

SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



How Did That Happen?: Practical Techniques for Analyzing Suspicious Traffic

Phill “Sherlock” Shade
merlions.keep@gmail.com

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
- US Navy Retired and the founder of Merlion’s Keep Consulting, a professional services company specializing in network and forensics analysis
- Member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, and the IEEE and volunteer at Cyber Warfare Forum Initiative
- Numerous certifications, including Certified Network Expert (CNX)-Ethernet, CCNA, Certified Wireless Network Administrator (CWNA), and WildPackets Certified Network Forensics Analysis Expert (WNAX)



Welcome to the Internet – Now What?



Patterns are Bad....

No.	IP - Src	IP - Dest	Protocol	Size (B)	Src Port	Dest Port	Info
25	10.129.211.13	205.188.226.24	TCP	62	1050	80	1050→80 [SYN] Seq=3446458898 Win=64240 Len=0 MSS=1460 SACK_PERM=1
26	205.188.226.248	10.129.211.13	ICMP	70	1050	80	Destination unreachable (Port unreachable)
27	10.129.211.13	10.129.102.0	TCP	62	1051	139	1051→139 [SYN] Seq=2728705414 Win=64240 Len=0 MSS=1460 SACK_PERM=1
28	10.129.211.13	10.129.102.1	TCP	62	1052	139	1052→139 [SYN] Seq=590255581 Win=64240 Len=0 MSS=1460 SACK_PERM=1
29	10.129.211.13	10.129.102.2	TCP	62	1053	139	1053→139 [SYN] Seq=435193567 Win=64240 Len=0 MSS=1460 SACK_PERM=1
30	10.129.211.13	10.129.102.3	TCP	62	1054	139	1054→139 [SYN] Seq=3315488781 Win=64240 Len=0 MSS=1460 SACK_PERM=1
31	10.129.211.13	10.129.102.4	TCP	62	1055	139	1055→139 [SYN] Seq=976544386 Win=64240 Len=0 MSS=1460 SACK_PERM=1
32	10.129.211.13	10.129.102.5	TCP	62	1056	139	1056→139 [SYN] Seq=1526887667 Win=64240 Len=0 MSS=1460 SACK_PERM=1
33	10.129.211.13	10.129.102.6	TCP	62	1057	139	1057→139 [SYN] Seq=2725936831 Win=64240 Len=0 MSS=1460 SACK_PERM=1
34	10.129.211.13	10.129.102.7	TCP	62	1058	139	1058→139 [SYN] Seq=3547812389 Win=64240 Len=0 MSS=1460 SACK_PERM=1
35	10.129.211.13	10.129.102.8	TCP	62	1059	139	1059→139 [SYN] Seq=876694737 Win=64240 Len=0 MSS=1460 SACK_PERM=1
36	10.129.211.13	10.129.102.9	TCP	62	1060	139	1060→139 [SYN] Seq=1360512525 Win=64240 Len=0 MSS=1460 SACK_PERM=1

TCP Conversations											
Address A	Port A	Address B	Port B	Bytes A -> B	Bytes B -> A	Bytes A -> B	Bytes B -> A	Bytes A -> B	Bytes B -> A	Bytes A -> B	Bytes B -> A
10.129.211.13	1060	10.129.102.9	139	1	62	1	62	0	0	0	0
10.129.211.13	1061	10.129.102.10	139	1	62	1	62	0	0	0	0
10.129.211.13	1062	10.129.102.11	139	1	62	1	62	0	0	0	0
10.129.211.13	1063	10.129.102.12	139	1	62	1	62	0	0	0	0
10.129.211.13	1064	10.129.102.13	139	1	62	1	62	0	0	0	0
10.129.211.13	1065	10.129.102.14	139	1	62	1	62	0	0	0	0
10.129.211.13	1066	10.129.102.15	139	1	62	1	62	0	0	0	0
10.129.211.13	1067	10.129.102.16	139	1	62	1	62	0	0	0	0
10.129.211.13	1068	10.129.102.17	139	1	62	1	62	0	0	0	0
10.129.211.13	1069	10.129.102.18	139	1	62	1	62	0	0	0	0
10.129.211.13	1070	10.129.102.19	139	1	62	1	62	0	0	0	0
10.129.211.13	1071	10.129.102.20	139	1	62	1	62	0	0	0	0
10.129.211.13	1072	10.129.102.21	139	1	62	1	62	0	0	0	0
10.129.211.13	1073	10.129.102.22	139	1	62	1	62	0	0	0	0
10.129.211.13	1074	10.129.102.23	139	1	62	1	62	0	0	0	0
10.129.211.13	1075	10.129.102.24	139	1	62	1	62	0	0	0	0
10.129.211.13	1076	10.129.102.25	139	1	62	1	62	0	0	0	0
10.129.211.13	1077	10.129.102.26	139	1	62	1	62	0	0	0	0
10.129.211.13	1078	10.129.102.27	139	1	62	1	62	0	0	0	0
10.129.211.13	1079	10.129.102.28	139	1	62	1	62	0	0	0	0
10.129.211.13	1080	10.129.102.29	139	1	62	1	62	0	0	0	0

10.129.102.0	6	404	2	140	4	264
10.129.102.1	6	404	2	140	4	264
10.129.102.2	6	404	2	140	4	264
10.129.102.3	6	404	2	140	4	264
10.129.102.4	6	404	2	140	4	264
10.129.102.5	6	404	2	140	4	264
10.129.102.6	6	404	2	140	4	264
10.129.102.7	6	404	2	140	4	264
10.129.102.8	6	404	2	140	4	264
10.129.102.9	6	404	2	140	4	264
10.129.102.10	6	404	2	140	4	264
10.129.102.11	6	404	2	140	4	264

Statistics -> Endpoints

Statistics -> Conversations

Color Rules are Your Best Friend

The image shows the Wireshark network protocol analyzer interface. A dialog box titled "Wireshark: Coloring Rules - Profile: Default" is open, displaying a list of custom rules. The rules are color-coded and listed in order of processing. The main window shows a packet capture with the first packet highlighted in green, and a subsequent packet highlighted in red, demonstrating the effect of the color rules.

Name	String	Color
Sec - Suspect Downloads (.exe or .jar or MS System Files MZ) (custom)	frame matches	Red
Sec - Scanner - Xprobe2 (Custom)	icmp.code ==	Red
Sec - Low Orbit Ion Cannon (Custom)	frame matches	Red
Sec - Scanner - Retina / Ettercap (Custom)	ip.id==0xe77e	Red
Sec - Scanner - Nessus (Custom)	frame matches	Red
Sec - Scanner - Null Scan (LC)	tcp.flags == 0x	Red
Sec - ARP Bogus Requests (Man in The Middle) (Custom)	not RFC 4436 (arp.opcode ==	Green
ARP (custom)	arp	Green
Sec - Bad Domains (CN, RU,...) (Custom)	http.host match	Yellow
Sec - DNS - Suspicious Count (High # of Record Answers (Custom)	dns.count.ansv	Yellow
DNS Response - Failures (Custom)	dns.flags.rcode	Yellow
DNS Cache Responses (Custom)	dns.flags.rcode	Yellow

Advanced Filtering - Perl-Compatible Regular Expressions (PCRE)

PCRE's are essentially a special text string for describing a search pattern (shortcut) that make a range of advanced actions available within the syntax of a standard display filter

PERC	Definition
\	Preceding one of the above, will suppress their special meaning
^ / \$	Start of String \ End of String
.	Any Character
	Alteration (implied OR)
* / +	0 or more previous expressions / 1 or more previous expressions
(?i)	Case insensitive search
?	0 or 1 of previous expression; forces matching when expression might match several strings within a search string
{...} / [...]	Explicit quantifier notation / Explicit set of characters to match
(...)	Logical grouping of part of an expression

Detecting Suspicious File transfers

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]

Color Rule: frame matches "\.(?i)tar " or frame matches "MZ" or frame matches "\.(?i)exe"

Forensic Diagramming a Picture is worth 1024 Words...



1. Pick a single conversation (Filter)
2. Add the MAC addresses in that conversation to your picture
 - Draw arrows representing the flow of packets between interfaces
 - Try to identify which interfaces belong to stations and which ones belong to routers
 - Identify Access Points by the BSSID field in packets
3. Add the logical addresses that correspond to each MAC address
4. Evaluate the flow of data at both the logical and physical layers to see if it is appropriate

Forensic Diagramming Aid - IPv4 Time-to-Live

The Time To Live count is decremented each time a packet enters a router

When the count reaches zero, the router discards the packet and reports an ICMP Time To Live Exceeded message back to the originator

Many common Operating Systems have standard or default TTL's:

OS Version	TCP TTL	UDP TTL
FreeBSD 2.1R and later / HP Unix 10.01	64	64
Linux (all flavors)	64	64
MS Windows for WG / 95 / NT 3.51	32	32
MS Windows NT 4.0	128	128
MS Windows 98 / ME / XP / Vista / Windows 7 / 8	128	128
MS Windows 2000 (Client & Server)/ Server 2003 / 2008	255	255

Forensic Diagramming Aid - Vendor ID's

While the 3-Byte Vendor Identification values (OUI) are assigned by the IEEE, many vendors have standardized the use of specific names to correlate to specific product lines; some examples follow:

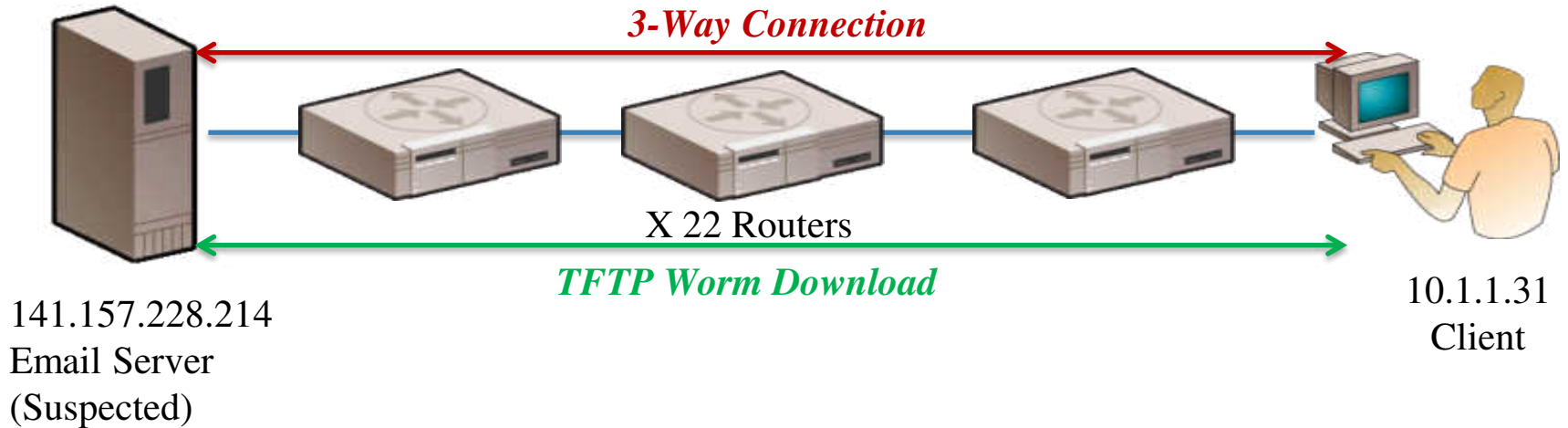
OUI	Product	OUI	Product
Cisco	Routers / Switches	Sony	Laptops
Aironet (Cisco)	Wireless Equipment	DellComp	Laptops / Desktops
Linksys	Wireless Equipment	Cadant	SoHo Routers
Hewlett Packard	Serves / Laptops	Colubris	Wireless Gateways
Compaq	Desktops	SymbolTe	Wireless Equipment

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=220592
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=220592
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=220592
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=2
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=2
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=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

What's hiding inside these seemingly harmless packets?

Forensic Diagramming



Analysis Aid – Name Tables

MK - Worm - Msblaster (Sucessful Attack2 - Edited).pcap [Phill's Magical Mystery Machine -]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save jpg Downloads

No.	IP - Src	IP - Dest	Time	DeltaTime	Protocol	Size (B)	Src Port	Dest Port	Info
1	141.157.228.12	10.1.1.31	0.000000	0.000000	TCP	62	1857	4444	1857 > 4444 [SYN]
2	10.1.1.31	141.157.228.12	0.000269	0.000269	TCP	62	4444	1857	4444 > 1857 [SYN, Seq=0, Win=0, Len=0]
3	141.157.228.12	10.1.1.31	0.082813	0.082813	TCP	60	1857	4444	1857 > 4444 [ACK, Seq=1857, Win=0, Len=0]
4	141.157.228.12	10.1.1.31	0.177883	0.095070	TCP	93	1857	4444	1857 > 4444 [PSH, Seq=1857, Win=0, Len=93]

Without Names

MK - Worm - Msblaster (Sucessful Attack2 - Edited).pcap [Phill's Magical Mystery Machine -]

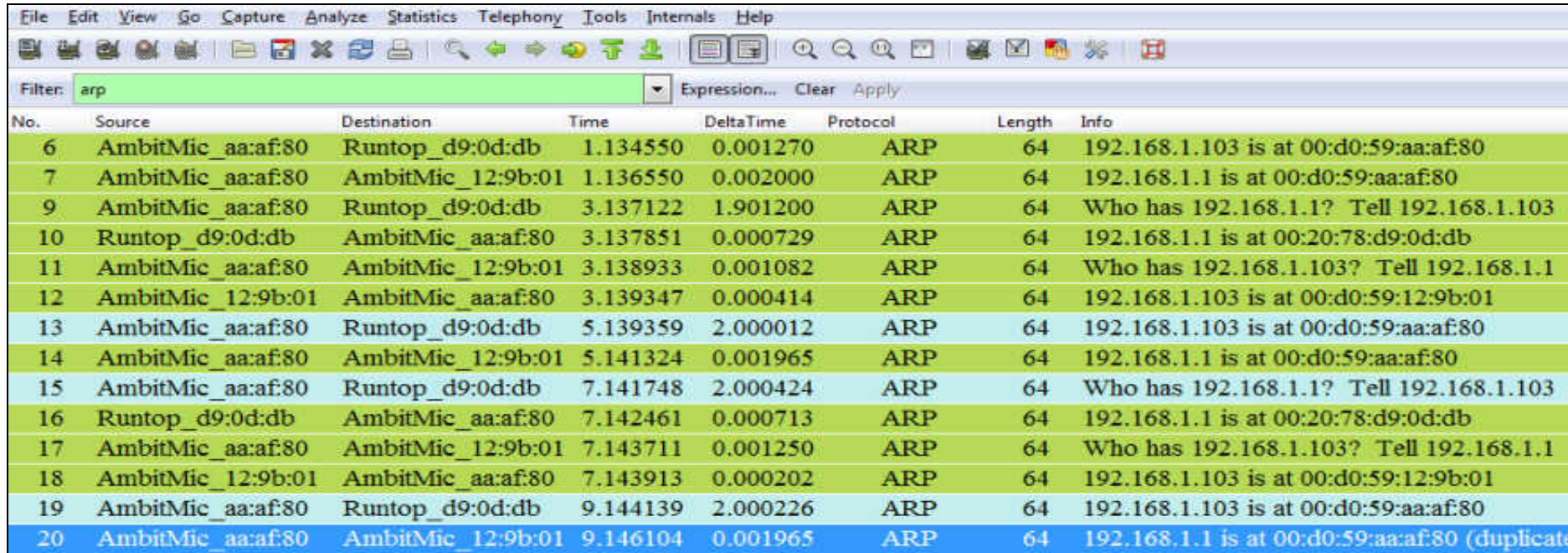
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save jpg Downloads

No.	Source	Destination	Time	Delta Time	Protocol	Length	Src Port	Dest Port	Info
1	Suspect	victim	0.000000	0.000000	TCP	62	1857	4444	
2	victim	suspect	0.000269	0.000269	TCP	62	4444	1857	
3	Suspect	victim	0.082813	0.082544	TCP	60	1857	4444	
4	Suspect	victim	0.177883	0.095070	TCP	93	1857	4444	
5	victim	Suspect	0.349041	0.171158	TCP	93	4444	1857	
6	victim	Suspect	0.349041	0.171158	TFTP	62	1028	69	
7	Suspect	victim	0.349041	0.171158	TCP	60	1857	4444	
8	victim	Suspect	0.349041	0.171158	TCP	158	4444	1857	
9	Suspect	victim	0.618459	0.061262	TFTP	558	69	1028	
10	victim	Suspect	0.617895	0.001436	TFTP	60	1028	69	
11	Suspect	victim	0.752105	0.134210	TCP	60	1857	4444	
12	12.243.154.137	victim	0.848049	0.095944	TCP	62	1818	135	
13	victim	12.243.154.137	0.848224	0.000175	TCP	60	135	1818	
14	12.243.154.137	victim	1.380230	0.532006	TCP	62	1818	135	
15	victim	12.243.154.137	1.380397	0.000167	TCP	60	135	1818	
16	Suspect	victim	1.519664	0.139267	TFTP	558	69	1028	
17	victim	Suspect	1.523540	0.003876	TFTP	60	1028	69	
18	12.243.154.137	victim	1.822370	0.298830	TCP	62	1818	135	
19	victim	12.243.154.137	1.822542	0.000172	TCP	60	135	1818	
20	Suspect	victim	2.425865	0.603323	TFTP	558	69	1028	

Using Custom Host File

Normal Behavior ?



The image shows a Wireshark network traffic capture window. The filter is set to 'arp'. The table below displays the captured ARP traffic, including source and destination MAC addresses, timestamps, and protocol details.

No.	Source	Destination	Time	DeltaTime	Protocol	Length	Info
6	AmbitMic_aa:af:80	Runtop_d9:0d:db	1.134550	0.001270	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
7	AmbitMic_aa:af:80	AmbitMic_12:9b:01	1.136550	0.002000	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80
9	AmbitMic_aa:af:80	Runtop_d9:0d:db	3.137122	1.901200	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
10	Runtop_d9:0d:db	AmbitMic_aa:af:80	3.137851	0.000729	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
11	AmbitMic_aa:af:80	AmbitMic_12:9b:01	3.138933	0.001082	ARP	64	Who has 192.168.1.103? Tell 192.168.1.1
12	AmbitMic_12:9b:01	AmbitMic_aa:af:80	3.139347	0.000414	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01
13	AmbitMic_aa:af:80	Runtop_d9:0d:db	5.139359	2.000012	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
14	AmbitMic_aa:af:80	AmbitMic_12:9b:01	5.141324	0.001965	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80
15	AmbitMic_aa:af:80	Runtop_d9:0d:db	7.141748	2.000424	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
16	Runtop_d9:0d:db	AmbitMic_aa:af:80	7.142461	0.000713	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
17	AmbitMic_aa:af:80	AmbitMic_12:9b:01	7.143711	0.001250	ARP	64	Who has 192.168.1.103? Tell 192.168.1.1
18	AmbitMic_12:9b:01	AmbitMic_aa:af:80	7.143913	0.000202	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01
19	AmbitMic_aa:af:80	Runtop_d9:0d:db	9.144139	2.000226	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
20	AmbitMic_aa:af:80	AmbitMic_12:9b:01	9.146104	0.001965	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicate)

Detecting Man-in-the-Middle Attacks

No.	Source	Destination	Time	Protocol	Size (B)	Info
7	AmbitMic_aa:af:80	AmbitMic_12:9b:01	1.136550000	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicate use of 192.168.1.103 detected!)
8	AmbitMic_aa:af:80	AmbitMic_12:9b:01	1.235922000	ICMP	64	Echo (ping) reply id=0xe77e, seq=256/1, ttl=150 (request in 5)
9	AmbitMic_aa:af:80	Runtop_d9:0d:db	3.137122000	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
10	Runtop_d9:0d:db	AmbitMic_aa:af:80	3.137851000	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
11	AmbitMic_aa:af:80	AmbitMic_12:9b:01	3.138933000	ARP	64	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	3.139347000	ARP	64	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	5.139359000	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
14	AmbitMic_aa:af:80	AmbitMic_12:9b:01	5.141324000	ARP	64	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	7.141748000	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
16	Runtop_d9:0d:db	AmbitMic_aa:af:80	7.142461000	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
17	AmbitMic_aa:af:80	AmbitMic_12:9b:01	7.143711000	ARP	64	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	7.143913000	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01 (duplicate use of 192.168.1.1 detected!)
19	AmbitMic_aa:af:80	Runtop_d9:0d:db	9.144139000	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80

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

Color Rule: (arp.opcode == 1) && !(eth.dst == ff:ff:ff:ff:ff:ff)

Identifying Reconnaissance Scanning

No. -	Source	Destination	Protocol	Info
2466	12.0.21.21	12.0.20.190	ICMP	Echo (ping) request
2467	12.0.20.190	12.0.21.21	ICMP	Echo (ping) reply
2468	12.0.21.21	12.0.20.190	ICMP	Address mask request
2469	12.0.21.21	12.0.20.190	ICMP	Timestamp request
2470	12.0.20.190	12.0.21.21	ICMP	Timestamp reply
2471	12.0.21.21	12.0.20.190	ICMP	Information request
2472	12.0.21.21	12.0.20.190	ICMP	Echo (ping) request
2473	12.0.20.190	12.0.21.21	ICMP	Echo (ping) reply
2474	12.0.21.21	12.0.20.190	UDP	Source port: 1222 Destination port: 0
2475	12.0.20.190	12.0.21.21	ICMP	Destination unreachable (Port unreachable)
2476	12.0.21.21	12.0.20.191	ICMP	Echo (ping) request
2477	12.0.20.191	12.0.21.21	ICMP	Echo (ping) reply
2478	12.0.21.21	12.0.20.191	ICMP	Address mask request
2479	12.0.21.21	12.0.20.191	ICMP	Timestamp request
2480	12.0.20.191	12.0.21.21	ICMP	Timestamp reply
2481	12.0.21.21	12.0.20.191	ICMP	Information request
2482	12.0.21.21	12.0.20.191	ICMP	Echo (ping) request
2483	12.0.20.191	12.0.21.21	ICMP	Echo (ping) reply
2484	12.0.21.21	12.0.20.191	UDP	Source port: 1222 Destination port: 0
2485	12.0.20.191	12.0.21.21	ICMP	Destination unreachable (Port unreachable)
2486	12.0.21.21	12.0.20.192	ICMP	Echo (ping) request
2487	12.0.20.192	12.0.21.21	ICMP	Echo (ping) reply
2488	12.0.21.21	12.0.20.192	ICMP	Address mask request
2489	12.0.21.21	12.0.20.192	ICMP	Timestamp request
2490	12.0.20.192	12.0.21.21	ICMP	Timestamp reply

Color Rule: icmp.type >12 && icmp.type <19

Sample Color Rules for Suspicious Activity

Suspicious File transfers

frame matches "\.(?i)tar " or frame matches "MZ" or frame matches "\.(?i)exe"

Man-in-the-Middle

(arp.opcode == 1) && !(eth.dst == ff:ff:ff:ff:ff:ff)

Reconnaissance or OS Fingerprinting Scan

icmp.type >12 && icmp.type <19

When All Else Fails...





Thank You !

Contact Information

Phill Shade: phill.shade@gmail.com

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

International: info@cybersecurityinstitute.eu



Merlion's Keep Consulting & Training

Packets Never Lie