Covert Channel – Needle in the Haystack

Write up by:

John Antone

835 COS

854 CPT

Covert Channel -
Needle In The Haystack

80

We captured a ton of traffic, can you sift through it to find anything interesting? Some people might think they are secure because they are hidden in the masses, the needle in the haystack.

To start off with on this Pcap we look at the Protocol Hierarchy page:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	26365	100.0	27140104	4112 k	0	0	0
Ethernet	100.0	26365	1.4	369110	55 k	0	0	0
Internet Protocol Version 6	0.1	25	0.0	1000	151	2	80	12
User Datagram Protocol	0.0	7	0.0	56	8	0	0	0
Link-local Multicast Name Resolution	0.0	5	0.0	163	24	5	163	24
DHCPv6	0.0	2	0.0	190	28	2	190	28
Internet Control Message Protocol v6	0.1	16	0.0	424	64	16	424	64
Internet Protocol Version 4	99.7	26283	1.9	525692	79 k	0	0	0
User Datagram Protocol	1.5	404	0.0	3232	489	0	0	0
Teredo IPv6 over UDP tunneling	0.0	8	0.0	606	91	0	0	0
Network Time Protocol	0.1	28	0.0	1344	203	28	1344	203
NetBIOS Name Service	0.0	3	0.0	204	30	3	204	30
Link-local Multicast Name Resolution	0.0	5	0.0	163	24	5	163	24
Domain Name System	0.1	22	0.0	1615	244	22	1615	244
Data	1.3	338	0.1	28110	4259	338	28110	4259
Transmission Control Protocol	98.1	25871	96.6	26204264	3970 k	23726	23400708	3545 k
Transport Layer Security	0.0	1	0.0	68	10	1	68	10
Telnet	0.3	77	0.0	334	50	77	334	50
SSH Protocol	0.0	8	0.0	4541	688	8	4541	688
Malformed Packet	0.1	24	0.0	0	0	24	0	0
DRDA	1.6	434	23.5	6368243	964 k	428	6239355	945 k
Data	0.1	19	0.0	5158	781	19	5158	781
BitTorrent	7.3	1915	16.4	4443937	673 k	1588	4370832	662 k
Internet Group Management Protocol	0.0	8	0.0	128	19	8	128	19
Address Resolution Protocol	0.2	65	0.0	2882	436	65	2882	436

We can see that we have the following Protocols to look into:

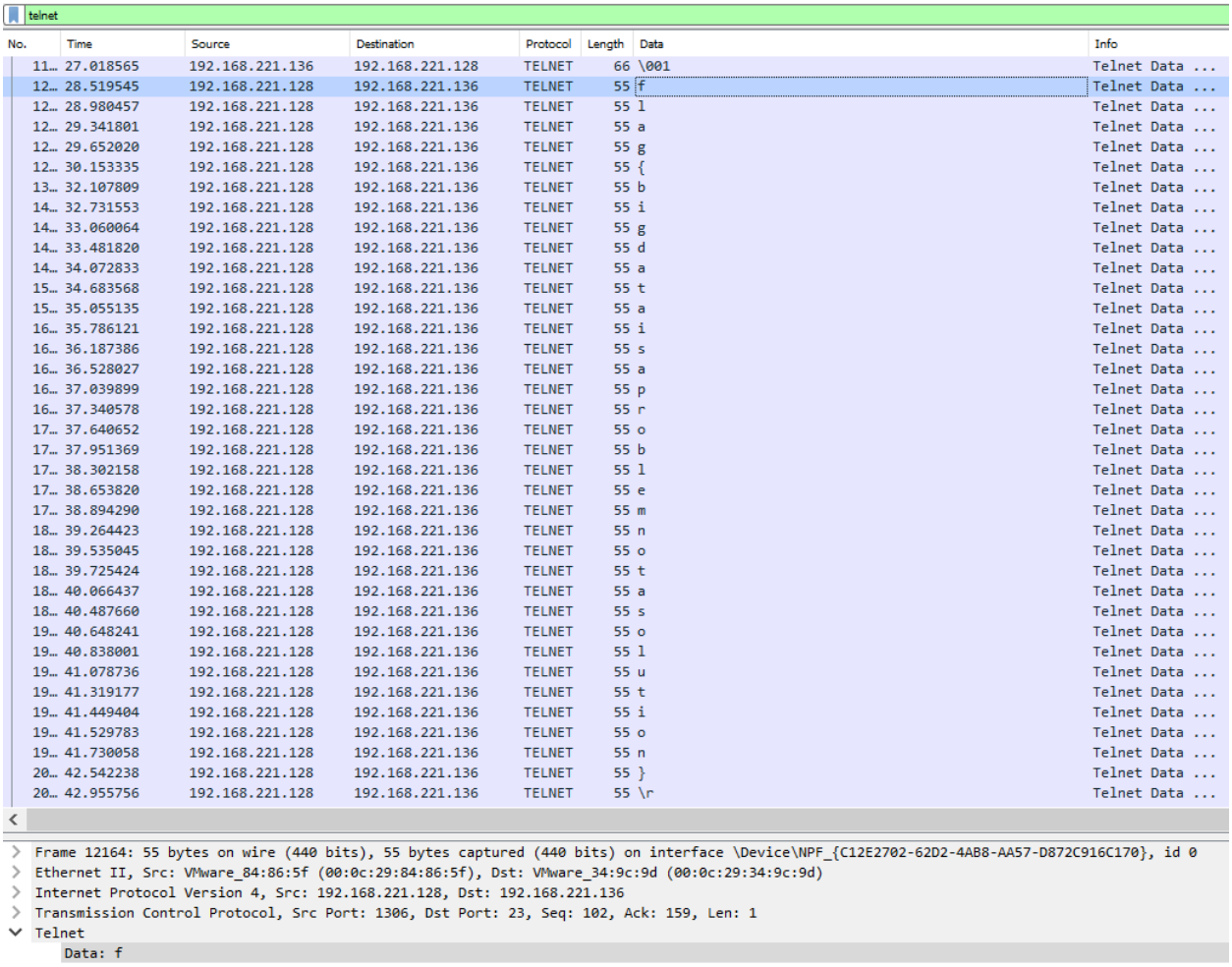
- UDP: NTP, NBNS, LLMNR, DNS, Data
- TCP: TLS, Telnet, SSH, DRDA, Data, BitTorrent, Malformed Packet

We might want to look at the Malformed Packet as we are looking for a needle in the haystack, but that leads us to a dead end.

_ws.malformed

No.	Time	Source	Destination	Protocol	Length	Host	Info
10…	26.618296	173.14.243.233	192.168.221.128	DRDA	1434		[Malformed Packet]
13…	32.286822	173.14.243.233	192.168.221.128	DRDA	1514		[Malformed Packet]
23…	48.400765	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]
23…	48.898397	74.95.93.93	192.168.221.128	BitTo…	1514		Piece[Malformed Packet]
23…	48.901764	74.95.93.93	192.168.221.128	BitTo…	1434		Piece[Malformed Packet]
23…	48.903706	74.95.93.93	192.168.221.128	BitTo…	1274		Piece[Malformed Packet]
23…	49.937686	74.95.93.93	192.168.221.128	BitTo…	1514		Piece[Malformed Packet]
24…	50.355080	74.95.93.93	192.168.221.128	BitTo…	1354		Piece[Malformed Packet]
24…	50.379941	74.95.93.93	192.168.221.128	BitTo…	1514		Piece[Malformed Packet]
24…	50.408300	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]
24…	50.483165	74.95.93.93	192.168.221.128	BitTo…	1434		Bitfield[Malformed Packet]
24…	50.538822	74.95.93.93	192.168.221.128	BitTo…	1354		Piece[Malformed Packet]
24…	50.539101	74.95.93.93	192.168.221.128	BitTo…	1434		Bitfield[Malformed Packet]
24…	50.633151	74.95.93.93	192.168.221.128	BitTo…	1434		Bitfield[Malformed Packet]
24…	50.637786	74.95.93.93	192.168.221.128	BitTo…	1354		Extended[Malformed Packet]
24…	50.694917	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]
24…	50.894788	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]
24…	50.994759	74.95.93.93	192.168.221.128	BitTo…	1514		Extended[Malformed Packet]
24…	51.041849	74.95.93.93	192.168.221.128	BitTo…	1434		Bitfield[Malformed Packet]
24…	51.063656	74.95.93.93	192.168.221.128	BitTo…	1434		Piece[Malformed Packet]
25…	51.143412	74.95.93.93	192.168.221.128	BitTo…	1274		Bitfield[Malformed Packet]
25…	51.306264	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]
25…	51.832520	74.95.93.93	192.168.221.128	BitTo…	1514		Bitfield[Malformed Packet]

Next thing to look at would be Telnet as this is easy to view because there is no encryption. We examine the Data field under Telnet to see what is being sent and we see all the characters being typed across the wire.



telnet

No.	Time	Source	Destination	Protocol	Length	Data	Info
11…	27.018565	192.168.221.136	192.168.221.128	TELNET	66	\001	Telnet Data ...
12…	28.519545	192.168.221.128	192.168.221.136	TELNET	55	f	Telnet Data ...
12…	28.980457	192.168.221.128	192.168.221.136	TELNET	55	l	Telnet Data ...
12…	29.341801	192.168.221.128	192.168.221.136	TELNET	55	a	Telnet Data ...
12…	29.652020	192.168.221.128	192.168.221.136	TELNET	55	g	Telnet Data ...
12…	30.153335	192.168.221.128	192.168.221.136	TELNET	55	{	Telnet Data ...
13…	32.107809	192.168.221.128	192.168.221.136	TELNET	55	b	Telnet Data ...
14…	32.731553	192.168.221.128	192.168.221.136	TELNET	55	i	Telnet Data ...
14…	33.060064	192.168.221.128	192.168.221.136	TELNET	55	g	Telnet Data ...
14…	33.481820	192.168.221.128	192.168.221.136	TELNET	55	d	Telnet Data ...
14…	34.072833	192.168.221.128	192.168.221.136	TELNET	55	a	Telnet Data ...
15…	34.683568	192.168.221.128	192.168.221.136	TELNET	55	t	Telnet Data ...
15…	35.055135	192.168.221.128	192.168.221.136	TELNET	55	a	Telnet Data ...
16…	35.786121	192.168.221.128	192.168.221.136	TELNET	55	i	Telnet Data ...
16…	36.187386	192.168.221.128	192.168.221.136	TELNET	55	s	Telnet Data ...
16…	36.528027	192.168.221.128	192.168.221.136	TELNET	55	a	Telnet Data ...
16…	37.039899	192.168.221.128	192.168.221.136	TELNET	55	p	Telnet Data ...
16…	37.340578	192.168.221.128	192.168.221.136	TELNET	55	r	Telnet Data ...
17…	37.640652	192.168.221.128	192.168.221.136	TELNET	55	o	Telnet Data ...
17…	37.951369	192.168.221.128	192.168.221.136	TELNET	55	b	Telnet Data ...
17…	38.302158	192.168.221.128	192.168.221.136	TELNET	55	l	Telnet Data ...
17…	38.653820	192.168.221.128	192.168.221.136	TELNET	55	e	Telnet Data ...
17…	38.894290	192.168.221.128	192.168.221.136	TELNET	55	m	Telnet Data ...
18…	39.264423	192.168.221.128	192.168.221.136	TELNET	55	n	Telnet Data ...
18…	39.535045	192.168.221.128	192.168.221.136	TELNET	55	o	Telnet Data ...
18…	39.725424	192.168.221.128	192.168.221.136	TELNET	55	t	Telnet Data ...
18…	40.066437	192.168.221.128	192.168.221.136	TELNET	55	a	Telnet Data ...
18…	40.487660	192.168.221.128	192.168.221.136	TELNET	55	s	Telnet Data ...
19…	40.648241	192.168.221.128	192.168.221.136	TELNET	55	o	Telnet Data ...
19…	40.838001	192.168.221.128	192.168.221.136	TELNET	55	l	Telnet Data ...
19…	41.078736	192.168.221.128	192.168.221.136	TELNET	55	u	Telnet Data ...
19…	41.319177	192.168.221.128	192.168.221.136	TELNET	55	t	Telnet Data ...
19…	41.449404	192.168.221.128	192.168.221.136	TELNET	55	i	Telnet Data ...
19…	41.529783	192.168.221.128	192.168.221.136	TELNET	55	o	Telnet Data ...
19…	41.730058	192.168.221.128	192.168.221.136	TELNET	55	n	Telnet Data ...
20…	42.542238	192.168.221.128	192.168.221.136	TELNET	55	}	Telnet Data ...
20…	42.955756	192.168.221.128	192.168.221.136	TELNET	55	\r	Telnet Data ...

```
> Frame 12164: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{C12E2702-62D2-4AB8-AA57-D872C916C170}, id 0
> Ethernet II, Src: VMware_84:86:5f (00:0c:29:84:86:5f), Dst: VMware_34:9c:9d (00:0c:29:34:9c:9d)
> Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.136
> Transmission Control Protocol, Src Port: 1306, Dst Port: 23, Seq: 102, Ack: 159, Len: 1
v Telnet
    Data: f
```

Answer: flag{bigdataisaproblemnotasolution}