

**Instituto Tecnológico de Cancún**

**Fundamentos de Telecomunicaciones**

**Lab41 - Export Malicious  
Redirection Packet Comments**

**Prof. Ismael Jiménez Sánchez**

**Alumno(a). Laury del Rosario Mex  
Martin**

**Ciclo 2020-B**

Anexaremos una columna nueva que será packets comments para visualizar las conversaciones que pueden ser malintencionados.

sec-suspicious101.pcapng

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización: <Ctrl+>

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info	Comment	Coloring Rule Name
1	0.000000	0.000000000	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...	This is the origi...	HTTP
23	0.146588	0.146588000	66.11.147.48	24.6.173.220	HTTP		HTTP/1.1 200 OK [Unresembled Packet]	This TCP connecti...	HTTP
87	0.011399	0.011399000	95.169.190.2...	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)	They're dropping ...	HTTP
84	0.000015	0.000015000	24.6.173.220	95.169.190.217	HTTP		Continuation	Please oh please ...	HTTP
75	0.002074	0.002074000	95.169.190.2...	24.6.173.220	HTTP		HTTP/1.1 302 Found	Our malicious hos...	HTTP
7	0.474442	0.000000000	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /imgres?imgur1=http://www.artbrokerage.com/artt...	Now we clicked on...	HTTP
21	0.000709	0.000709000	24.6.173.220	77.93.251.49	HTTP	www.ulisse-	GET /stat/gthyu/index.php?p=peter-lik-inner-peace-f...	Now we are making...	HTTP
5	0.000003	0.000003000	74.125.224.84	24.6.173.220	HTTP		Continuation	In this response...	HTTP
67	0.048584	0.547913000	77.93.251.49	24.6.173.220	HTTP		HTTP/1.1 302 Found	Here's the redire...	HTTP
15	0.002104	0.000000000	24.6.173.220	66.11.147.48	TCP		50317 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4...	Here we begin con...	HTTP
79	0.002733	0.000000000	24.6.173.220	95.169.190.217	TCP		50320 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4...	And here we go....	HTTP
104	0.001678	0.001678000	24.6.173.220	78.41.203.19	TCP		50324 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	And another termi...	TCP RST
172	0.199772	0.199772000	24.6.173.220	74.125.224.84	TCP		50220 > 80 [ACK] Seq=3289 Ack=7473 Win=16349 Len=0		HTTP
171	0.038057	0.038057000	74.125.224.84	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/javascript)		HTTP
170	0.743225	0.961508000	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /image?ei=ejsdTslwPH40msQ0fo9u6DA&page=5&star...		HTTP
169	0.198540	0.198540000	24.6.173.220	74.125.224.84	TCP		50263 > 80 [ACK] Seq=2737 Ack=3477 Win=16307 Len=0		HTTP
168	0.019743	0.036977000	74.125.224.84	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/javascript)		HTTP
167	0.000562	0.000562000	24.6.173.220	74.125.224.84	TCP		50220 > 80 [ACK] Seq=2447 Ack=7091 Win=16445 Len=0		HTTP
166	0.000003	0.000003000	74.125.224.84	24.6.173.220	HTTP		Continuation		HTTP
165	0.001192	0.001192000	74.125.224.84	24.6.173.220	HTTP		Continuation		HTTP
164	0.015477	0.053611000	74.125.224.84	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/javascript)		HTTP
163	0.038134	0.188427000	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /image?ei=ejsdTslwPH40msQ0fo9u6DA&page=6&star...		HTTP
162	0.150293	15.380818000	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...		HTTP
161	0.020323	0.020323000	74.125.224.84	24.6.173.220	HTTP		HTTP/1.1 204 No Content		HTTP
160	0.015491	0.015491000	74.125.224.84	24.6.173.220	TCP		80 > 50263 [ACK] Seq=2926 Ack=1886 Win=350 Len=0		HTTP
158	0.188038	0.188038000	95.169.190.2...	24.6.173.220	TCP		80 > 50353 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS...		HTTP
157	0.121210	0.000000000	24.6.173.220	95.169.190.217	TCP		50353 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4...		HTTP
156	0.598362	4.199916000	78.41.203.19	24.6.173.220	TCP		[TCP Retransmission] 80 > 50325 [SYN, ACK] Seq=0 Ac...		T-Retransmissions

Packet comments

- > This is the original search query for the "Peter Lik for sale" images.
- > Frame 1: 1097 bytes on wire (8776 bits), 1097 bytes captured (8776 bits) on interface unknown, id 0
- > Ethernet II, Src: HewlettP\_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)
- > Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.84
- > Transmission Control Protocol, Src Port: 50263, Dst Port: 80, Seq: 1, Ack: 1, Len: 1043
- > Hypertext Transfer Protocol

Paquetes: 172 · Mostrado: 172 (100.0%) · Comentarios: 19 · Perfil: wireshark 101

Y vamos a exportar el archivo como un cvs para que también ahí se vea aplicado la columna que anexamos.

sec-suspicious101 - Excel

Laury del Rosario Mex Martin

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Ayuda ¿Qué desea hacer?

Calibri 11 Fuente Alineación Número General

Formato Dar formato Estilos de condicional como tabla Estilos

Insertar Eliminar Formato Celdas

Ordenar y filtrar Buscar y filtrar Edición

Confidencialidad

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info	Comment	Coloring Rule Name
1	0	0	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...	This is the original search query for the "Peter Lik for sale" images.	HTTP
5	0.000003	0.000003	74.125.224.84	24.6.173.220	HTTP		Continuation	In this response, the server sends numerous thumbnail images along w	HTTP
7	0.474442	0	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /imgres	Now we clicked on the image load the expanded thumbnail from Google	HTTP
12	0.000014	0.000014	74.125.224.84	24.6.173.220	HTTP		Continuation	We get the expanded image through Google - there are a lot of web dis	HTTP
14	0.024191	0	24.6.173.220	77.93.251.49	TCP		50316 > 80	We clicked on the web link associated with the expanded image. This is	HTTP
15	0.002104	0	24.6.173.220	66.11.147.48	TCP		50317 > 80	Here we begin connecting to www.artbrokerage.com at 66.11.147.48. Th	HTTP
18	0.000565	0.000565	24.6.173.220	66.11.147.48	HTTP	www.artbro-	GET /artthru	We request an 850x600 size of a Peter Lik photo.	HTTP
21	0.000709	0.000709	24.6.173.220	77.93.251.49	HTTP	www.ulisse-	GET /stat/gt	Now we are making a request to www.ulisseide.org.	HTTP
23	0.146588	0.146588	66.11.147.48	24.6.173.220	HTTP		HTTP/1.1 200	This TCP connection is used to get the image file from artbrokerage.com	HTTP
67	0.048584	0.547913	77.93.251.49	24.6.173.220	HTTP		HTTP/1.1 302	Here's the redirection to the malicious site. See the Location line. We a	HTTP
68	0.00217	0	24.6.173.220	95.169.190.2...	TCP		50319 > 80	We removed the DNS queries from the trace file - we must have looked	HTTP
75	0.002074	0.002074	95.169.190.2...	24.6.173.220	HTTP		HTTP/1.1 302	Our malicious host is redirecting us to run a CGI script (in.cgi). We'll hav	HTTP
79	0.002733	0	24.6.173.220	95.169.190.2...	TCP		50320 > 80	And here we go... this is the ugly connection.	HTTP
84	0.000015	0.000015	24.6.173.220	95.169.190.2...	HTTP		Continuation	Please oh please hit us over the head with a baseball bat! We ask for th	HTTP
87	0.011399	0.011399	95.169.190.2...	24.6.173.220	HTTP		HTTP/1.1 200	They're dropping a cookie on our drive and giving us a link to a .info site	HTTP
96	0.002946	0.002946	24.6.173.220	78.41.203.19	TCP		50321 > 80	Well that didn't go so well for them... our Symantec software terminat	TCP RST
104	0.001678	0.001678	24.6.173.220	78.41.203.19	TCP		50324 > 80	And another termination triggered by Symantec.	TCP RST
117	0.001682	0.001682	24.6.173.220	78.41.203.19	TCP		50326 > 80	Yes, Symantec is screaming with messages on our system...	TCP RST
159	0.327815	15.712621	24.6.173.220	74.125.224.84	HTTP	www.google-	GET /gen_20	We're just returning to Google after a little sidetrack to the dark side...	HTTP

sec-suspicious101

Recuento: 20