20 – How did that Happen?

Case Files from the Network Forensics World

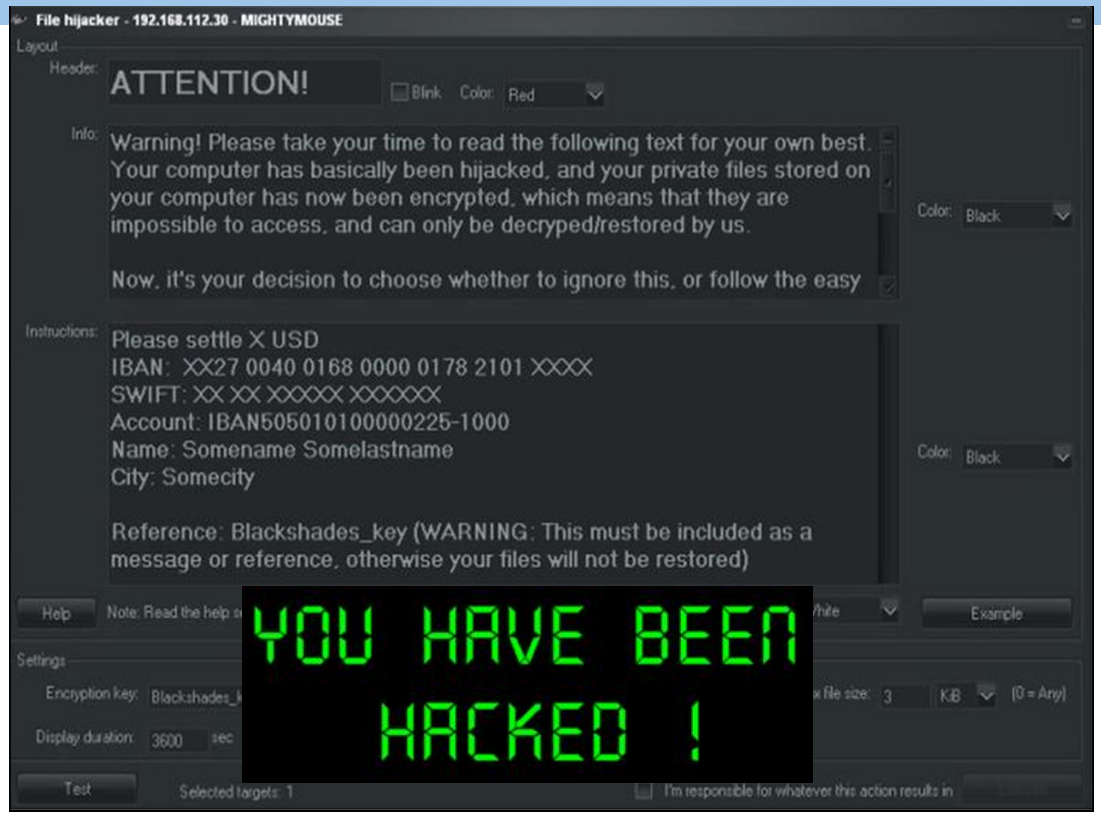
Phill "Sherlock" Shade
Merlion's Keep Consulting

Phillip "Sherlock" Shade (Phill)

phill.shade@gmail.com

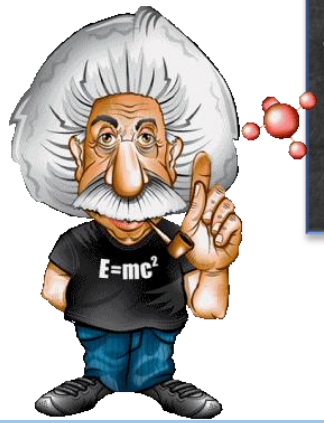
- Certified instructor and internationally recognized network security and forensics expert with more than 30 years of experience
- Retired US Navy and the founder of Merlion's Keep Consulting, a professional services company specializing in network and forensics analysis
- A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, and the IEEE and volunteer at Cyber Warfare Forum Initiative
- Holds numerous certifications, including Certified Network Expert (CNX)-Ethernet, CCNA, Certified Wireless Network Administrator (CWNA), and WildPackets Certified Network Forensics Analysis Expert (WNAX)
- Certified Wireshark University, Sniffer University and Planet 3 Wireless instructor

Thank You for Joining Us Today



Today's Agenda

1. Troubleshooting vs. Forensics
2. Case Study #1 Application Based Attacks / Exploits
3. Case Study #2 – Bot's and Botnets – Zbots & Mirai
4. Case Study #3 – Attacking from Within – Man in the Middle
5. Case Study #4 – A fly on the Wall – Call / Data Interception



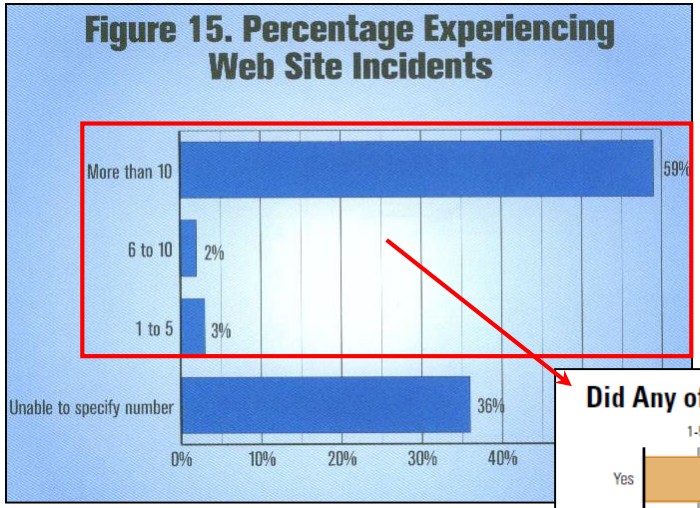
Troubleshooting vs. Forensics

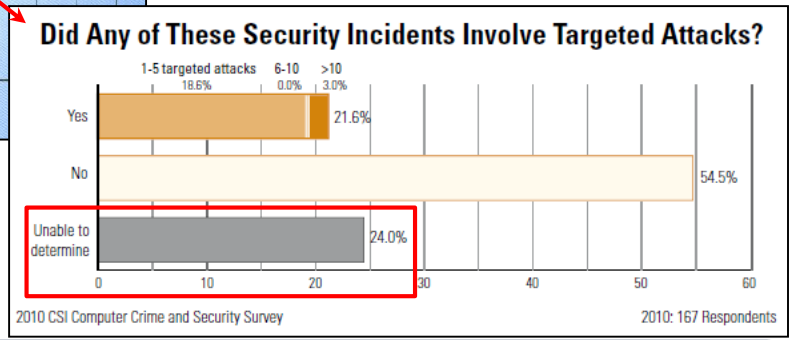
1. What is the cause of my performance issue?
2. How do I locate and resolve the performance issue?

1. What Damage has been Done?
2. Who was the intruder and how did they penetrate the existing security precautions?
2. Did the intruder leave anything such as a new user account, or perhaps some new type of Malware behind?
4. Is there sufficient data to analyze & reproduce the attack and verify the fix will work?

Application Based Attacks / Exploits…

An Interesting Statistic...





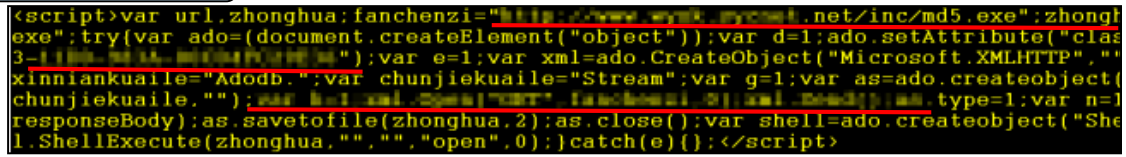
Web-based attacks and incidents continue to rise as more application become web-based.

Web-Based Hijack Exploit (1)

Web-Based Hijack Exploit (2)

Malicious Code Encoded:

Malicious Code Decoded:



Vulnerability - Clear-Text Protocols

- The following protocols send passwords in clear text:
  - Internet - HTTP / NNTP / IRC / Yahoo / AIM / MSN / Skype Chat
  - File transfer - FTP / TFTP / Most Peer-to-Peer Sharing Software
  - Email - POP3 / IMAP / SMTP
  - Network Monitoring - SNMP / RMON
  - Telnet
  - VoIP – Signaling Set-up (SIP, Megaco, SCCP, H.323, and Others?)

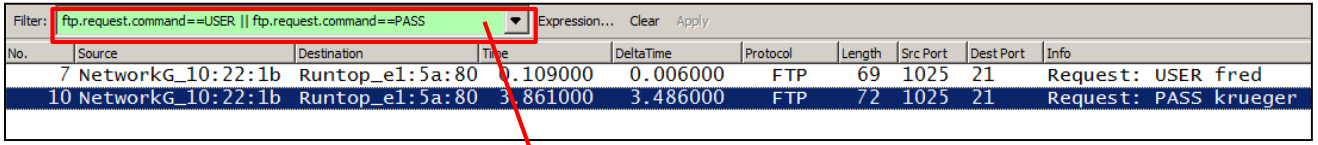
2017 Most Common Passwords Are...

#	Password	Change	#	Password	Change	#	Password	Change
1	123456	0	**11**	1234567	-4	**21**	superman	new
2	password	0	**12**	monkey	+5	**22**	696969	new
3	12345	+ 17	**13**	letmein	+1	**23**	123123	-12
4	12345678	-1	**14**	abc123	-9	**24**	batman	new
5	qwerty	-1	**15**	111111	-8	**25**	trustno1	-1
6	123456789	0	**16**	mustang	new	**26**	iloveyou	-17
7	1234	+9	**17**	access	new	**27**	adobe123	0
8	baseball	new	**18**	shadow	0	**28**	dvork	-10
9	dragon	new	**19**	master	new	**29**	admin	0
10	football	new	**20**	michael	new	**30**	administrator	0

Is yours here?

Hackers use 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)



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

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 take considerable time due to the number of combinations
    - Example: 5 character password:
    - 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

Sample Password Cracking...

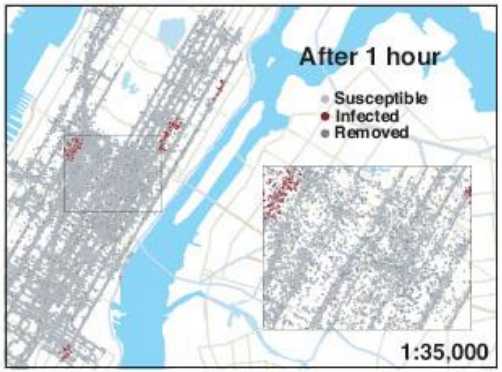
Source	Destination	Protocol	Info
200.90.26.22	67.161.39.233	TCP	33928 > ftp [SYN] Seq=0 Len=0 MSS=1460 TSV=118
67.161.39.233	200.90.26.22	TCP	ftp > 33928 [SYN, ACK] Seq=0 Ack=1 Win=262140
200.90.26.22	67.161.39.233	TCP	33928 > ftp [ACK] Seq=1 Ack=1 Win=5840 Len=0
67.161.39.233	200.90.26.22	FTP	Response: 220-creditus.com
200.90.26.22	67.161.39.233	TCP	33928 > ftp [ACK] Seq=1 Ack=48 Win=5840 Len=0
200.90.26.22	67.161.39.233	FTP	Request: USER Administrator
67.161.39.233	200.90.26.22	FTP	Response: 331 User name okay, Need password.
200.90.26.22	67.161.39.233	FTP	Request: PASS
67.161.39.233	200.90.26.22	FTP	Response: 530 Password not accepted.
200.90.26.22	67.161.39.233	FTP	Request: USER Administrator
67.161.39.233	200.90.26.22	FTP	Response: 331 User name okay, Need password.
200.90.26.22	67.161.39.233	FTP	Request: PASS abc123
67.161.39.233	200.90.26.22	FTP	Response: 530 Password not accepted.
200.90.26.22	67.161.39.233	FTP	Request: USER Administrator
67.161.39.233	200.90.26.22	FTP	Response: 331 User name okay, Need password.
200.90.26.22	67.161.39.233	FTP	Request: PASS password
67.161.39.233	200.90.26.22	FTP	Response: 530 Password not accepted.
200.90.26.22	67.161.39.233	FTP	Request: USER Administrator
67.161.39.233	200.90.26.22	FTP	Response: 331 User name okay, Need password.

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

Bot's and Botnets

Bots & Botnets

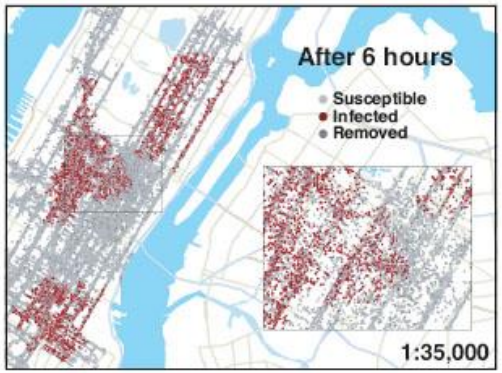
How Fast Do They Spread?



WiFi Networks and Malware Epidemiology

Hao Hua, Steven Myers, Vittoria Colizzac, and Alessandro Vespignani

Illustration of the spread of a worm through Manhattan in several time slices.



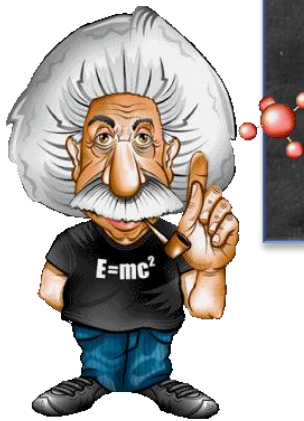
Case Study: Mirai (The Future) Bot Network

The Mirai botnet seeks out poorly secured Internet of Things (IoT) devices

Primarily targets online consumer devices such as IP cameras, home routers and medical equipment

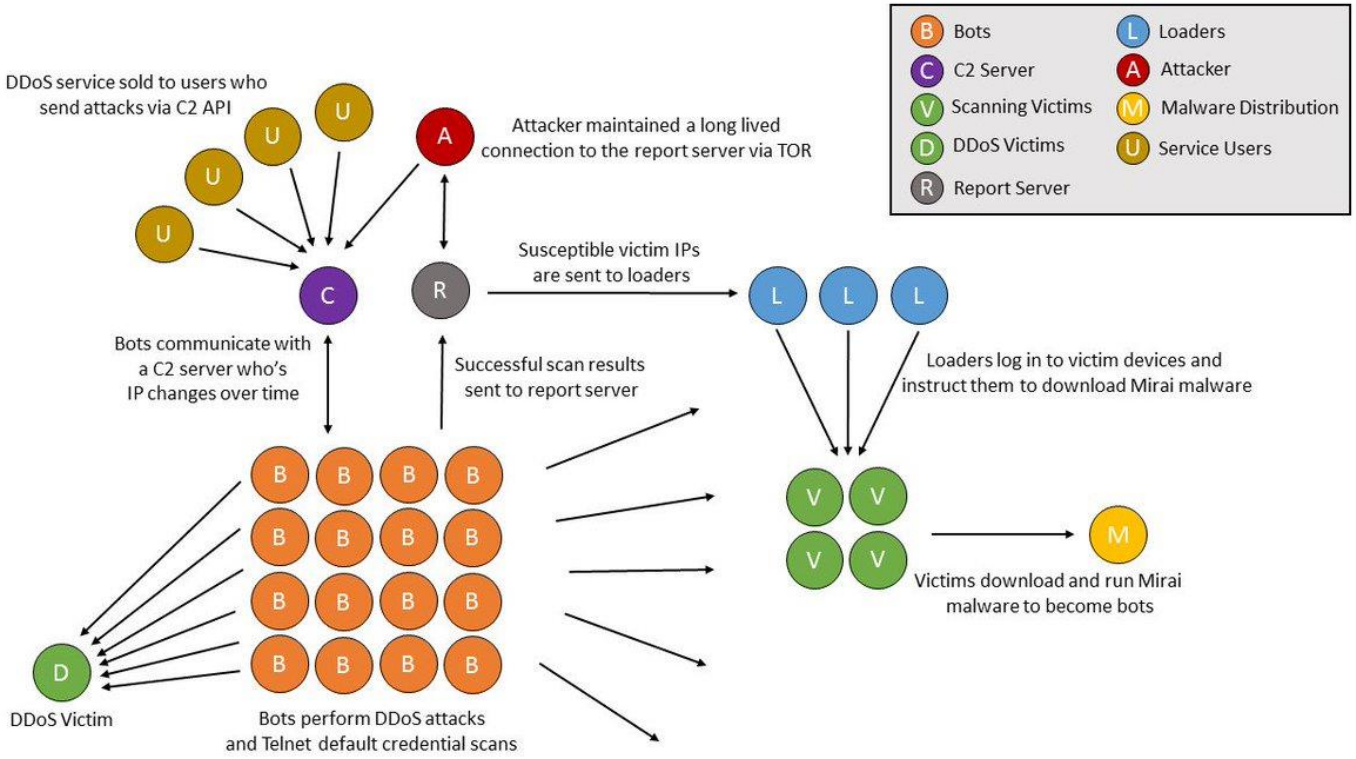
In October 2016, a massive DDoS attack target portions of the DNS architecture in the United States; in particular DYN

10.5 million Mirai-powered TCP SYN floods, peaking at 280 Gbps / 130 Mpps



Botnet of Things

Mirai Mechanism Mechanic's



Compromise Mechanism – Brute Force

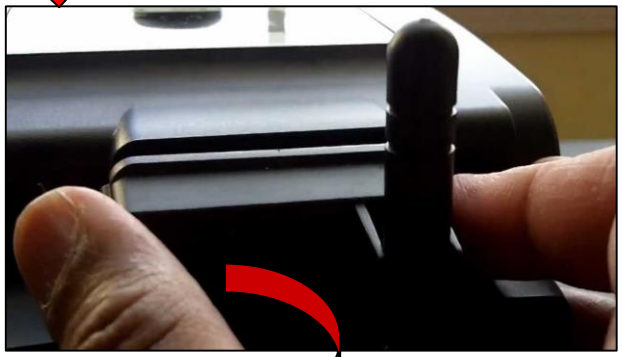
Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	

Sample Mirai Command / Control

No.	Source	Destination	Length	Protocol	Info
1	10.16.0.5	10.16.0.100	74	TCP	54650 → 23 [SYN] Seq=2031964219 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=136171 TSecr=
2	10.16.0.100	10.16.0.5	74	TCP	23 → 54650 [SYN, ACK] Seq=3643247368 Ack=2031964220 Win=28960 Len=0 MSS=1460 SACK_PERM=
3	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964220 Ack=3643247369 Win=29312 Len=0 TSval=136171 TSecr=998715
4	10.16.0.5	10.16.0.100	70	TELNET	Telnet Data ...
5	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964224 Win=28992 Len=0 TSval=998715 TSecr=136171
6	10.16.0.5	10.16.0.100	67	TELNET	Telnet Data ...
7	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964225 Win=28992 Len=0 TSval=998715 TSecr=136171
8	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
9	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964227 Win=28992 Len=0 TSval=1001217 TSecr=138674
10	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
11	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964227 Ack=3643247371 Win=29312 Len=0 TSval=138674 TSecr=1001217
12	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
13	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
14	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964229 Ack=3643247373 Win=29312 Len=0 TSval=153690 TSecr=1016233
15	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
16	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
17	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964231 Ack=3643247375 Win=29312 Len=0 TSval=168704 TSecr=1031248

Mac address: 08:00:27 Vendor: PcsCompu PCS Computer Systems GmbH

Here was the Device...



ResMed S9 Wireless Module

Mirai TCP SYN Attack (1)

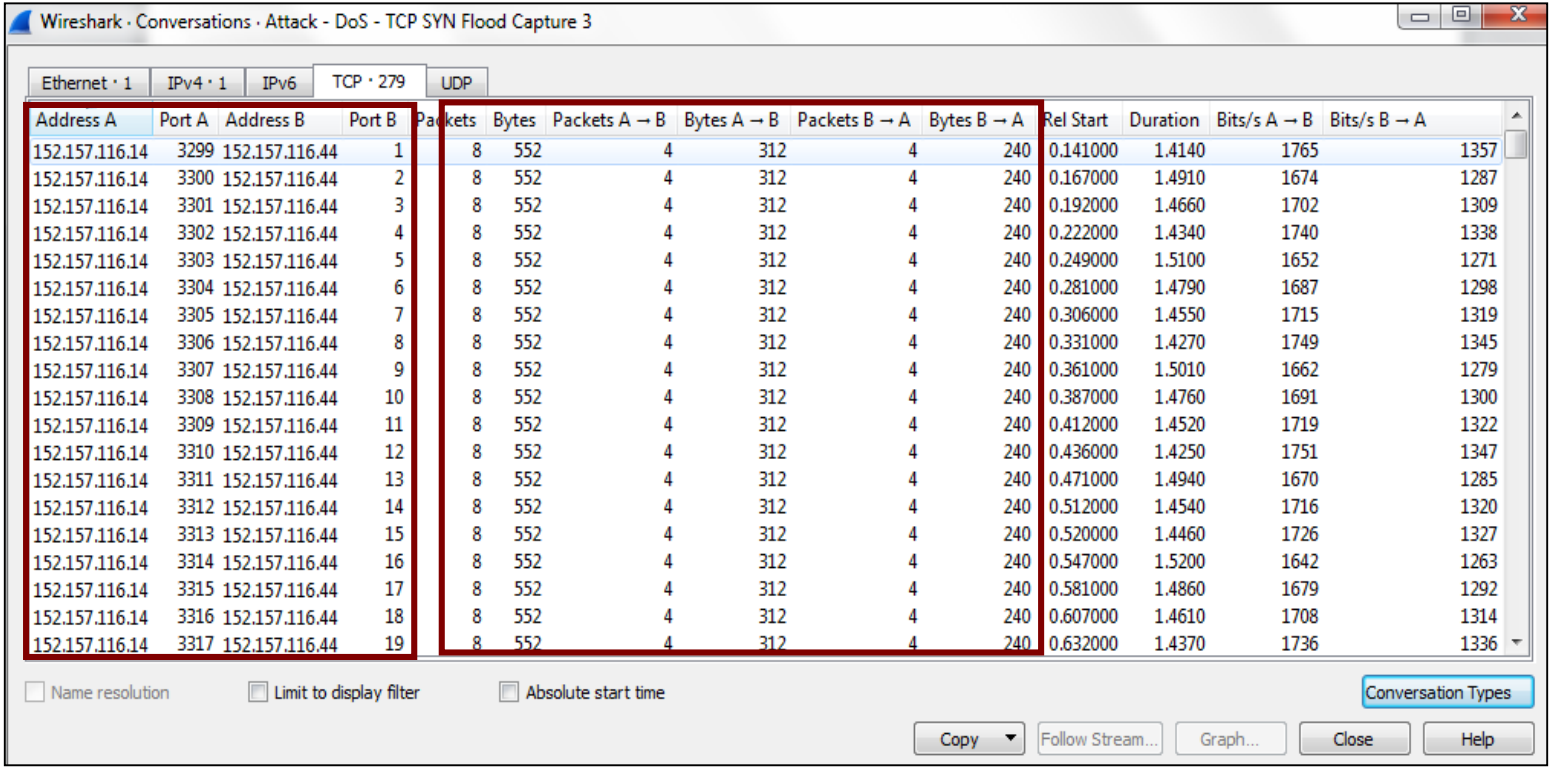
#1

	Source	Destination	Protocol	Info
1	10.8.0.184	10.8.0.131	TCP	2997 > http [SYN] Seq=0 Len=0 MSS=1460
2	10.8.0.184	10.8.0.131	TCP	2998 > http [SYN] Seq=0 Len=0 MSS=1460
3	10.8.0.184	10.8.0.131	TCP	2999 > http [SYN] Seq=0 Len=0 MSS=1460
4	10.8.0.184	10.8.0.131	TCP	3000 > http [SYN] Seq=0 Len=0 MSS=1460
5	10.8.0.184	10.8.0.131	TCP	3001 > http [SYN] Seq=0 Len=0 MSS=1460
6	10.8.0.184	10.8.0.131	TCP	3002 > http [SYN] Seq=0 Len=0 MSS=1460
7	10.8.0.184	10.8.0.131	TCP	3003 > http [SYN] Seq=0 Len=0 MSS=1460
8	10.8.0.184	10.8.0.131	TCP	3004 > http [SYN] Seq=0 Len=0 MSS=1460
9	10.8.0.184	10.8.0.131	TCP	3005 > http [SYN] Seq=0 Len=0 MSS=1460
10	10.8.0.184	10.8.0.131	TCP	3006 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.8.0.184	10.8.0.131	TCP	3007 > http [SYN] Seq=0 Len=0 MSS=1460
12	10.8.0.184	10.8.0.131	TCP	3008 > http [SYN] Seq=0 Len=0 MSS=1460
13	10.8.0.184	10.8.0.131	TCP	3009 > http [SYN] Seq=0 Len=0 MSS=1460
14	10.8.0.184	10.8.0.131	TCP	3010 > http [SYN] Seq=0 Len=0 MSS=1460
15	10.8.0.184	10.8.0.131	TCP	3011 > http [SYN] Seq=0 Len=0 MSS=1460
16	10.8.0.184	10.8.0.131	TCP	3012 > http [SYN] Seq=0 Len=0 MSS=1460
17	10.8.0.184	10.8.0.131	TCP	3013 > http [SYN] Seq=0 Len=0 MSS=1460
18	10.8.0.184	10.8.0.131	TCP	3014 > http [SYN] Seq=0 Len=0 MSS=1460

#2

	Source	Destination	Protocol	Info
1	152.157.116.14	152.157.116.44	ICMP	Echo (ping) request
2	152.157.116.44	152.157.116.14	ICMP	Echo (ping) reply
3	152.157.116.14	152.157.116.44	TCP	3299 > 1 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
4	152.157.116.44	152.157.116.14	TCP	1 > 3299 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
5	152.157.116.14	152.157.116.44	TCP	3300 > 2 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
6	152.157.116.44	152.157.116.14	TCP	2 > 3300 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
7	152.157.116.14	152.157.116.44	TCP	3301 > 3 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
8	152.157.116.44	152.157.116.14	TCP	3 > 3301 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
9	152.157.116.14	152.157.116.44	TCP	3302 > 4 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
10	152.157.116.44	152.157.116.14	TCP	4 > 3302 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
11	152.157.116.14	152.157.116.44	TCP	3303 > 5 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
12	152.157.116.44	152.157.116.14	TCP	5 > 3303 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
13	152.157.116.14	152.157.116.44	TCP	3304 > 6 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
14	152.157.116.44	152.157.116.14	TCP	6 > 3304 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
15	152.157.116.14	152.157.116.44	TCP	3305 > echo [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
16	152.157.116.44	152.157.116.14	TCP	echo > 3305 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
17	152.157.116.14	152.157.116.44	TCP	3306 > 8 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
18	152.157.116.44	152.157.116.14	TCP	8 > 3306 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0

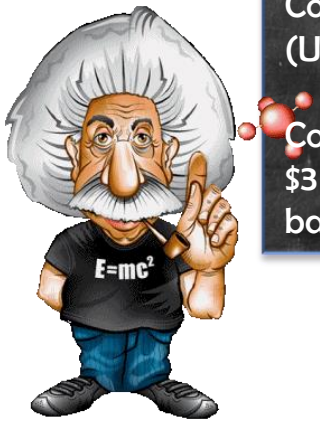
Mirai TCP SYN Attack (2)



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
152.157.116.14	3299	152.157.116.44	1	8	552	4	312	4	240	0.141000	1.4140	1765	1357
152.157.116.14	3300	152.157.116.44	2	8	552	4	312	4	240	0.167000	1.4910	1674	1287
152.157.116.14	3301	152.157.116.44	3	8	552	4	312	4	240	0.192000	1.4660	1702	1309
152.157.116.14	3302	152.157.116.44	4	8	552	4	312	4	240	0.222000	1.4340	1740	1338
152.157.116.14	3303	152.157.116.44	5	8	552	4	312	4	240	0.249000	1.5100	1652	1271
152.157.116.14	3304	152.157.116.44	6	8	552	4	312	4	240	0.281000	1.4790	1687	1298
152.157.116.14	3305	152.157.116.44	7	8	552	4	312	4	240	0.306000	1.4550	1715	1319
152.157.116.14	3306	152.157.116.44	8	8	552	4	312	4	240	0.331000	1.4270	1749	1345
152.157.116.14	3307	152.157.116.44	9	8	552	4	312	4	240	0.361000	1.5010	1662	1279
152.157.116.14	3308	152.157.116.44	10	8	552	4	312	4	240	0.387000	1.4760	1691	1300
152.157.116.14	3309	152.157.116.44	11	8	552	4	312	4	240	0.412000	1.4520	1719	1322
152.157.116.14	3310	152.157.116.44	12	8	552	4	312	4	240	0.436000	1.4250	1751	1347
152.157.116.14	3311	152.157.116.44	13	8	552	4	312	4	240	0.471000	1.4940	1670	1285
152.157.116.14	3312	152.157.116.44	14	8	552	4	312	4	240	0.512000	1.4540	1716	1320
152.157.116.14	3313	152.157.116.44	15	8	552	4	312	4	240	0.520000	1.4460	1726	1327
152.157.116.14	3314	152.157.116.44	16	8	552	4	312	4	240	0.547000	1.5200	1642	1263
152.157.116.14	3315	152.157.116.44	17	8	552	4	312	4	240	0.581000	1.4860	1679	1292
152.157.116.14	3316	152.157.116.44	18	8	552	4	312	4	240	0.607000	1.4610	1708	1314
152.157.116.14	3317	152.157.116.44	19	8	552	4	312	4	240	0.632000	1.4370	1736	1336

The Result...

Case Study: A Zeus Bot Network



Zeus is a do-it-yourself kit that allows the creation of custom malware with a point and click interface

In October 2010, a Zeus-bot network owned by "Kristina Svechinskaya" struck numerous major financial institutions principally in the U.S. and UK

Compromised accounts experienced a transaction "fee" of $0.99 (USD) during a 30-minute period

Cost is estimated to be in excess of $12.5 million (USD)
$3 million dollars from American banks and $9.5 million from UK banks

Sample Zbot Download

No.	Source	Destination	Time	DeltaTime	Protocol	Length	Info
1	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.000000	0.000000	TCP	62	1051 > 80 [SYN] Seq=3862586801 Win=6
2	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.219794	0.219794	TCP	62	80 > 1051 [SYN, ACK] Seq=4069722703
3	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.221962	0.002168	TCP	60	1051 > 80 [ACK] Seq=3862586802 Ack=4
4	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.223935	0.001973	HTTP	219	GET /ribbn.tar HTTP/1.1
5	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.444535	0.220600	TCP	54	80 > 1051 [ACK] Seq=4069722704 Ack=3
6	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449296	0.004761	TCP	1426	[TCP segment of a reassembled PDU]
7	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449819	0.000523	TCP	1426	[TCP segment of a reassembled PDU]
8	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.451005	0.001186	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
9	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.675966	0.224961	TCP	1426	[TCP segment of a reassembled PDU]
10	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.676292	0.000326	TCP	1426	[TCP segment of a reassembled PDU]
11	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.677088	0.000796	TCP	1426	[TCP segment of a reassembled PDU]
12	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.677937	0.000849	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
13	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.856904	0.178967	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
14	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.902107	0.045203	TCP	1426	[TCP segment of a reassembled PDU]

This example contains a copy of the “Ribbon – Zbot Worm” designed to install a remote back-door access point into the client machine

Network Forensics Case Study #3 -

Attacking From Within
–
The Man-in-The-Middle…

Anatomy of a Man-in-the-Middle Attack

- Attacker attempts to "insert" itself into a key location within the network
  - Favorite of industrial espionage and banking attackers
  - Originated within the early Ethernet community, returned with the advent of wide-spread Wi-Fi networking
- It will then launch a diversionary attack such as the classic "ARP-poison" to trick the targeted systems into accepting it as the "true" Server / Gateway / Router / Client / etc..
- The targeted devices will now send their traffic to the intruder
  - Intruder can copy / reinsert / manipulate the traffic

MiTM Hardware Tools

WiFi Pineapple
2.4/5 GHz a/b/g/n
Power over USB Ethernet Port
Power over USB Serial Port

PwnPlug

Real World Event – Software Vendor

- A major network analysis vendor had been working on a key project for 2 years…
  - One (1) week prior to product launch, a competitor suddenly trademarked the primary name for the product as well as all of the secondary's
  - Company was forced to research, develop and produce an entirely new marketing campaign, literature and product documentation

- A forensics investigation reveled that the software company had been "Man-in-the-Middle" victimized
  - Cost to company was in excess of four million (USD)

Scene of the Crime...

Sample ARP Poison (Before Color Rule)

arp

Expression... + TCP Syn TCP SA Malware HTTP

No.	Source	Destination	Length	Protocol	Info
6	AmbitMic_aa:af:80	Runtop_d9:0d:db	64	ARP	192.168.1.103 is at 00:d0:59:aa:af:80
7	AmbitMic_aa:af:80	AmbitMic_12:9b:01	64	ARP	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicate use of 192.168.1.103 detected!)
9	AmbitMic_aa:af:80	Runtop_d9:0d:db	64	ARP	Who has 192.168.1.1? Tell 192.168.1.103
10	Runtop_d9:0d:db	AmbitMic_aa:af:80	64	ARP	192.168.1.1 is at 00:20:78:d9:0d:db
11	AmbitMic_aa:af:80	AmbitMic_12:9b:01	64	ARP	Who has 192.168.1.103? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)
12	AmbitMic_12:9b:01	AmbitMic_aa:af:80	64	ARP	192.168.1.103 is at 00:d0:59:12:9b:01 (duplicate use of 192.168.1.1 detected!)
13	AmbitMic_aa:af:80	Runtop_d9:0d:db	64	ARP	192.168.1.103 is at 00:d0:59:aa:af:80
14	AmbitMic_aa:af:80	AmbitMic_12:9b:01	64	ARP	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicate use of 192.168.1.103 detected!)
15	AmbitMic_aa:af:80	Runtop_d9:0d:db	64	ARP	Who has 192.168.1.1? Tell 192.168.1.103
16	Runtop_d9:0d:db	AmbitMic_aa:af:80	64	ARP	192.168.1.1 is at 00:20:78:d9:0d:db
17	AmbitMic_aa:af:80	AmbitMic_12:9b:01	64	ARP	Who has 192.168.1.103? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)
18	AmbitMic_12:9b:01	AmbitMic_aa:af:80	64	ARP	192.168.1.103 is at 00:d0:59:12:9b:01 (duplicate use of 192.168.1.1 detected!)

Sample ARP Poison (After Color Rule)

No.	Source	Destination	Time	Protocol	Info
6	AmbitMic_aa:af:80	Runtop_d9:0d:db	1.134550000	ARP	192.168.1.103 is at 00:d0:59:aa:af:80
7	AmbitMic_aa:af:80	AmbitMic_12:9b:01	1.136550000	ARP	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicat
9	AmbitMic_aa:af:80	Runtop_d9:0d:db	3.137122000	ARP	Who has 192.168.1.1? Tell 192.168.1.103
10	Runtop_d9:0d:db	AmbitMic_aa:af:80	3.137851000	ARP	192.168.1.1 is at 00:20:78:d9:0d:db
11	AmbitMic_aa:af:80	AmbitMic_12:9b:01	3.138933000	ARP	Who has 192.168.1.103? Tell 192.168.1.1
12	AmbitMic_12:9b:01	AmbitMic_aa:af:80	3.139347000	ARP	192.168.1.103 is at 00:d0:59:12:9b:01 (dupl
13	AmbitMic_aa:af:80	Runtop_d9:0d:db	5.139359000	ARP	192.168.1.103 is at 00:d0:59:aa:af:80
14	AmbitMic_aa:af:80	AmbitMic_12:9b:01	5.141324000	ARP	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicat
15	AmbitMic_aa:af:80	Runtop_d9:0d:db	7.141748000	ARP	Who has 192.168.1.1? Tell 192.168.1.103
16	Runtop_d9:0d:db	AmbitMic_aa:af:80	7.142461000	ARP	192.168.1.1 is at 00:20:78:d9:0d:db
17	AmbitMic_aa:af:80	AmbitMic_12:9b:01	7.143711000	ARP	Who has 192.168.1.103? Tell 192.168.1.1
18	AmbitMic_12:9b:01	AmbitMic_aa:af:80	7.143913000	ARP	192.168.1.103 is at 00:d0:59:12:9b:01 (dupl
19	AmbitMic_aa:af:80	Runtop_d9:0d:db	9.144139000	ARP	192.168.1.103 is at 00:d0:59:aa:af:80
20	AmbitMic_aa:af:80	AmbitMic_12:9b:01	9.146104000	ARP	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicat

The device AmbitMic_aa:af:80 is attempting to trick the Runtop_d9:0d:db into thinking it is the client while making the client (AmbitMic_aa:af:01) think it is the Router

Forensic Reconstruction of the Crime...

Before Intrusion

No Encryption

No Encryption

After Intrusion

Dual-Radio Access Point

Results of the Investigation…

The results of the internal Forensic Investigation revealed several findings:

1. The original Wired Projector in the executive conference room had been replaced with an unauthorized WiFi model (that did not support any type of NAC or encryption)
2. Encryption was switched off on the presenters laptop to enable connecting to the WiFi projector
3. Rogue Access point was located outside conference room in a tree!

Network Forensics Case Study #4 -

A Fly on The Wall
-
Call Interception…

Security Issue - Bluebug

- Software exploit developed by a German researcher (Hefurt)
  - Exploit that allows the attacker to use the phone to initiate calls to premium rate numbers, send SMS messages, read SMS messages, connect to data services such as the Internet, and even eavesdrop on conversations in the vicinity
    - Done via a voice call over the GSM network
      - Allows the listening post to be anywhere in the world.
  - Bluetooth access is only required for a few seconds in order to set up the call
- Creates a serial profile connection to the device, giving full access to the AT command set, which is then exploited using standard off the shelf tools
  - PPP for networking or gnokii for messaging,

Security Issue – BlueSnarfing

- BlueSnarfing is the unauthorized accessing of features on Bluetooth-enabled devices
  - Phones
  - PDA's
  - WLAN network devices
- Typically employed in long-range attacks
  - Favorite industrial espionage attack

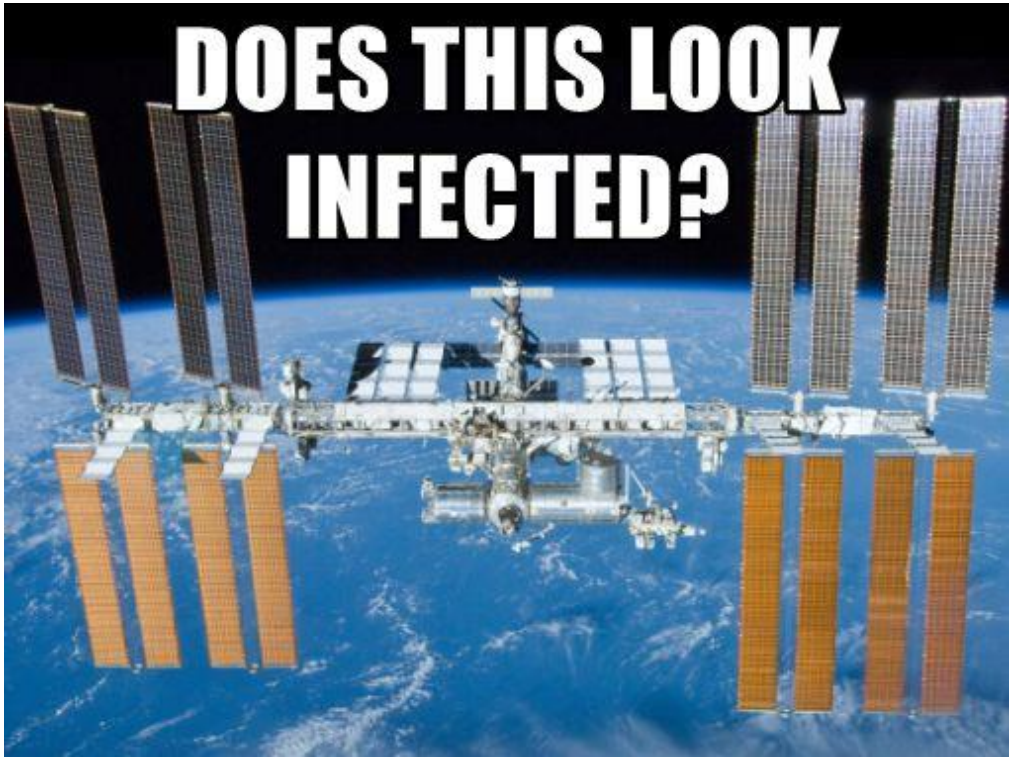
"…BlueSniper rifle, a Yagi-antenna and scope affixed to a gun-like stock that this week broke a distance record for BlueSnarfing… by slurping data from a Nokia 6310i from 1.1 away (2 Km) away…" Wired News Aug 2004

Sample Audio 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

A Final Example...



Questions and Answers / Discussion

Instructor Contact Information

Phill Shade: phill.shade@gmail.com

LinkedIn: Phill “Sherlock” Shade

Merlion’s Keep Consulting: merlions.keep@gmail.com

International: info@cybersecurityinstitute.eu

Merlion’s Keep Consulting & Training

Packets Never Lie


LOUNGE BAR
Thank You!