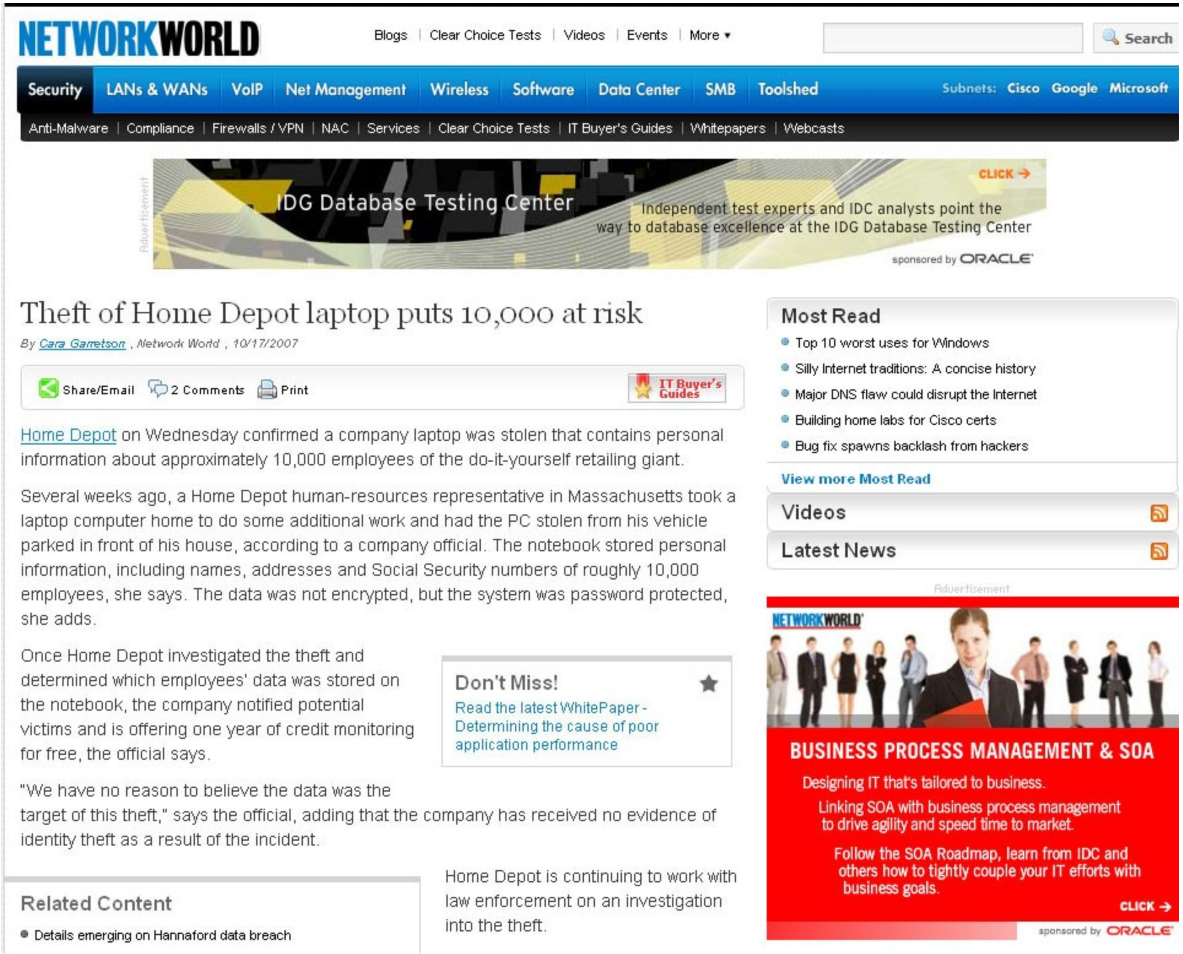
Data Leakage and Seepage

- Data Leakage occurs when private and sensitive information revealed, either accidentally or through carelessness.
  - This can be due to programming errors, improper handling of sensitive information, or malicious internal threats.
- Data breaches cost companies millions of dollars (a study by the Ponemon Institute estimates the costs in 2009 to be an average of $6.75 million).

- The most expensive data breach event included in the 2009 study cost a company nearly $31 million to resolve.
- The least expensive total cost of data breach for a company included in the study was $750,000.
- In addition to the direct costs, a well-publicized data breach can also translate into lost business opportunities.

Examples of Leakage


NETWORKWORLD
Blogs | Clear Choice Tests | Videos | Events | More ▾
Search
Security | LANs & WANs | VoIP | Net Management | Wireless | Software | Data Center | SMB | Toolshed
Subnets: Cisco Google Microsoft
Anti-Malware | Compliance | Firewalls / VPN | NAC | Services | Clear Choice Tests | IT Buyer's Guides | Whitepapers | Webcasts

Theft of Home Depot laptop puts 10,000 at risk

By Cara Garretson , Network World , 10/17/2007

Share/Email
2 Comments
Print
IT Buyer's Guides

Home Depot on Wednesday confirmed a company laptop was stolen that contains personal information about approximately 10,000 employees of the do-it-yourself retailing giant.

Several weeks ago, a Home Depot human-resources representative in Massachusetts took a laptop computer home to do some additional work and had the PC stolen from his vehicle parked in front of his house, according to a company official. The notebook stored personal information, including names, addresses and Social Security numbers of roughly 10,000 employees, she says. The data was not encrypted, but the system was password protected, she adds.

Once Home Depot investigated the theft and determined which employees' data was stored on the notebook, the company notified potential victims and is offering one year of credit monitoring for free, the official says.

"We have no reason to believe the data was the target of this theft," says the official, adding that the company has received no evidence of identity theft as a result of the incident.

Home Depot is continuing to work with law enforcement on an investigation into the theft.

Don't Miss!

Read the latest WhitePaper - Determining the cause of poor application performance

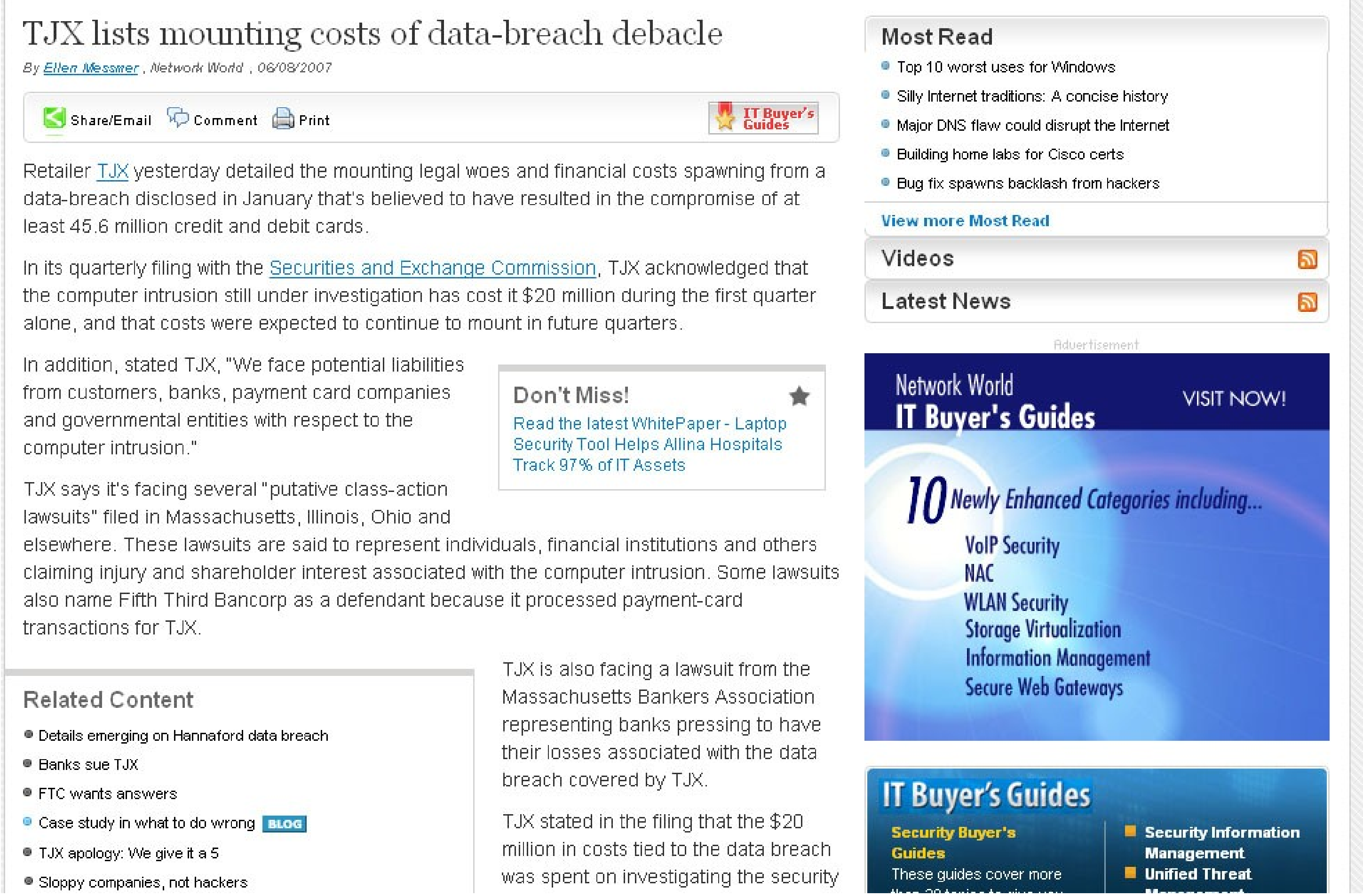
Related Content

- Details emerging on Hannaford data breach

Most Read

- Top 10 worst uses for Windows
- Silly Internet traditions: A concise history
- Major DNS flaw could disrupt the Internet
- Building home labs for Cisco certs
- Bug fix spawns backlash from hackers

View more Most Read



TJX lists mounting costs of data-breach debacle

By Ellen Messmer , Network World , 06/08/2007

Retailer TJX yesterday detailed the mounting legal woes and financial costs spawning from a data-breach disclosed in January that's believed to have resulted in the compromise of at least 45.6 million credit and debit cards.

In its quarterly filing with the Securities and Exchange Commission, TJX acknowledged that the computer intrusion still under investigation has cost it $20 million during the first quarter alone, and that costs were expected to continue to mount in future quarters.

In addition, stated TJX, "We face potential liabilities from customers, banks, payment card companies and governmental entities with respect to the computer intrusion."

TJX says it's facing several "putative class-action lawsuits" filed in Massachusetts, Illinois, Ohio and elsewhere. These lawsuits are said to represent individuals, financial institutions and others claiming injury and shareholder interest associated with the computer intrusion. Some lawsuits also name Fifth Third Bancorp as a defendant because it processed payment-card transactions for TJX.

TJX is also facing a lawsuit from the Massachusetts Bankers Association representing banks pressing to have their losses associated with the data breach covered by TJX.

TJX stated in the filing that the $20 million in costs tied to the data breach was spent on investigating the security

Don't Miss!

Read the latest WhitePaper - Laptop Security Tool Helps Allina Hospitals Track 97% of IT Assets

Related Content

- Details emerging on Hannaford data breach
- Banks sue TJX
- FTC wants answers
- Case study in what to do wrong BLOG
- TJX apology: We give it a 5
- Sloppy companies, not hackers

Most Read

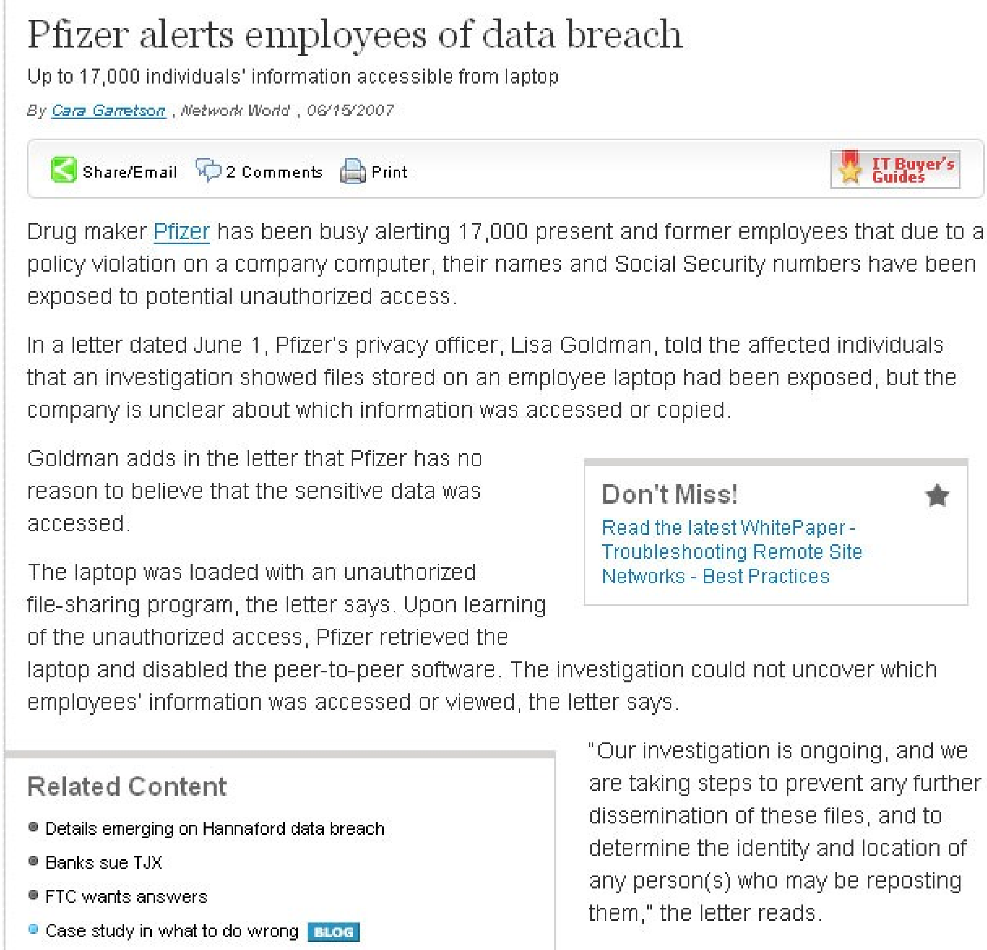
- Top 10 worst uses for Windows
- Silly Internet traditions: A concise history
- Major DNS flaw could disrupt the Internet
- Building home labs for Cisco certs
- Bug fix spawns backlash from hackers

View more Most Read

Videos

Latest News

Hazards of File Sharing programs!



Pfizer alerts employees of data breach

Up to 17,000 individuals' information accessible from laptop

By Cara Garretson , Network World , 06/15/2007

Drug maker Pfizer has been busy alerting 17,000 present and former employees that due to a policy violation on a company computer, their names and Social Security numbers have been exposed to potential unauthorized access.

In a letter dated June 1, Pfizer's privacy officer, Lisa Goldman, told the affected individuals that an investigation showed files stored on an employee laptop had been exposed, but the company is unclear about which information was accessed or copied.

Goldman adds in the letter that Pfizer has no reason to believe that the sensitive data was accessed.

The laptop was loaded with an unauthorized file-sharing program, the letter says. Upon learning of the unauthorized access, Pfizer retrieved the laptop and disabled the peer-to-peer software. The investigation could not uncover which employees' information was accessed or viewed, the letter says.

"Our investigation is ongoing, and we are taking steps to prevent any further dissemination of these files, and to determine the identity and location of any person(s) who may be reposting them," the letter reads.

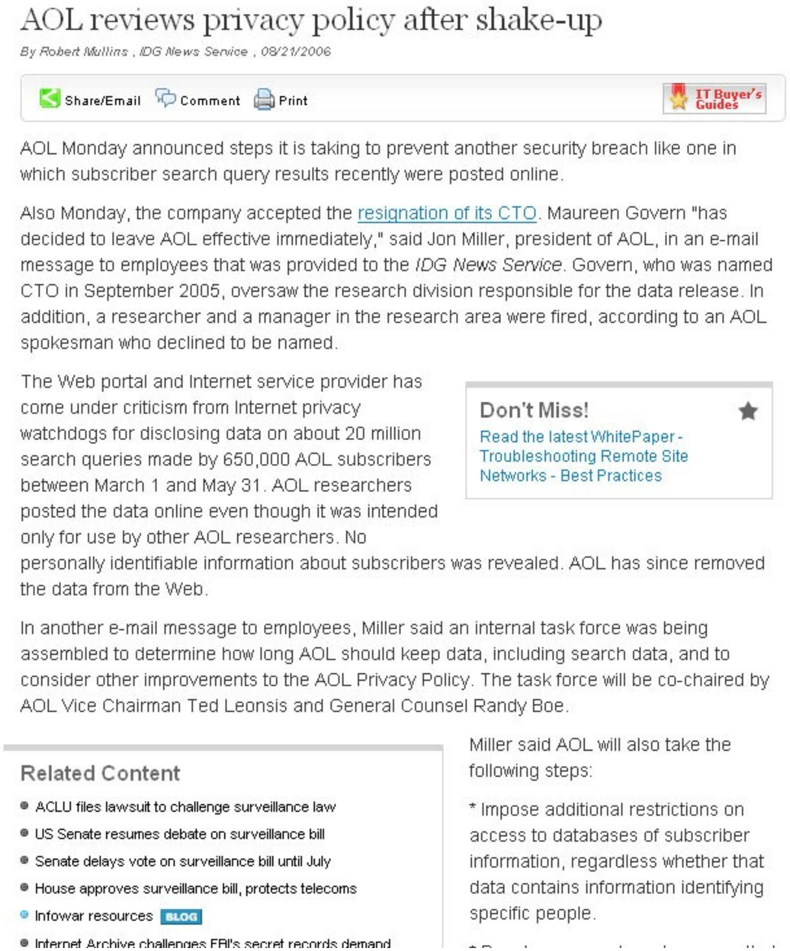
Don't Miss!

Read the latest WhitePaper - Troubleshooting Remote Site Networks - Best Practices

Related Content

- Details emerging on Hannaford data breach
- Banks sue TJX
- FTC wants answers
- Case study in what to do wrong BLOG

Be careful where you post information!



AOL reviews privacy policy after shake-up

By Robert Mullins , IDG News Service , 08/21/2006

AOL Monday announced steps it is taking to prevent another security breach like one in which subscriber search query results recently were posted online.

Also Monday, the company accepted the resignation of its CTO. Maureen Govern "has decided to leave AOL effective immediately," said Jon Miller, president of AOL, in an e-mail message to employees that was provided to the *IDG News Service*. Govern, who was named CTO in September 2005, oversaw the research division responsible for the data release. In addition, a researcher and a manager in the research area were fired, according to an AOL spokesman who declined to be named.

The Web portal and Internet service provider has come under criticism from Internet privacy watchdogs for disclosing data on about 20 million search queries made by 650,000 AOL subscribers between March 1 and May 31. AOL researchers posted the data online even though it was intended only for use by other AOL researchers. No personally identifiable information about subscribers was revealed. AOL has since removed the data from the Web.

In another e-mail message to employees, Miller said an internal task force was being assembled to determine how long AOL should keep data, including search data, and to consider other improvements to the AOL Privacy Policy. The task force will be co-chaired by AOL Vice Chairman Ted Leonsis and General Counsel Randy Boe.

Miller said AOL will also take the following steps:

* Impose additional restrictions on access to databases of subscriber information, regardless whether that data contains information identifying specific people.

Related Content

- ACLU files lawsuit to challenge surveillance law
- US Senate resumes debate on surveillance bill
- Senate delays vote on surveillance bill until July
- House approves surveillance bill, protects telecoms
- Infowar resources BLOG
- Internet Archive challenges FBI's secret records demand

Data Seepage?

- Data Seepage occurs for example, when your machine boots up and some desktop applications are set to automatically connect to internal mail servers or shared folders.
- Basically It is all about how “chatty” client machines are. This is compounded with the rise in targeted attacks and mobile enterprise users increasingly working off public WiFi connections while on the road or in the coffee shop.
- An attacker using a sniffer on a wired or wireless LAN can "see" the victim's machine gathering DNS server names or other information on network resources and use that information to better hone in on the target.
- If the machine is too chatty when it connects to the resources, then it "seeps" data.
- Outlook, for instance, will look for its Exchange server, Windows will try to reconnect to mapped drives.
- AIM will try to connect to its network server.
- This chattiness allows an attacker to gain information about a target without raising and alerts.

- Always be aware of what your laptop or workstation does when it starts up:
  - Programs set to autostart
  - Looking for certain resources like intranet homepage and shared drives
  - Email clients
  - Instant messaging clients

Essential Elements of Friendly Information - EEFI

- This is a military term and is defined as:
  - “Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness.”

EEFI: Example (Courtesy of Errata Security)

Him: When can I see you again?

Her: How about next week? My boss, the director of the NSA has a trip he is going on he can’t even tell me about. It makes me so mad, how am I suppose to help coordinate things if I don’t even know where he is going. He did ask me to buy a lot of suntan lotion though…

Him: Excuse me, I have to make a phone call…..to my sister…about…trees.

Her: Ok hurry back, I am going to order another drink.

Inference Channels – A form of EEFI

- Movements and business trips of CEOs, sales staff, or even engineers can tell a diligent observer about your business.
  - Repeated trips to a competitors headquarters?
  - Sales people cancelling engagements near end of month or end of quarter.
  - Engineers working lots of overtime (cars in parking lots) as a ship date gets critical.

Inference Example (Courtesy of Errata Security)

Him: When can I see you again?

Her: How about next week? My boss, the CEO, is out all next week on some sort of secret trip. Its his third time going to Redmond this month and he hasn’t even brought me a present, but I have to be on call at all hours to coordinate a conference call with all the C level execs.

Him: Excuse me, I have to make a phone call…..to my brother… about…a playdate for our dogs…

Her: That’s so sweet, Hurry back, I am ordering more drinks.

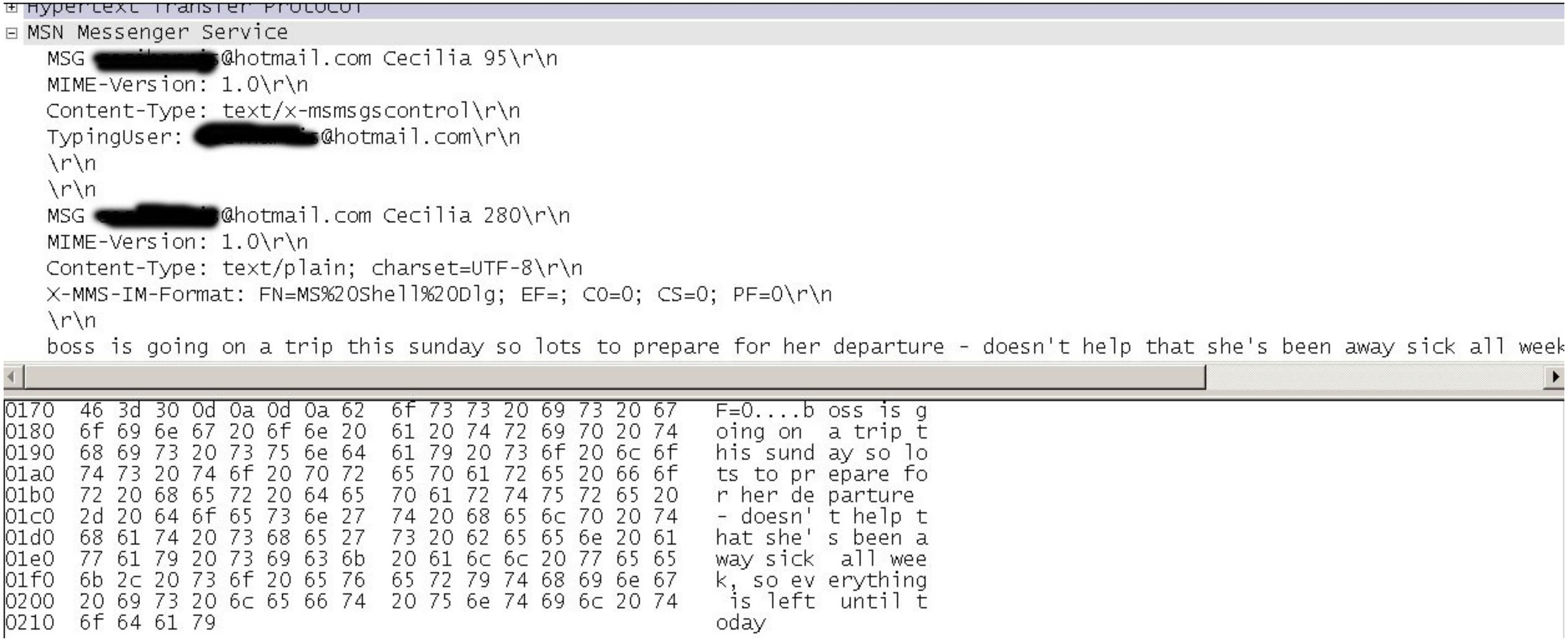
Many Such Examples:

- A company keeps ordering a lot of delivery food for several days.
- Increased shipping activity in business warehouses as the end of quarter approaches.
- A small company placing an order for 50 new workstations or placing an order to for more VoIP quality circuits to locations they where they don’t have offices.

An MSN Example

- Consider the following series of packet captures that can be used very effectively for social engineering.
- Note that the actual names have been sanitized but this is a “real” capture of a local 802.11 network.
- Also note that since the complete frame has been captured, information such as the company IP address, etc is available.

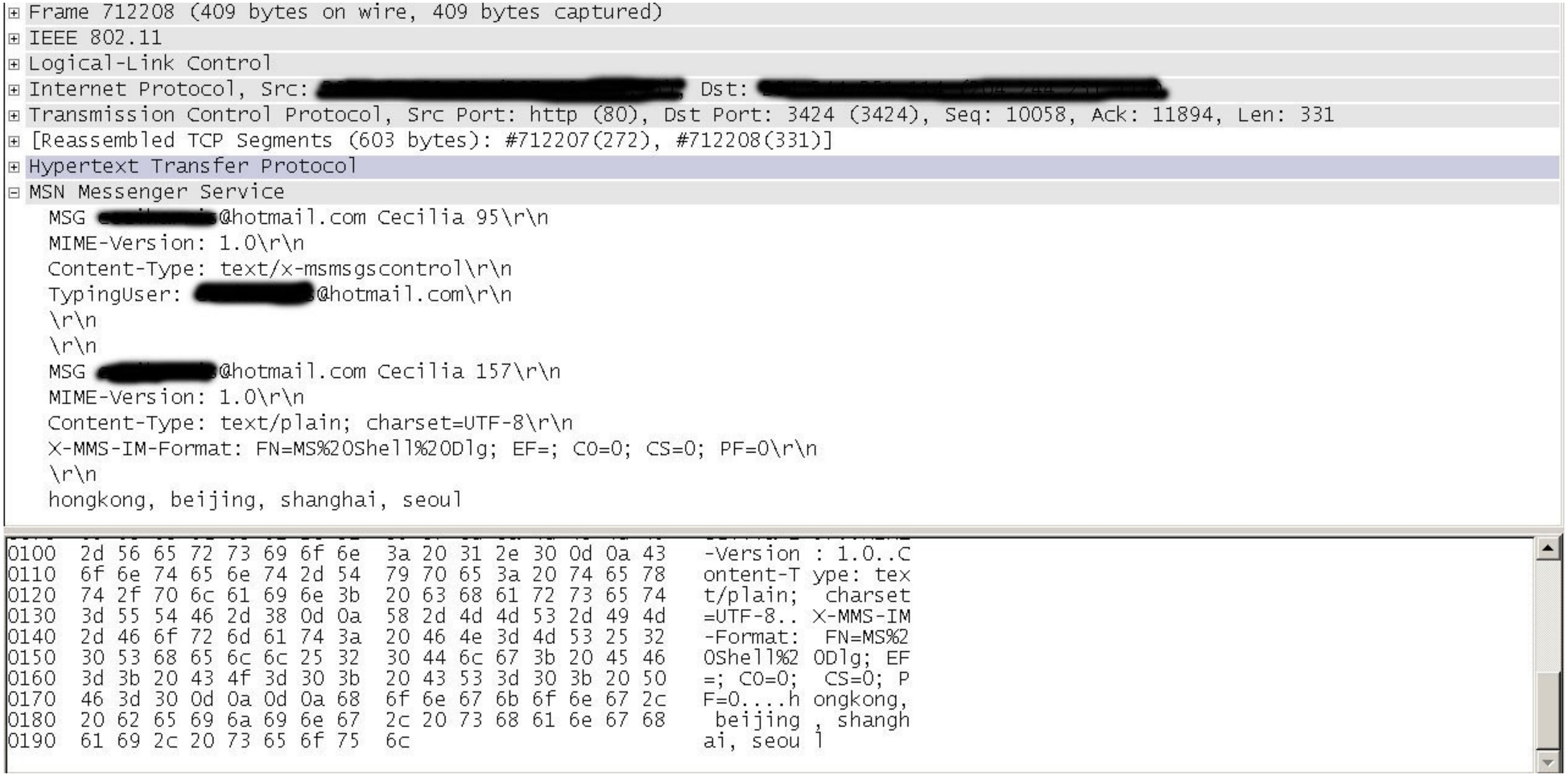
Frame #1- Boss is going away on a business trip



```
⊞ Hypertext Transfer Protocol
⊟ MSN Messenger Service
    MSG [redacted]@hotmail.com Cecilia 95\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/x-msmsgscontrol\r\n
    TypingUser: [redacted]@hotmail.com\r\n
    \r\n
    \r\n
    MSG [redacted]@hotmail.com Cecilia 280\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0\r\n
    \r\n
    boss is going on a trip this sunday so lots to prepare for her departure - doesn't help that she's been away sick all week
```

```
0170  46 3d 30 0d 0a 0d 0a 62  6f 73 73 20 69 73 20 67   F=0....b oss is g
0180  6f 69 6e 67 20 6f 6e 20  61 20 74 72 69 70 20 74   oing on  a trip t
0190  68 69 73 20 73 75 6e 64  61 79 20 73 6f 20 6c 6f   his sund ay so lo
01a0  74 73 20 74 6f 20 70 72  65 70 61 72 65 20 66 6f   ts to pr epare fo
01b0  72 20 68 65 72 20 64 65  70 61 72 74 75 72 65 20   r her de parture
01c0  2d 20 64 6f 65 73 6e 27  74 20 68 65 6c 70 20 74   - doesn' t help t
01d0  68 61 74 20 73 68 65 27  73 20 62 65 65 6e 20 61   hat she' s been a
01e0  77 61 79 20 73 69 63 6b  20 61 6c 6c 20 77 65 65   way sick  all wee
01f0  6b 2c 20 73 6f 20 65 76  65 72 79 74 68 69 6e 67   k, so ev erything
0200  20 69 73 20 6c 65 66 74  20 75 6e 74 69 6c 20 74    is left  until t
0210  6f 64 61 79                                        oday
```

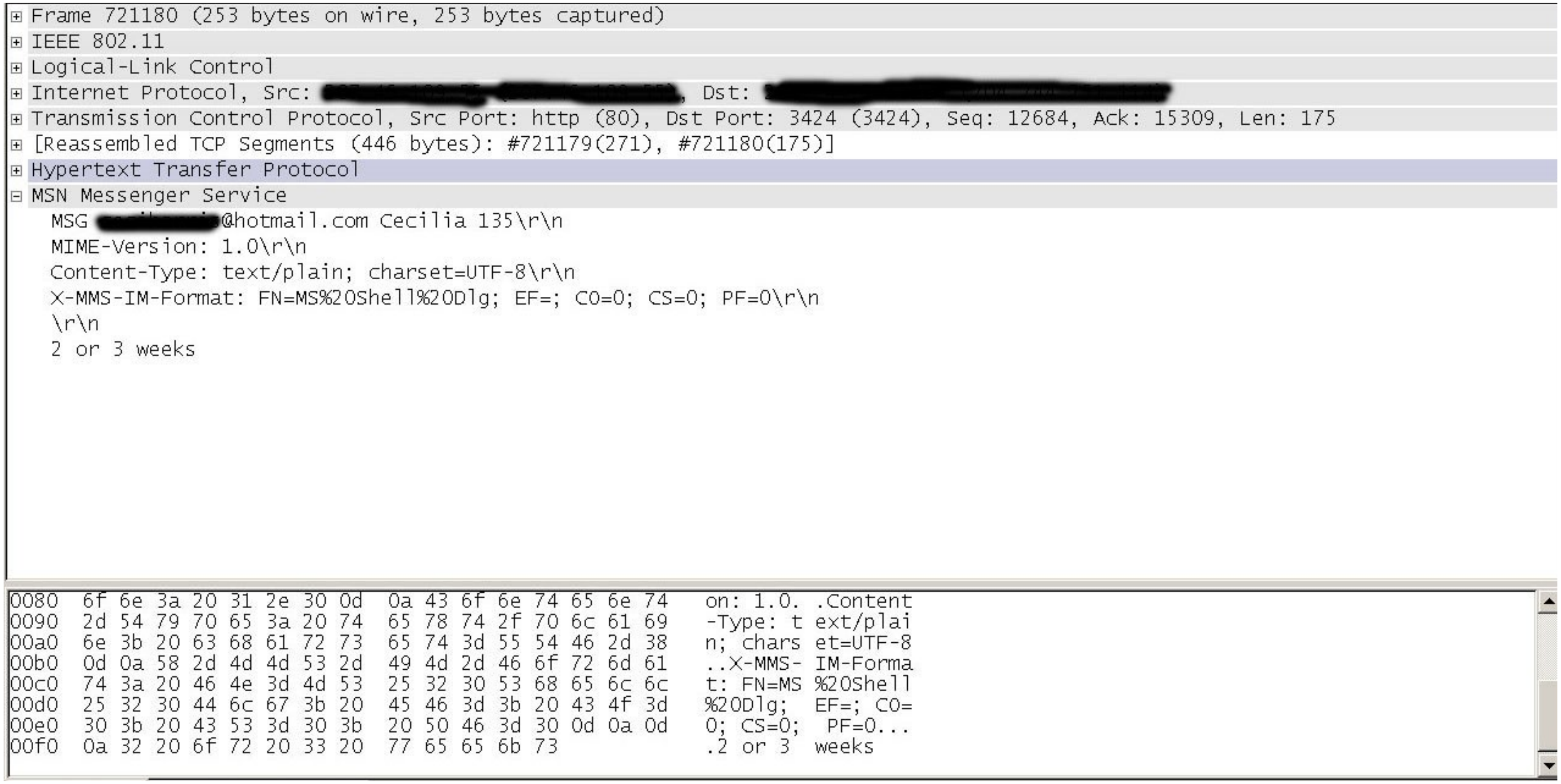
Frame #2 – Where did you say she was going?



```
⊞ Frame 712208 (409 bytes on wire, 409 bytes captured)
⊞ IEEE 802.11
⊞ Logical-Link Control
⊞ Internet Protocol, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3424 (3424), Seq: 10058, Ack: 11894, Len: 331
⊞ [Reassembled TCP Segments (603 bytes): #712207(272), #712208(331)]
⊞ Hypertext Transfer Protocol
⊟ MSN Messenger Service
    MSG [redacted]@hotmail.com Cecilia 95\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/x-msmsgscontrol\r\n
    TypingUser: [redacted]@hotmail.com\r\n
    \r\n
    \r\n
    MSG [redacted]@hotmail.com Cecilia 157\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0\r\n
    \r\n
    hongkong, beijing, shanghai, seoul
```

```
0100  2d 56 65 72 73 69 6f 6e  3a 20 31 2e 30 0d 0a 43   -Version : 1.0..C
0110  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0120  74 2f 70 6c 61 69 6e 3b  20 63 68 61 72 73 65 74   t/plain;  charset
0130  3d 55 54 46 2d 38 0d 0a  58 2d 4d 4d 53 2d 49 4d   =UTF-8.. X-MMS-IM
0140  2d 46 6f 72 6d 61 74 3a  20 46 4e 3d 4d 53 25 32   -Format:  FN=MS%2
0150  30 53 68 65 6c 6c 25 32  30 44 6c 67 3b 20 45 46   0Shell%2 0Dlg; EF
0160  3d 3b 20 43 4f 3d 30 3b  20 43 53 3d 30 3b 20 50   =; CO=0;  CS=0; P
0170  46 3d 30 0d 0a 0d 0a 68  6f 6e 67 6b 6f 6e 67 2c   F=0....h ongkong,
0180  20 62 65 69 6a 69 6e 67  2c 20 73 68 61 6e 67 68    beijing , shangh
0190  61 69 2c 20 73 65 6f 75  6c                        ai, seou l
```

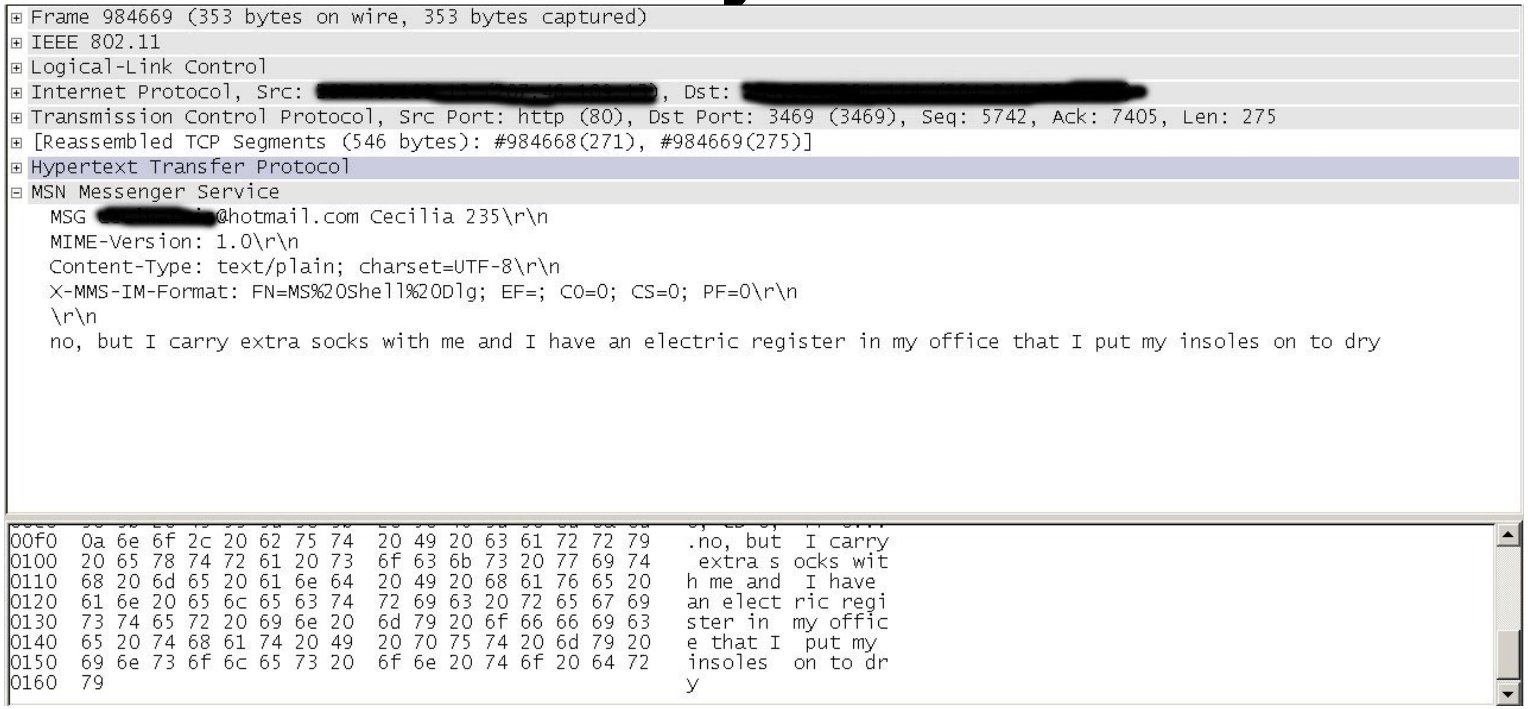
Frame #3: For How Long?



```
⊞ Frame 721180 (253 bytes on wire, 253 bytes captured)
⊞ IEEE 802.11
⊞ Logical-Link Control
⊞ Internet Protocol, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3424 (3424), Seq: 12684, Ack: 15309, Len: 175
⊞ [Reassembled TCP Segments (446 bytes): #721179(271), #721180(175)]
⊞ Hypertext Transfer Protocol
⊟ MSN Messenger Service
    MSG [redacted]@hotmail.com Cecilia 135\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0\r\n
    \r\n
    2 or 3 weeks
```

```
0080  6f 6e 3a 20 31 2e 30 0d  0a 43 6f 6e 74 65 6e 74   on: 1.0. .Content
0090  2d 54 79 70 65 3a 20 74  65 78 74 2f 70 6c 61 69   -Type: t ext/plai
00a0  6e 3b 20 63 68 61 72 73  65 74 3d 55 54 46 2d 38   n; chars et=UTF-8
00b0  0d 0a 58 2d 4d 4d 53 2d  49 4d 2d 46 6f 72 6d 61   ..X-MMS- IM-Forma
00c0  74 3a 20 46 4e 3d 4d 53  25 32 30 53 68 65 6c 6c   t: FN=MS %20Shell
00d0  25 32 30 44 6c 67 3b 20  45 46 3d 3b 20 43 4f 3d   %20Dlg;  EF=; CO=
00e0  30 3b 20 43 53 3d 30 3b  20 50 46 3d 30 0d 0a 0d   0; CS=0;  PF=0...
00f0  0a 32 20 6f 72 20 33 20  77 65 65 6b 73            .2 or 3  weeks
```

Frame #4: Social Engineering Anyone?



```
⊞ Frame 984669 (353 bytes on wire, 353 bytes captured)
⊞ IEEE 802.11
⊞ Logical-Link Control
⊞ Internet Protocol, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3469 (3469), Seq: 5742, Ack: 7405, Len: 275
⊞ [Reassembled TCP Segments (546 bytes): #984668(271), #984669(275)]
⊞ Hypertext Transfer Protocol
⊟ MSN Messenger Service
    MSG [redacted]@hotmail.com Cecilia 235\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0\r\n
    \r\n
    no, but I carry extra socks with me and I have an electric register in my office that I put my insoles on to dry
```

```
00f0  0a 6e 6f 2c 20 62 75 74  20 49 20 63 61 72 72 79   .no, but  I carry
0100  20 65 78 74 72 61 20 73  6f 63 6b 73 20 77 69 74    extra s ocks wit
0110  68 20 6d 65 20 61 6e 64  20 49 20 68 61 76 65 20   h me and  I have
0120  61 6e 20 65 6c 65 63 74  72 69 63 20 72 65 67 69   an elect ric regi
0130  73 74 65 72 20 69 6e 20  6d 79 20 6f 66 66 69 63   ster in  my offic
0140  65 20 74 68 61 74 20 49  20 70 75 74 20 6d 79 20   e that I  put my
0150  69 6e 73 6f 6c 65 73 20  6f 6e 20 74 6f 20 64 72   insoles  on to dr
0160  79                                                 y
```

- I am stuck here at the airport in Seoul. Can you please send me a copy of that report again (use my personal email: pseudoboss@hotmail.com). Thanks. Oh, and Cecilia, be careful with that heater and your insoles o.k.? ;-)

Seepage From Devices:

- Laptops, PDAs, and mobile phones will give up a lot information that may not seem important but combined with other info can paint a picture for malicious intruders.
- A very simple example is to set up a Bluetooth device on a laptop and perform a scan of other Bluetooth-enabled devices (laptops, smart phones) in the vicinity and pair up with them.
- After that it is simple matter of

Other Examples:

- Wifi packets
- DHCP Broadcast
- NetBIOS/SMB Broadcast
- DNS/Bonjour Requests
  - **Bonjour**, formerly **Rendezvous**, is Apple Inc’s trade name for its implementation of Zeroconf, a service discovery protocol.
  - Bonjour locates devices such as printers, as well as other computers, and the services that those devices offer on a LAN using DNS service records.

Wifi Packets - KARMA

- When a Wifi enabled laptop starts up it will look for a list of “known networks” or networks it has previously associated with before.
- This list can be used to determine the location history of usage for the laptop.
- KARMA is a set of tools for assessing the security of wireless clients at multiple layers.
- Wireless sniffing tools discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames.
- From there, individual clients can be targeted by creating a Rogue AP for one of their probed networks (which they may join automatically) or using a custom driver that responds to probes and association requests for any SSID.
- Higher-level fake services can then capture credentials or exploit client-side vulnerabilities on the host.

A Simple Scenario:

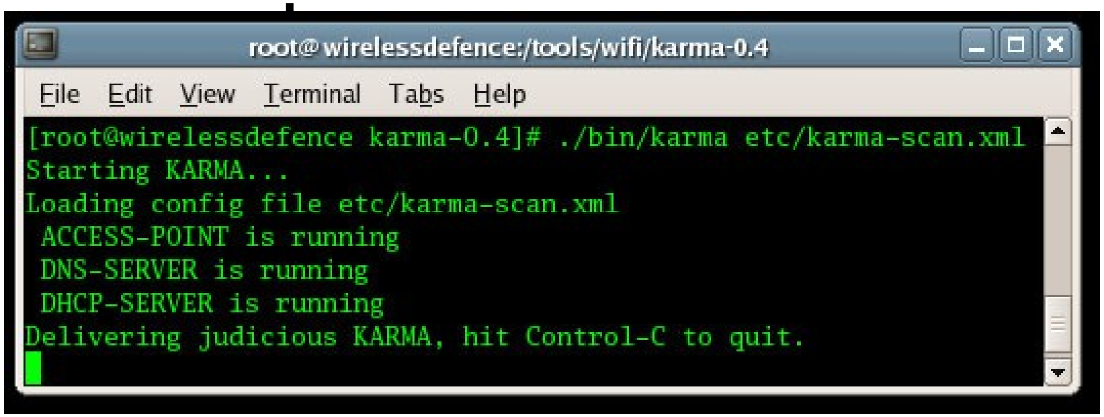
- Alice has a wireless access point at home with an SSID of "linksys", which she has successfully set up and connected to with her laptop.
- Alice goes to the airport (or train station or coffee shop) and opens her laptop.
- Bob, who is sitting next to Alice, has a laptop configured with an ad-hoc network advertising an SSID of "linksys“.
- Alice's laptop when started looks for the SSID of "linksys", and attaches to Bob's ad-hoc network.
- The next time Alice boots up the laptop when the Ethernet cable is not attached and there is no "linksys" SSID in range, Alice starts advertising an ad-hoc network with an SSID of "linksys".
- This is basically a configuration error that spreads virus-like from laptop to laptop.
- In field tests, numerous ad-hoc SSIDs such as "linksys", "dlink", "tmobile", "hpsetup", and others

Karma Project

- A set of Wifi tools that will allow an attacker to masquerade as a variety of servers to attract unsuspecting target machines:
  - Respond to WiFi “probe”
  - Respond with DHCP address
  - Respond to ARPs
  - Respond to NetBIOS queries
  - Respond to SMB/DCE-RPC connections
  - Respond to DNS queries
  - Respond to SMTP connections

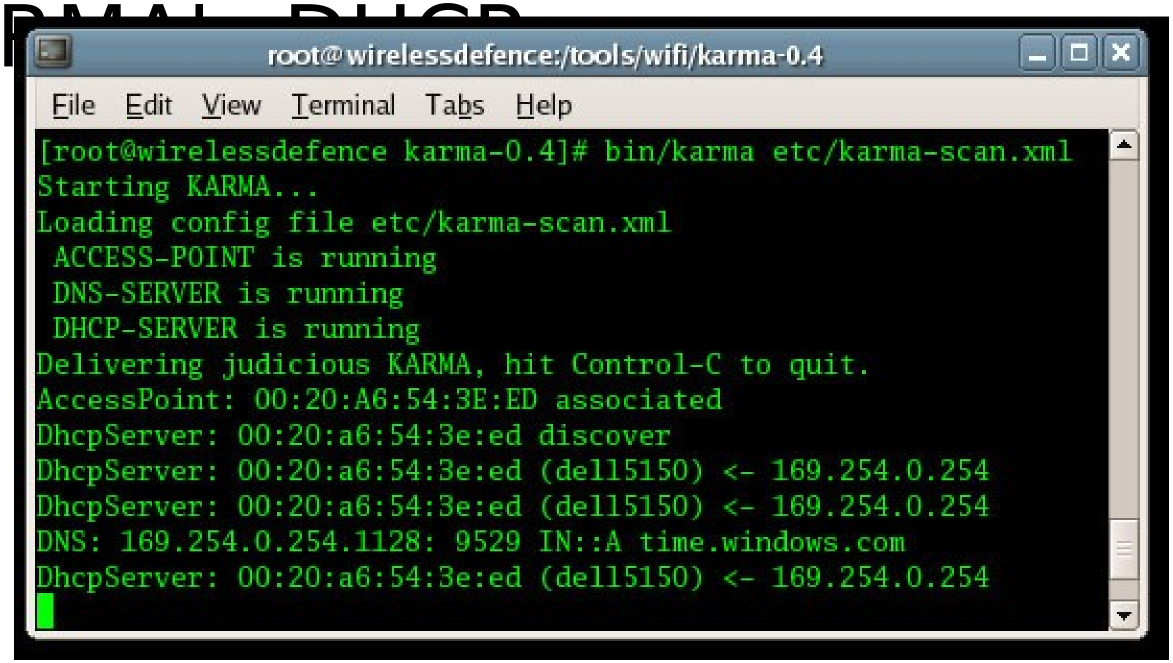
Karma Screenshots:

- Once Karma is installed and invoked, the rogue services are started.
- Any probing clients will now connect to KARMA on the rogue machine using whichever SSID their machine ch



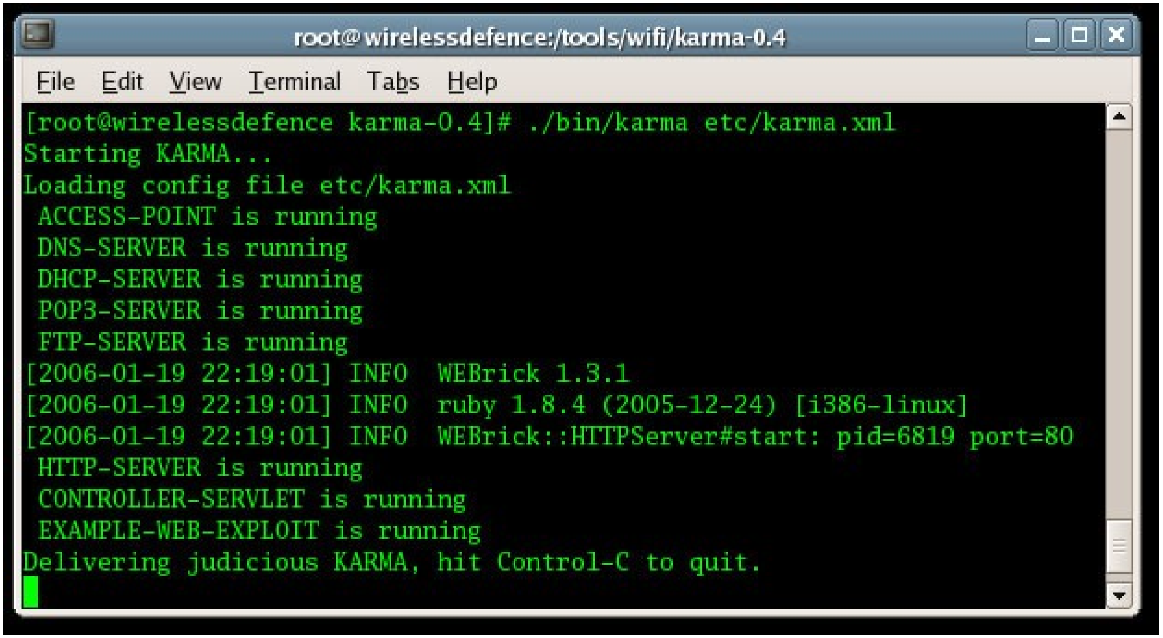
```
[root@wirelessdefence karma-0.4]# ./bin/karma etc/karma-scan.xml
Starting KARMA...
Loading config file etc/karma-scan.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
Delivering judicious KARMA, hit Control-C to quit.
```

- The next screenshot shows that an unsuspecting client received the IP address **169.254.0.254** from KARMA's DHCP



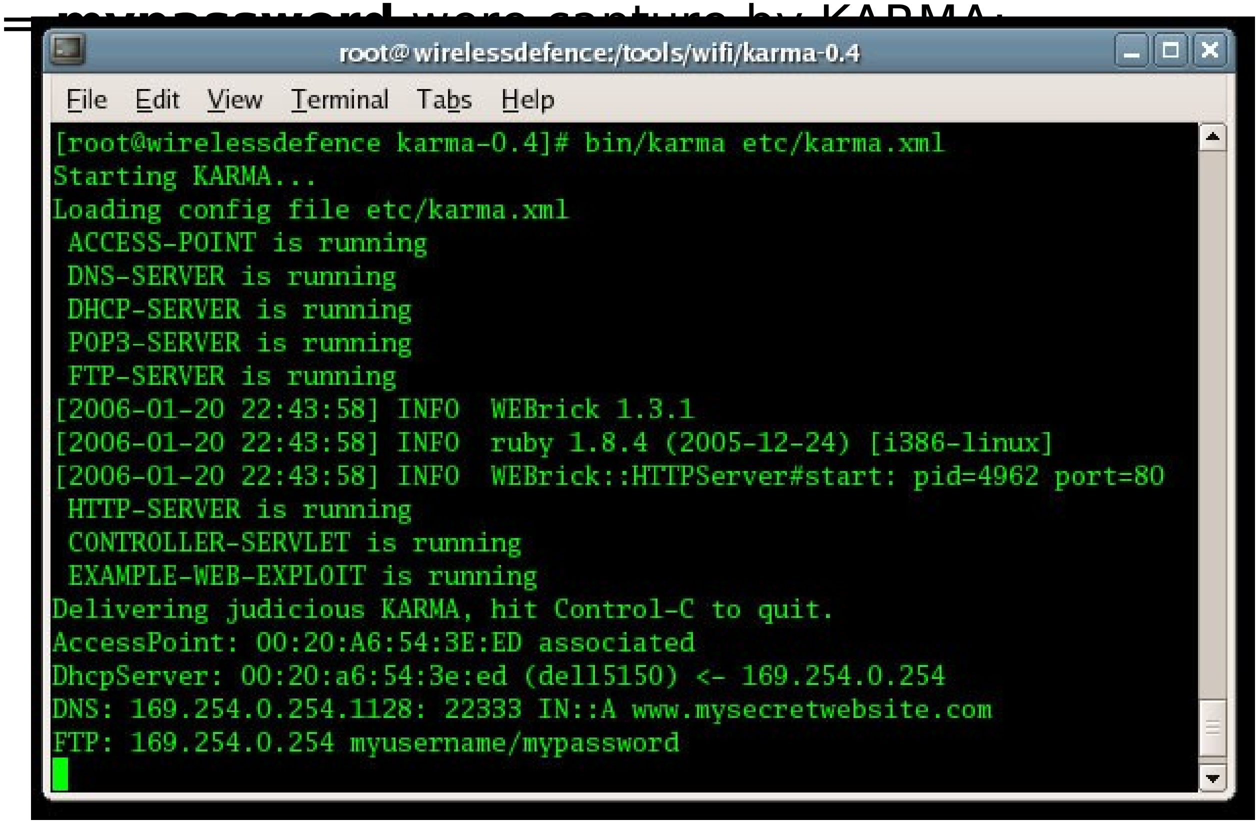
```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma-scan.xml
Starting KARMA...
Loading config file etc/karma-scan.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
Delivering judicious KARMA, hit Control-C to quit.
AccessPoint: 00:20:A6:54:3E:ED associated
DhcpServer: 00:20:a6:54:3e:ed discover
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 9529 IN::A time.windows.com
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
```

- The following invocation shows how KARMA can offer a variety of services (POP, FTP and HTTP) for any curious clien


root@wirelessdefence:/tools/wifi/karma-0.4
File Edit View Terminal Tabs Help

```
[root@wirelessdefence karma-0.4]# ./bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
 POP3-SERVER is running
 FTP-SERVER is running
[2006-01-19 22:19:01] INFO  WEBrick 1.3.1
[2006-01-19 22:19:01] INFO  ruby 1.8.4 (2005-12-24) [i386-linux]
[2006-01-19 22:19:01] INFO  WEBrick::HTTPServer#start: pid=6819 port=80
 HTTP-SERVER is running
 CONTROLLER-SERVLET is running
 EXAMPLE-WEB-EXPLOIT is running
Delivering judicious KARMA, hit Control-C to quit.
```

- The following is an illustration of an attempted FTP connection to **www.mysecretwebsite.com** which actually was received by KARMA and the users credentials - username = **myusername** and password = **mypassword** were capture by KARMA:

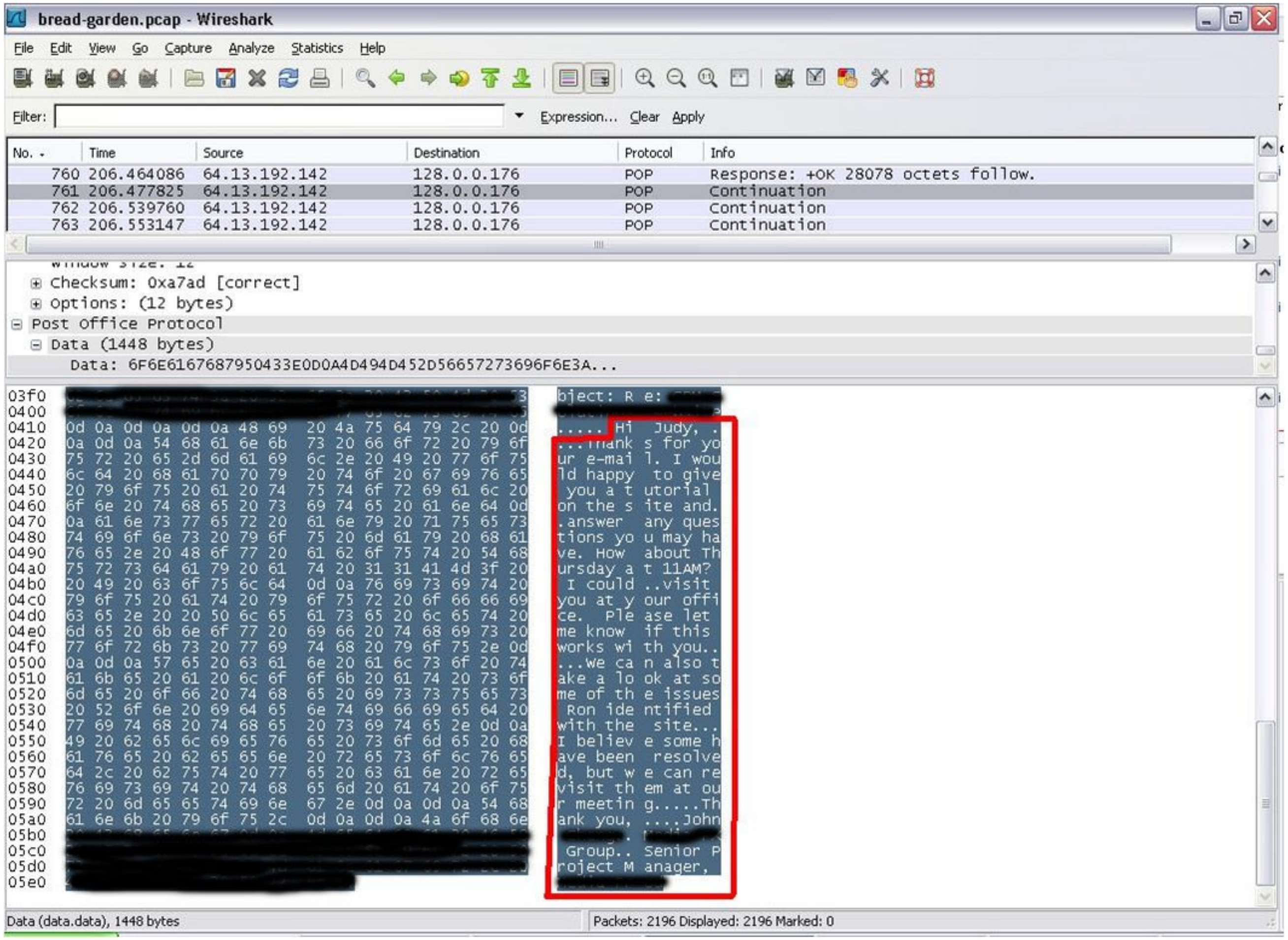


```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
 POP3-SERVER is running
 FTP-SERVER is running
[2006-01-20 22:43:58] INFO  WEBrick 1.3.1
[2006-01-20 22:43:58] INFO  ruby 1.8.4 (2005-12-24) [i386-linux]
[2006-01-20 22:43:58] INFO  WEBrick::HTTPServer#start: pid=4962 port=80
 HTTP-SERVER is running
 CONTROLLER-SERVLET is running
 EXAMPLE-WEB-EXPLOIT is running
Delivering judicious KARMA, hit Control-C to quit.
AccessPoint: 00:20:A6:54:3E:ED associated
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```

Using The Information

- The following is an actual session capture carried out at an unprotected wireless LAN at a local Bread Garden that could very easily be used to compromise the victim’s security. (Identities have been sanitized and or changed to protect the real identities of the careless individuals!).
- Basically, the “attackers” were able to capture an entire email regarding a meeting between a vice-president and other employees from two separate companies.
- This information was gathered when John Smith was checking his email using Microsoft Outlook.
- The meeting location was 2xxx Eton St. in Vancouver at 1100 hrs on a Thursday.
- With this information a malicious attacker has several options open to them.
- For example, send a spoofed email to cancel the meeting or change locations so the parties would have trouble meeting – this will cost them valuable business time and lost productivity.
- Another option would be to spy on them during the meeting for the purpose of finding physical information about the targets.
- Yet another option is to use their email information to send disinformation to others within or outside the company.

Captured Email:



bread-garden.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time        Source          Destination   Protocol  Info
  760 206.464086  64.13.192.142   128.0.0.176   POP       Response: +OK 28078 octets follow.
  761 206.477825  64.13.192.142   128.0.0.176   POP       Continuation
  762 206.539760  64.13.192.142   128.0.0.176   POP       Continuation
  763 206.553147  64.13.192.142   128.0.0.176   POP       Continuation
```

```
   Window size: 12
 ⊞ Checksum: 0xa7ad [correct]
 ⊞ Options: (12 bytes)
⊟ Post Office Protocol
 ⊟ Data (1448 bytes)
     Data: 6F6E6167687950433E0D0A4D494D452D56657273696F6E3A...
```

```
03f0  [redacted]                                          bject: R e: [redacted]
0400                                                      [redacted]
0410  0d 0a 0d 0a 0d 0a 48 69  20 4a 75 64 79 2c 20 0d   ......Hi  Judy, .
0420  0a 0d 0a 54 68 61 6e 6b  73 20 66 6f 72 20 79 6f   ...Thank s for yo
0430  75 72 20 65 2d 6d 61 69  6c 2e 20 49 20 77 6f 75   ur e-mai l. I wou
0440  6c 64 20 68 61 70 70 79  20 74 6f 20 67 69 76 65   ld happy  to give
0450  20 79 6f 75 20 61 20 74  75 74 6f 72 69 61 6c 20    you a t utorial
0460  6f 6e 20 74 68 65 20 73  69 74 65 20 61 6e 64 0d   on the s ite and.
0470  0a 61 6e 73 77 65 72 20  61 6e 79 20 71 75 65 73   .answer  any ques
0480  74 69 6f 6e 73 20 79 6f  75 20 6d 61 79 20 68 61   tions yo u may ha
0490  76 65 2e 20 48 6f 77 20  61 62 6f 75 74 20 54 68   ve. How  about Th
04a0  75 72 73 64 61 79 20 61  74 20 31 31 41 4d 3f 20   ursday a t 11AM?
04b0  20 49 20 63 6f 75 6c 64  0d 0a 76 69 73 69 74 20    I could ..visit
04c0  79 6f 75 20 61 74 20 79  6f 75 72 20 6f 66 66 69   you at y our offi
04d0  63 65 2e 20 20 50 6c 65  61 73 65 20 6c 65 74 20   ce.  Ple ase let
04e0  6d 65 20 6b 6e 6f 77 20  69 66 20 74 68 69 73 20   me know  if this
04f0  77 6f 72 6b 73 20 77 69  74 68 20 79 6f 75 2e 0d   works wi th you..
0500  0a 0d 0a 57 65 20 63 61  6e 20 61 6c 73 6f 20 74   ...We ca n also t
0510  61 6b 65 20 61 20 6c 6f  6f 6b 20 61 74 20 73 6f   ake a lo ok at so
0520  6d 65 20 6f 66 20 74 68  65 20 69 73 73 75 65 73   me of th e issues
0530  20 52 6f 6e 20 69 64 65  6e 74 69 66 69 65 64 20    Ron ide ntified
0540  77 69 74 68 20 74 68 65  20 73 69 74 65 2e 0d 0a   with the  site...
0550  49 20 62 65 6c 69 65 76  65 20 73 6f 6d 65 20 68   I believ e some h
0560  61 76 65 20 62 65 65 6e  20 72 65 73 6f 6c 76 65   ave been  resolve
0570  64 2c 20 62 75 74 20 77  65 20 63 61 6e 20 72 65   d, but w e can re
0580  76 69 73 69 74 20 74 68  65 6d 20 61 74 20 6f 75   visit th em at ou
0590  72 20 6d 65 65 74 69 6e  67 2e 0d 0a 0d 0a 54 68   r meetin g.....Th
05a0  61 6e 6b 20 79 6f 75 2c  0d 0a 0d 0a 4a 6f 68 6e   ank you, ....John
05b0  [redacted]                                          [redacted]. [redacted]
05c0                                                       Group.. Senior P
05d0                                                      roject M anager,
05e0                                                      [redacted]
```

Data (data.data), 1448 bytes | Packets: 2196 Displayed: 2196 Marked: 0

The Gist of It:

- X-Mailer: Microsoft Office Outlook 11
-
- Return-path: "Judy Wong" <judy@bigsolutions.ca>
- Envelope-to: "John Smith" <john@mediagroup.com>
-
- Subject: RE: BIG Solutions website
-
- This is a multi-part message in MIME format.
-
- ------=_NextPart_000_0030_01C877C0.EE453BC0
- Content-Type: text/plain;
- charset="us-ascii"
- Content-Transfer-Encoding: 7bit
-
- Hi John,
-
- Yes, Thursday at 11:00 a.m. would be fine.   Leanne and I will be here!
-
- Regards,
-
-
-
- Judy Wong
-
- Vice-President, Administration
-
- Big Solutions Ltd.
-

- From: John Smith [mailto:john@mediagroup.com]
- Sent: February 22, 2008 3:47 PM
- To: Judy Wong
- Cc: A whole bunch of people!
- Subject: Re: Big Solutions website
-
-
- Hi Judy,
-
- Thanks for your e-mail. I would happy to give you a tutorial on the site and
- answer any questions you may have. How about Thursday at 11AM? I could
- visit you at your office. Please let me know if this works with you.
-
- We can also take a look at some of the issues Ron identified with the site.
- I believe some have been resolved, but we can revisit them at our meeting.
-
- Thank you,
-
- John Smith
- Media Group
- Senior Project Manager, Media Producer
- Phone: (604) 3xx-xxxx
- Email: john@mediagroup.com
- web: <http://www.........>

- And so it goes...

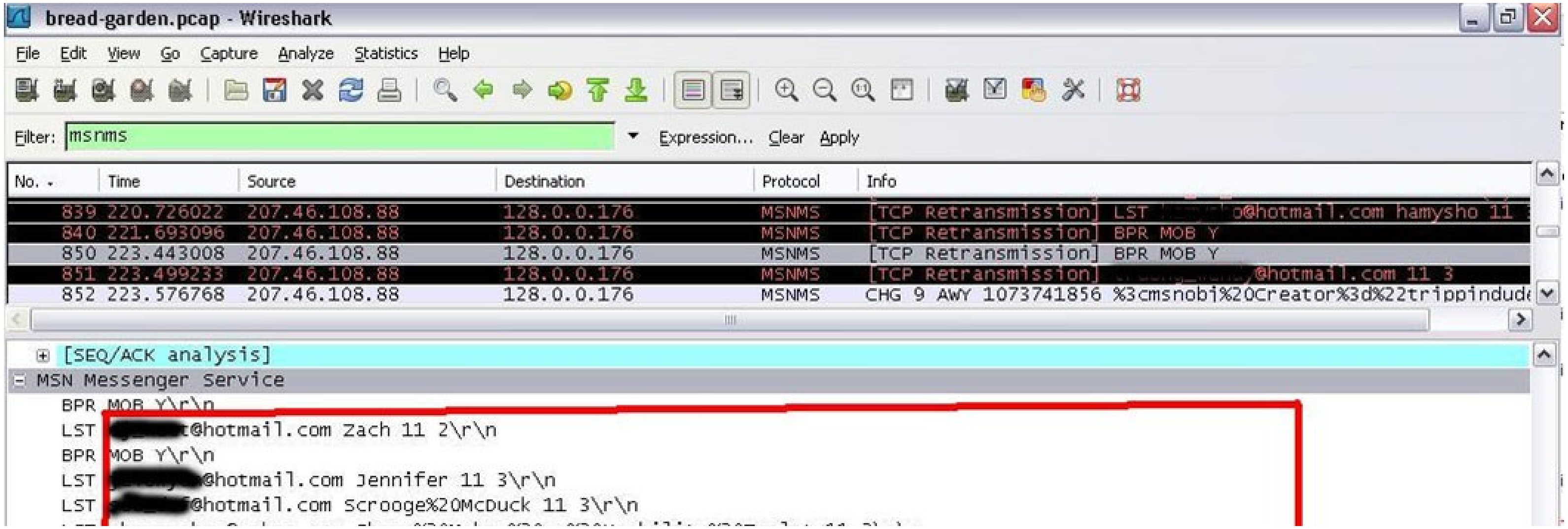
Applying The Information

- So what can you determine about this if you know BigSolutions and MediaGroup are rival companies?
  - Sounds like a merger or buyout.
- Since we know John’s pop password we can try it against MediaGroup webmail client, he might use the same password.
- Social Engineering – “Hey wasn’t that a lousy lunch we had at that meeting….Btw, run this program to update your accounting software.”

If All that is Not Enough!

- It appears John Smith uses MSN messenger and he actually logged on and started using it, yielding a lot of additional information.
- His entire contact listing was harvested and information on his contacts was gathered via checking Windows Live, Myspace, and Youtube.
- Going through the usernames of each contact, the attackers were able to grab information by adding their usernames to the end of website URLs that would take them to their homepage if it existed.
- Examples of such URLs would be:
- http://spaces.live.com/profile.aspx?mem=username
- http://www.myspace.com/username
- http://www.youtube.com/username

MSN Contact List:

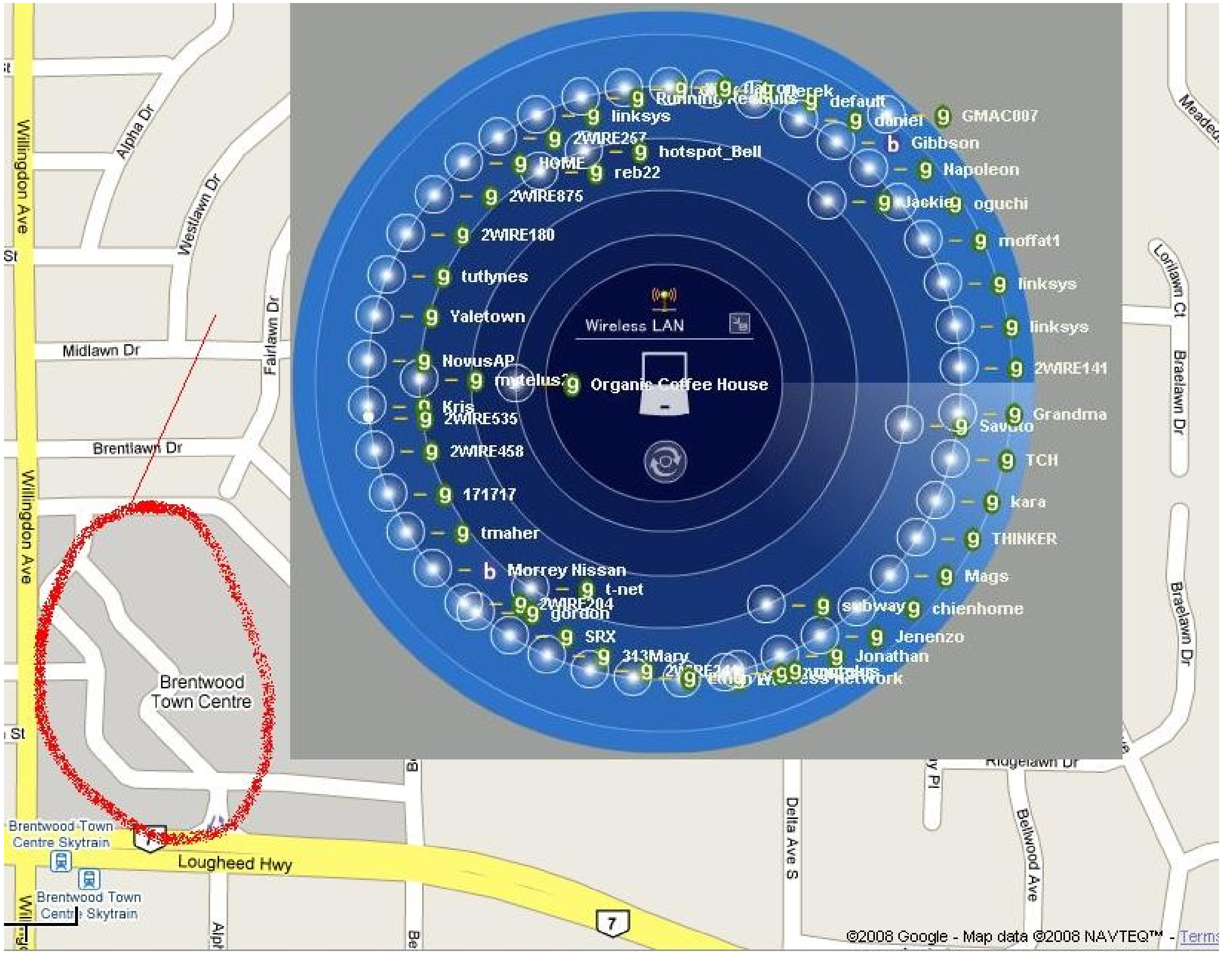

bread-garden.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: msnms
Expression... Clear Apply

```
No.  Time        Source          Destination   Protocol  Info
839 220.726022  207.46.108.88   128.0.0.176   MSNMS     [TCP Retransmission] LST [redacted]o@hotmail.com hamysho 11
840 221.693096  207.46.108.88   128.0.0.176   MSNMS     [TCP Retransmission] BPR MOB Y
850 223.443008  207.46.108.88   128.0.0.176   MSNMS     [TCP Retransmission] BPR MOB Y
851 223.499233  207.46.108.88   128.0.0.176   MSNMS     [TCP Retransmission] [redacted]@hotmail.com 11 3
852 223.576768  207.46.108.88   128.0.0.176   MSNMS     CHG 9 AWY 1073741856 %3cmsnobj%20Creator%3d%22trippindude
```

```
⊞ [SEQ/ACK analysis]
⊟ MSN Messenger Service
    BPR MOB Y\r\n
    LST [redacted]t@hotmail.com Zach 11 2\r\n
    BPR MOB Y\r\n
    LST [redacted]@hotmail.com Jennifer 11 3\r\n
    LST [redacted]@hotmail.com Scrooge%20McDuck 11 3\r\n
```

- The partial contact list clearly provides enough details for an attacker to perform a myriad of social engineering and identity theft exploits.
- For example a phone number was obtained for Jennifer, who is a 27 year old female living in Vancouver and is single.
- Stalkers could make great use of wireless sniffing. Any of John’s contact’s emails could be spoofed in order to persuade him to open a Trojan Virus.
- This would be most effective if we got him to open this virus on his work computer and have it spread around his entire company’s network silently. “Hey John check out this video of me. See attachment”.

An Abundance of Targets



Tools

- To start of with, you will need some of the basic sniffing tools to capture the information, for example:
  - Wireless sniffing kit (Wireless card that works with Wireshark, external antennae)
  - Kismet, Aircrack, Airodump
  - Dsniff or Ettercap (active sniffing)
- For more sophisticated data stealing there is a suit of tools called “Sidejack”

Sidejacking – Hamster and Ferret

- Sidejacking is the process of sniffing cookie information, then replaying them against websites in order to clone a victim’s session.
- Note that this is quite different from typical MITM attacks.
- An MITM attack actually intrudes upon and existing session and actually interferes with it.
- Sidejacking is a passive technique that does not interfere with an existing or original session.
- The victim continues to use his/her session blissfully unaware that we are also in his/her account .

FERRET – Data seepage monitor

- Ferret can be used very effective to capture data seepage.
- Similar to a password sniffer, but sniffs more than just passwords
- It can sniff legitimate operations and formats them in a way that makes it very convenient to view with a tool like Hamster.
- Supported Protocols: DHCP, SNMP, DNS, HTTP, AIM, MSN-MSGR, Yahoo

Protecting Against Data Leakage and Seepage

- Use Personal firewalls
  - Don’t allow any traffic unless you are on a trusted network.
  - Unfortunately users will just blindly click through them
- Set strict Corporate Polices
  - Unfortunately these and never really monitored much less enforced.
- The best solution for this is simply to be aware of the vulnerabilities of unsecured and open networks
  - Everyone really doesn’t need to work from a coffee shop.