:50:00 | C&C: 94.23.88.149:51987 8 115

C&C-94.23.88.149:51987: Machine is connecting to a command and control node and may be under remote control
SCORE: 39.23

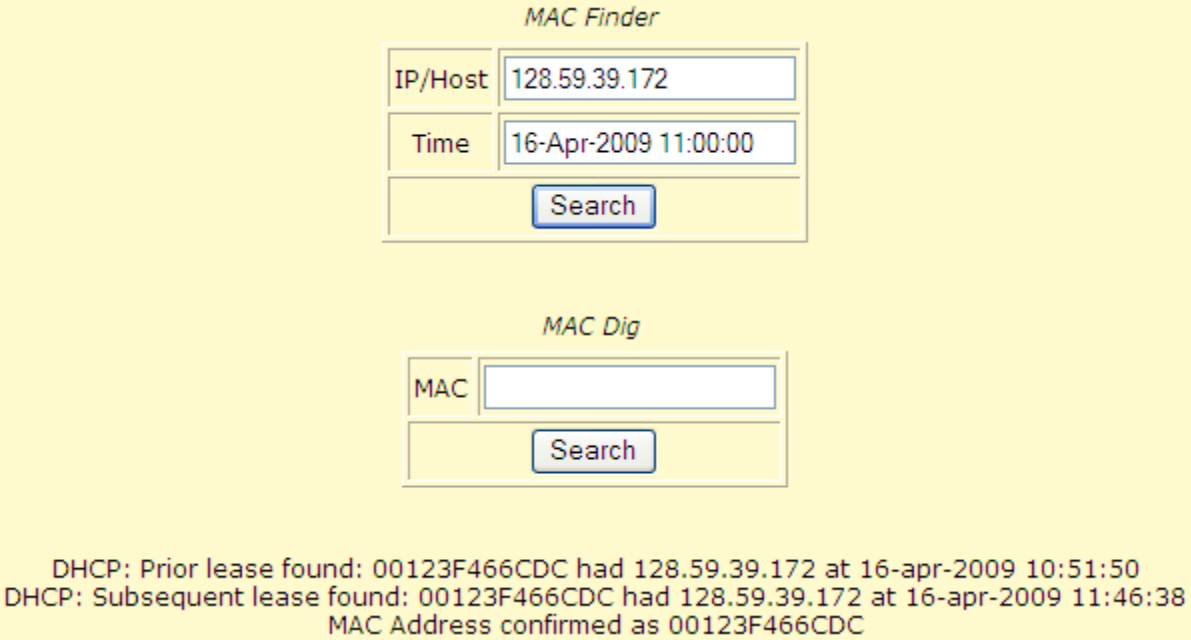
18-Aug-2009 09:14:58 GMT-0400 160.39.72.213:1276 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:15:21 GMT-0400 160.39.72.213:1284 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:15:45 GMT-0400 160.39.72.213:1292 -> 94.23.88.149:51987 6 128
18-Aug-2009 09:16:04 GMT-0400 160.39.72.213:1298 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:16:27 GMT-0400 160.39.72.213:1305 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:16:48 GMT-0400 160.39.72.213:1309 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:17:10 GMT-0400 160.39.72.213:1318 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:17:32 GMT-0400 160.39.72.213:1324 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:17:54 GMT-0400 160.39.72.213:1331 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:18:15 GMT-0400 160.39.72.213:1338 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:18:37 GMT-0400 160.39.72.213:1345 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:18:59 GMT-0400 160.39.72.213:1352 -> 94.23.88.149:51987 6 192
18-Aug-2009 09:19:20 GMT-0400 160.39.72.213:1358 -> 94.23.88.149:51987 6 192

Capture System

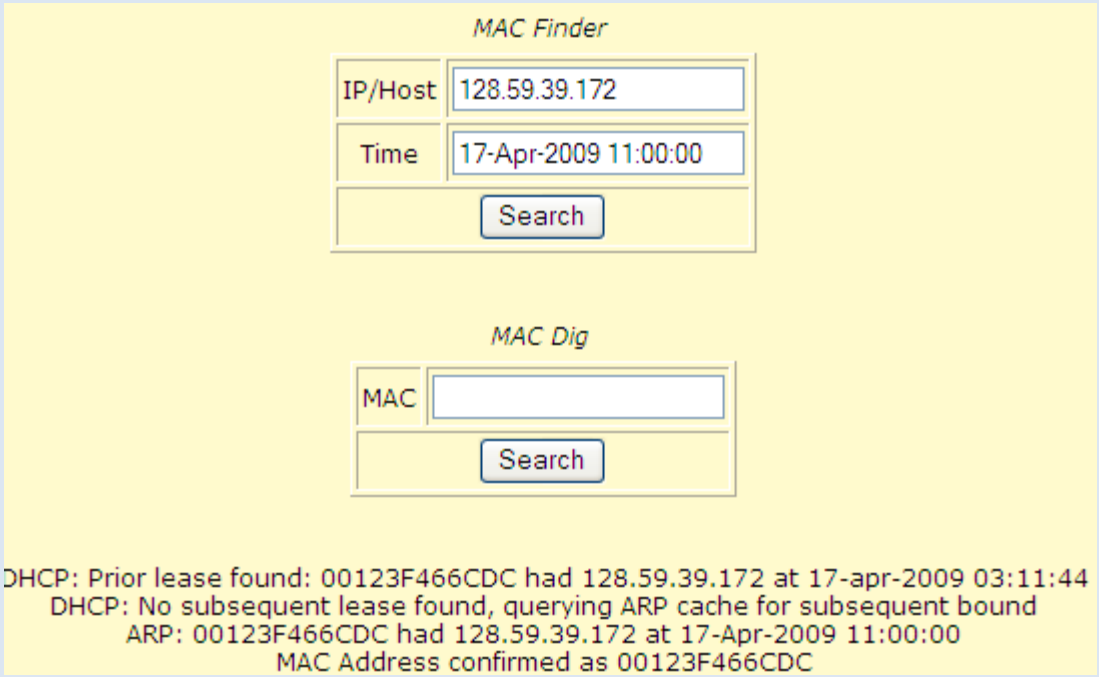
Step 1 - Resolve MAC

- Using bad traffic timestamp, check for prior DHCP entry
  - If next DHCP entry matches, pass to Mitigation
  - If no DHCP, check if arp matches, if not, then pass information in an email to POC Security

MAC Resolution – type 1



MAC Resolution – type 2



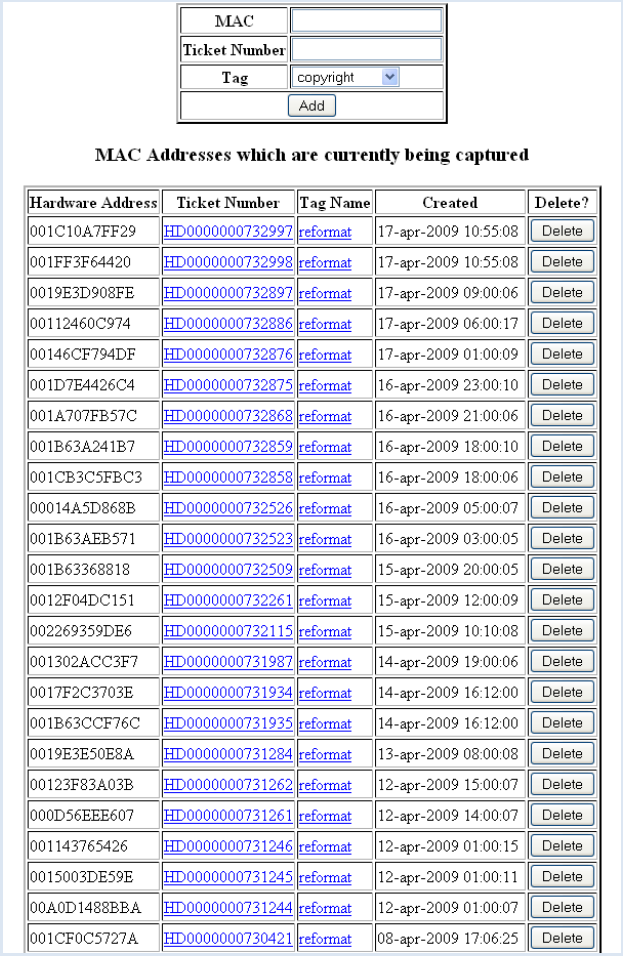
Step 2 - Mitigation

- Capture MAC address called out by IP in Resolve step
- Assign ticket to WormBusters group with status defined to “assigned”
- A process runs nightly to find captured MAC addresses not using DHCP
- A process is run to find MAC spoofers

Build your own Capture system

- Build non-routable campus wide Vlan
- Since everyone is required to use DHCP, offer non-routable addresses to captured MACs
- Fix DNS server on capture network to only offer address of capture WEB server
- Capture WEB server does all heavy lifting

Capture system web interface



MAC	
Ticket Number	
Tag	copyright
	Add

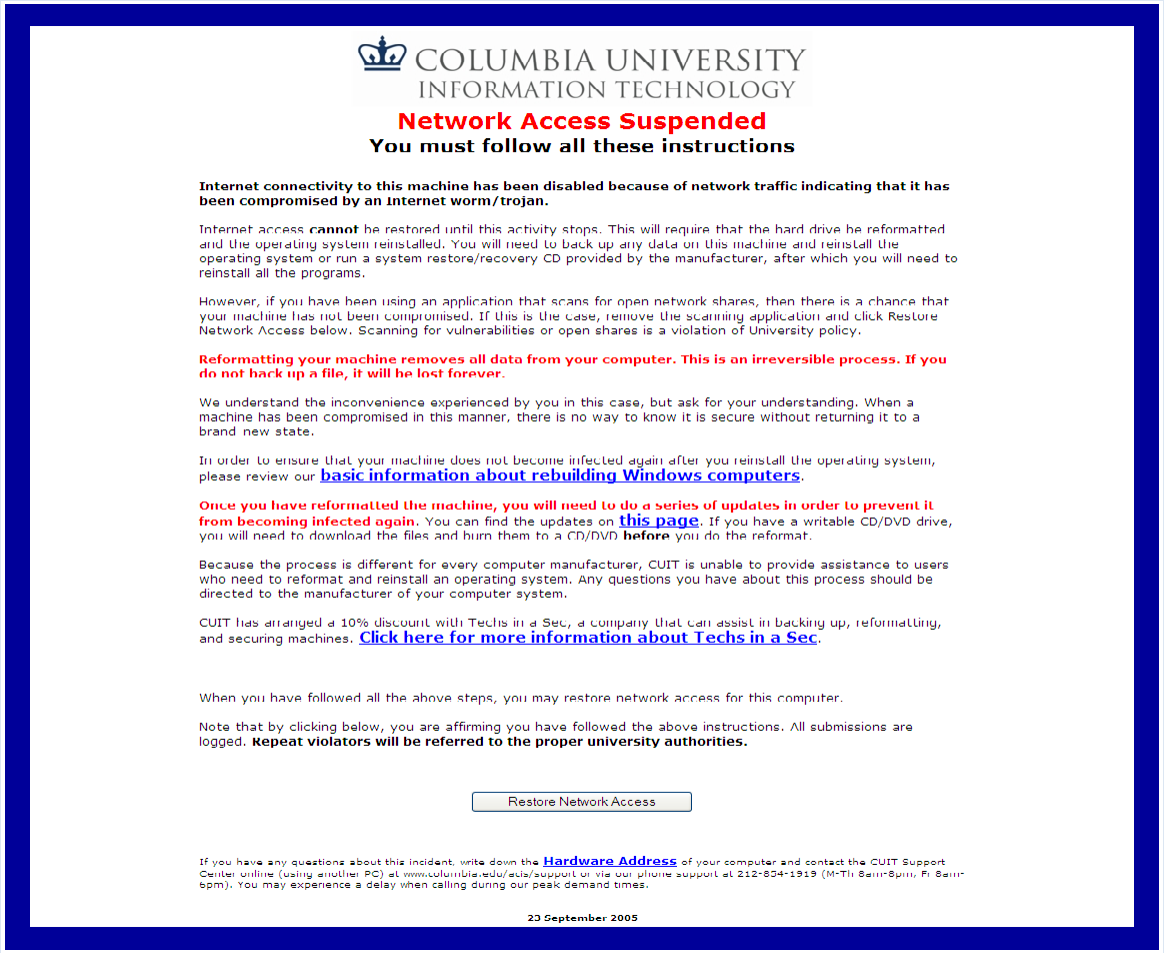
MAC Addresses which are currently being captured

Hardware Address	Ticket Number	Tag Name	Created	Delete?
001C10A7FF29	HD0000000732997	reformat	17-apr-2009 10:55:08	Delete
001FF3F64420	HD0000000732998	reformat	17-apr-2009 10:55:08	Delete
0019E3D908FE	HD0000000732897	reformat	17-apr-2009 09:00:06	Delete
00112460C974	HD0000000732886	reformat	17-apr-2009 06:00:17	Delete
00146CF794DF	HD0000000732876	reformat	17-apr-2009 01:00:09	Delete
001D7E4426C4	HD0000000732875	reformat	16-apr-2009 23:00:10	Delete
001A707FB57C	HD0000000732868	reformat	16-apr-2009 21:00:06	Delete
001B63A241B7	HD0000000732859	reformat	16-apr-2009 18:00:10	Delete
001CB3C5FBC3	HD0000000732858	reformat	16-apr-2009 18:00:06	Delete
00014A5D868B	HD0000000732526	reformat	16-apr-2009 05:00:07	Delete
001B63AEB571	HD0000000732523	reformat	16-apr-2009 03:00:05	Delete
001B63368818	HD0000000732509	reformat	15-apr-2009 20:00:05	Delete
0012F04DC151	HD0000000732261	reformat	15-apr-2009 12:00:09	Delete
002269359DE6	HD0000000732115	reformat	15-apr-2009 10:10:08	Delete
001302ACC3F7	HD0000000731987	reformat	14-apr-2009 19:00:06	Delete
0017F2C3703E	HD0000000731934	reformat	14-apr-2009 16:12:00	Delete
001B63CCF76C	HD0000000731935	reformat	14-apr-2009 16:12:00	Delete
0019E3E50E8A	HD0000000731284	reformat	13-apr-2009 08:00:08	Delete
00123F83A03B	HD0000000731262	reformat	12-apr-2009 15:00:07	Delete
000D56EEE607	HD0000000731261	reformat	12-apr-2009 14:00:07	Delete
001143765426	HD0000000731246	reformat	12-apr-2009 01:00:15	Delete
0015003DE59E	HD0000000731245	reformat	12-apr-2009 01:00:11	Delete
00A0D1488BBA	HD0000000731244	reformat	12-apr-2009 01:00:07	Delete
001CF0C5727A	HD0000000730421	reformat	08-apr-2009 17:06:25	Delete

User experience

- Bringing up a web browser on a captured machine will display the Network Access Suspended notice, it …
  - Informs the user that they are infected
  - Informs the user that they must reformat
  - Gives them an out if they are scanning machines on purpose
  - Points them to a “How to” on reformating a machine
  - Points them to a local vendor for the faint of heart

Reformat capture page



COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Network Access Suspended

You must follow all these instructions

Internet connectivity to this machine has been disabled because of network traffic indicating that it has been compromised by an internet worm/trojan.

Internet access **cannot** be restored until this activity stops. This will require that the hard drive be reformatted and the operating system reinstalled. You will need to back up any data on this machine and reinstall the operating system or run a system restore/recovery CD provided by the manufacturer, after which you will need to reinstall all the programs.

However, if you have been using an application that scans for open network shares, then there is a chance that your machine has not been compromised. If this is the case, remove the scanning application and click Restore Network Access below. Scanning for vulnerabilities or open shares is a violation of University policy.

Reformatting your machine removes all data from your computer. This is an irreversible process. If you do not back up a file, it will be lost forever.

We understand the inconvenience experienced by you in this case, but ask for your understanding. When a machine has been compromised in this manner, there is no way to know it is secure without returning it to a brand new state.

In order to ensure that your machine does not become infected again after you reinstall the operating system, please review our **basic information about rebuilding Windows computers**.

Once you have reformatted the machine, you will need to do a series of updates in order to prevent it from becoming infected again. You can find the updates on **this page**. If you have a writable CD/DVD drive, you will need to download the files and burn them to a CD/DVD **before** you do the reformat.

Because the process is different for every computer manufacturer, CUIT is unable to provide assistance to users who need to reformat and reinstall an operating system. Any questions you have about this process should be directed to the manufacturer of your computer system.

CUIT has arranged a 10% discount with Techs in a Sec, a company that can assist in backing up, reformatting, and securing machines. **Click here for more information about Techs in a Sec**.

When you have followed all the above steps, you may restore network access for this computer.

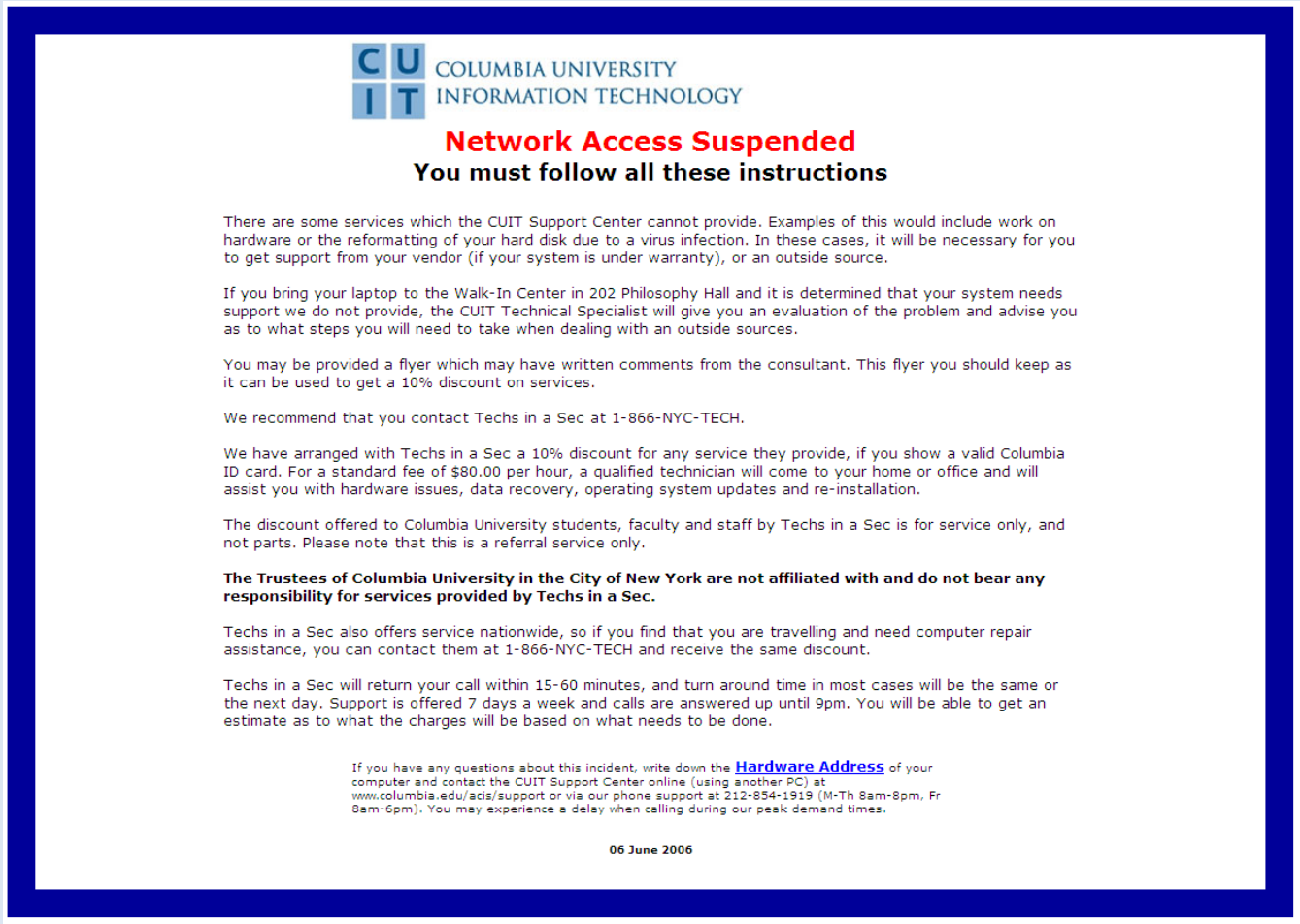
Note that by clicking below, you are affirming you have followed the above instructions. All submissions are logged. **Repeat violators will be referred to the proper university authorities.**

Restore Network Access

If you have any questions about this incident, write down the **Hardware Address** of your computer and contact the CUIT Support Center online (using another PC) at www.columbia.edu/acis/support or via our phone support at 212-854-1919 (M-Th 8am-8pm, Fr 8am-6pm). You may experience a delay when calling during our peak demand times.

23 September 2005

Techs in a Sec



COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Network Access Suspended

You must follow all these instructions

There are some services which the CUIT Support Center cannot provide. Examples of this would include work on hardware or the reformatting of your hard disk due to a virus infection. In these cases, it will be necessary for you to get support from your vendor (if your system is under warranty), or an outside source.

If you bring your laptop to the Walk-In Center in 202 Philosophy Hall and it is determined that your system needs support we do not provide, the CUIT Technical Specialist will give you an evaluation of the problem and advise you as to what steps you will need to take when dealing with an outside sources.

You may be provided a flyer which may have written comments from the consultant. This flyer you should keep as it can be used to get a 10% discount on services.

We recommend that you contact Techs in a Sec at 1-866-NYC-TECH.

We have arranged with Techs in a Sec a 10% discount for any service they provide, if you show a valid Columbia ID card. For a standard fee of $80.00 per hour, a qualified technician will come to your home or office and will assist you with hardware issues, data recovery, operating system updates and re-installation.

The discount offered to Columbia University students, faculty and staff by Techs in a Sec is for service only, and not parts. Please note that this is a referral service only.

The Trustees of Columbia University in the City of New York are not affiliated with and do not bear any responsibility for services provided by Techs in a Sec.

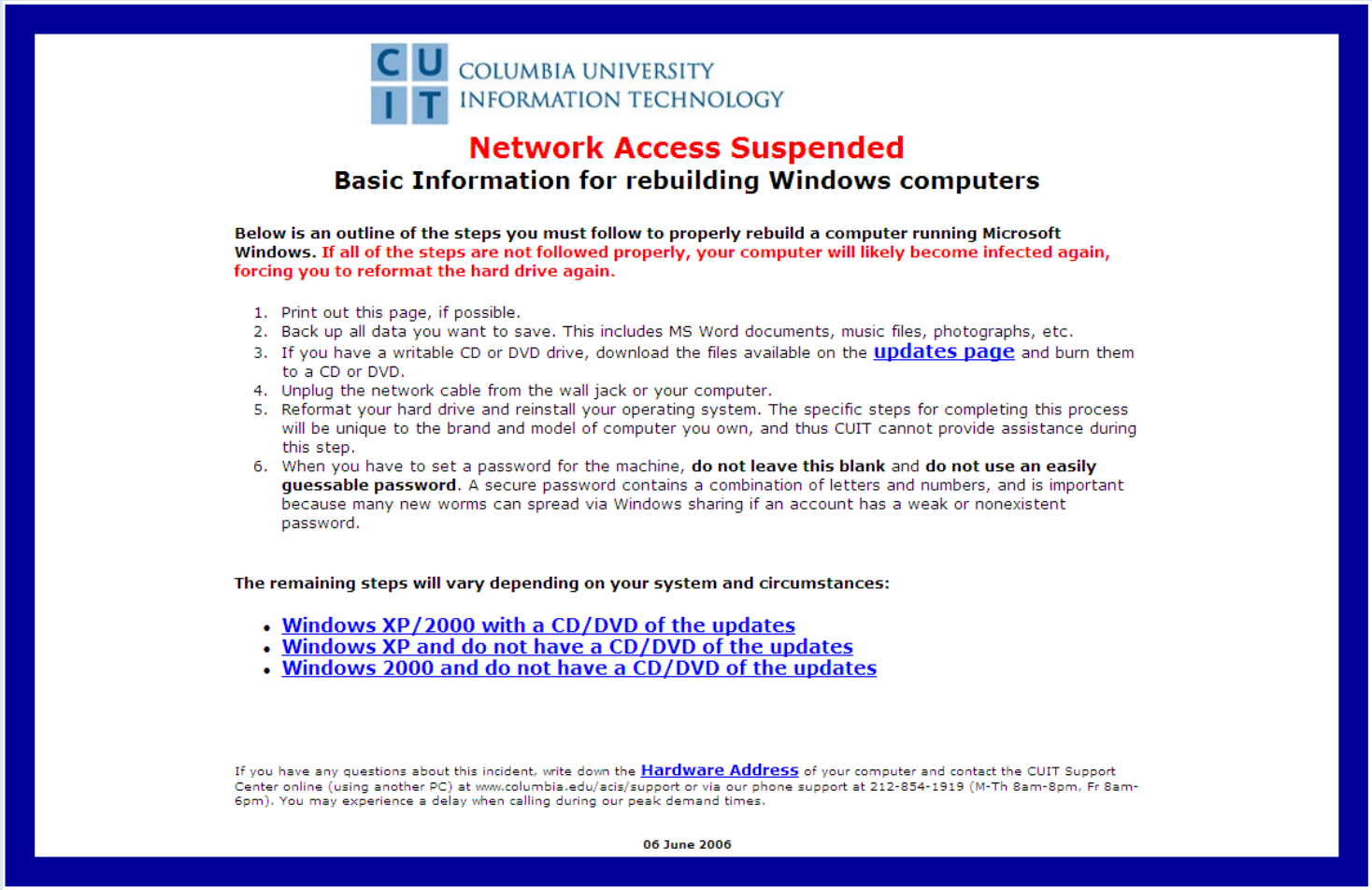
Techs in a Sec also offers service nationwide, so if you find that you are travelling and need computer repair assistance, you can contact them at 1-866-NYC-TECH and receive the same discount.

Techs in a Sec will return your call within 15-60 minutes, and turn around time in most cases will be the same or the next day. Support is offered 7 days a week and calls are answered up until 9pm. You will be able to get an estimate as to what the charges will be based on what needs to be done.

If you have any questions about this incident, write down the **Hardware Address** of your computer and contact the CUIT Support Center online (using another PC) at www.columbia.edu/acis/support or via our phone support at 212-854-1919 (M-Th 8am-8pm, Fr 8am-6pm). You may experience a delay when calling during our peak demand times.

06 June 2006

How to rebuild Windows



COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Network Access Suspended

Basic Information for rebuilding Windows computers

Below is an outline of the steps you must follow to properly rebuild a computer running Microsoft Windows. If all of the steps are not followed properly, your computer will likely become infected again, forcing you to reformat the hard drive again.

1. Print out this page, if possible.
2. Back up all data you want to save. This includes MS Word documents, music files, photographs, etc.
3. If you have a writable CD or DVD drive, download the files available on the **updates page** and burn them to a CD or DVD.
4. Unplug the network cable from the wall jack or your computer.
5. Reformat your hard drive and reinstall your operating system. The specific steps for completing this process will be unique to the brand and model of computer you own, and thus CUIT cannot provide assistance during this step.
6. When you have to set a password for the machine, **do not leave this blank** and **do not use an easily guessable password**. A secure password contains a combination of letters and numbers, and is important because many new worms can spread via Windows sharing if an account has a weak or nonexistent password.

The remaining steps will vary depending on your system and circumstances:

- **Windows XP/2000 with a CD/DVD of the updates**
- **Windows XP and do not have a CD/DVD of the updates**
- **Windows 2000 and do not have a CD/DVD of the updates**

If you have any questions about this incident, write down the **Hardware Address** of your computer and contact the CUIT Support Center online (using another PC) at www.columbia.edu/acis/support or via our phone support at 212-854-1919 (M-Th 8am-8pm, Fr 8am-6pm). You may experience a delay when calling during our peak demand times.

06 June 2006

Uncapture

- Once the machine is clean, the user brings up a web browser and clicks on the restore network access button
- The user is asked to authenticate and network access will be restored in about 2 hours – no checking is done
- If the user did not reformat, they will be recaptured – rinse & repeat

Additiona PaIRS features

- An ignore list exists to allow legitimate behaviors (i.e. a mail server)
- Traffic coming into Columbia is processed and scored – we generate about 500 emails a day to ISPs that have machines behaving badly

Please stop email

This is an automated message from Columbia University IT Security. You are receiving it because you are listed as the abuse contact for the machine referred to below. This machine attempted to gain unauthorized access to one or more machines at Columbia University.

Details are provided below. Please take all necessary steps to mitigate such attacks.

If you have received this message in error, or if this incident reported is inappropriate, please contact security@columbia.edu so that we can update our procedures. Please include the entire body of this message.

Thank You.

Columbia University IT Security
security@columbia.edu

Name: ???
Address: 95.58.11.228

Incident type: 23/tcp
First attempt: 12-aug-2009 08:05:00 GMT-0400
Last attempt: 12-aug-2009 08:35:00 GMT-0400
Total attempts: 8071

12-Aug-2009 08:08:40 GMT-0400 95.58.11.228:2875 -> 209.2.48.1:23 6 286
12-Aug-2009 08:09:11 GMT-0400 95.58.11.228:3839 -> 209.2.51.197:23 6 102
12-Aug-2009 08:09:11 GMT-0400 95.58.11.228:3840 -> 209.2.51.198:23 6 102
12-Aug-2009 08:09:11 GMT-0400 95.58.11.228:3841 -> 209.2.51.199:23 6 102
12-Aug-2009 08:09:11 GMT-0400 95.58.11.228:3842 -> 209.2.51.200:23 6 286
12-Aug-2009 08:09:12 GMT-0400 95.58.11.228:3852 -> 209.2.51.210:23 6 102
12-Aug-2009 08:09:12 GMT-0400 95.58.11.228:3850 -> 209.2.51.208:23 6 102
12-Aug-2009 08:09:11 GMT-0400 95.58.11.228:3837 -> 209.2.51.195:23 6 102
12-Aug-2009 08:09:12 GMT-0400 95.58.11.228:3848 -> 209.2.51.206:23 6 102
12-Aug-2009 08:09:12 GMT-0400 95.58.11.228:3849 -> 209.2.51.207:23 6 102
12-Aug-2009 08:09:12 GMT-0400 95.58.11.228:3850 -> 209.2.51.208:23 6 102

Summary

- The PaIRS system is has been running since 2005, not as neat and cool as now, but the basic concepts are well tested
- Future PaIRS enhancements will include a Neural network to look for low and slow behaviors
- Based on the number of reports received from outside sources about infected Columbia IPs, PaIRS keeps the Columbia network about 99% clean

Questions?

Joel Rosenblatt

joel AT columbia.edu

212 854 3033