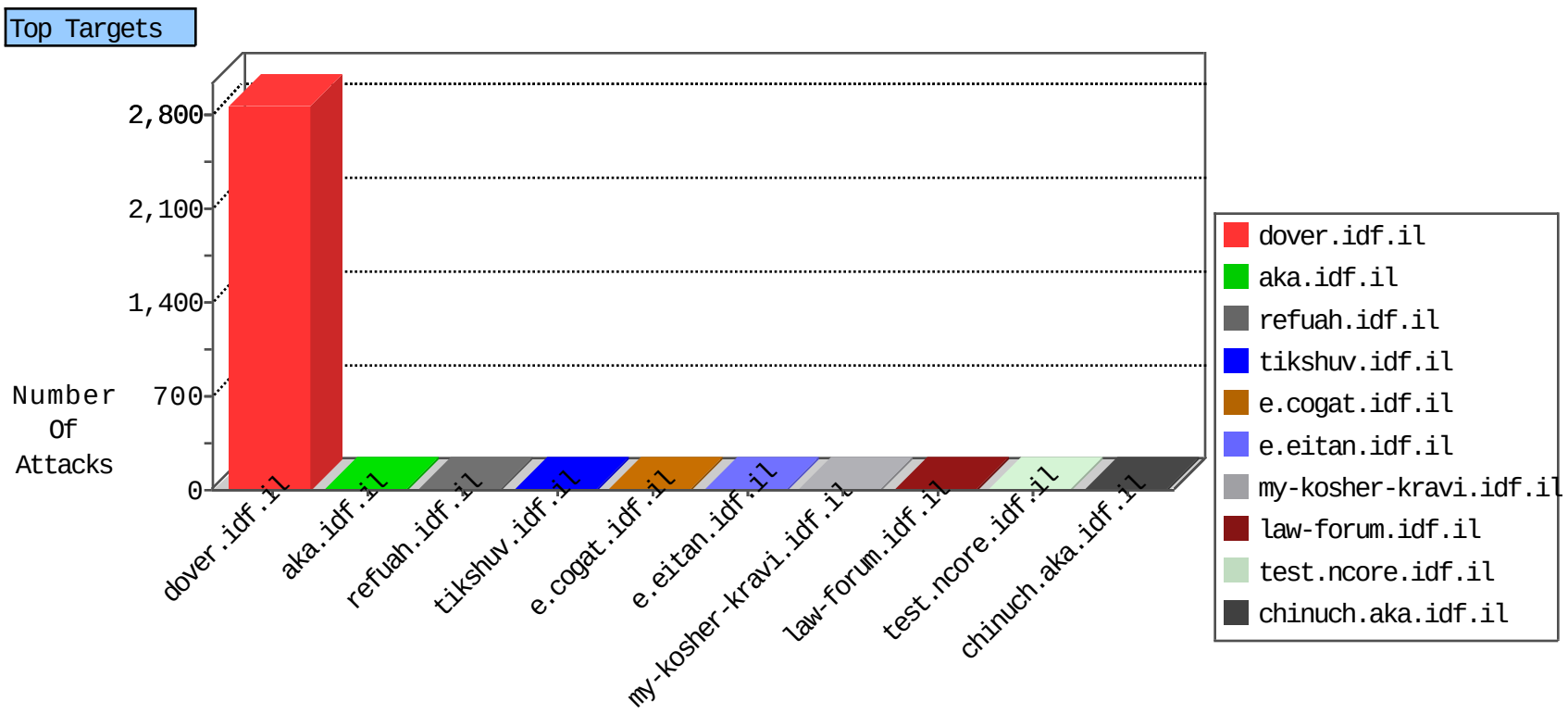
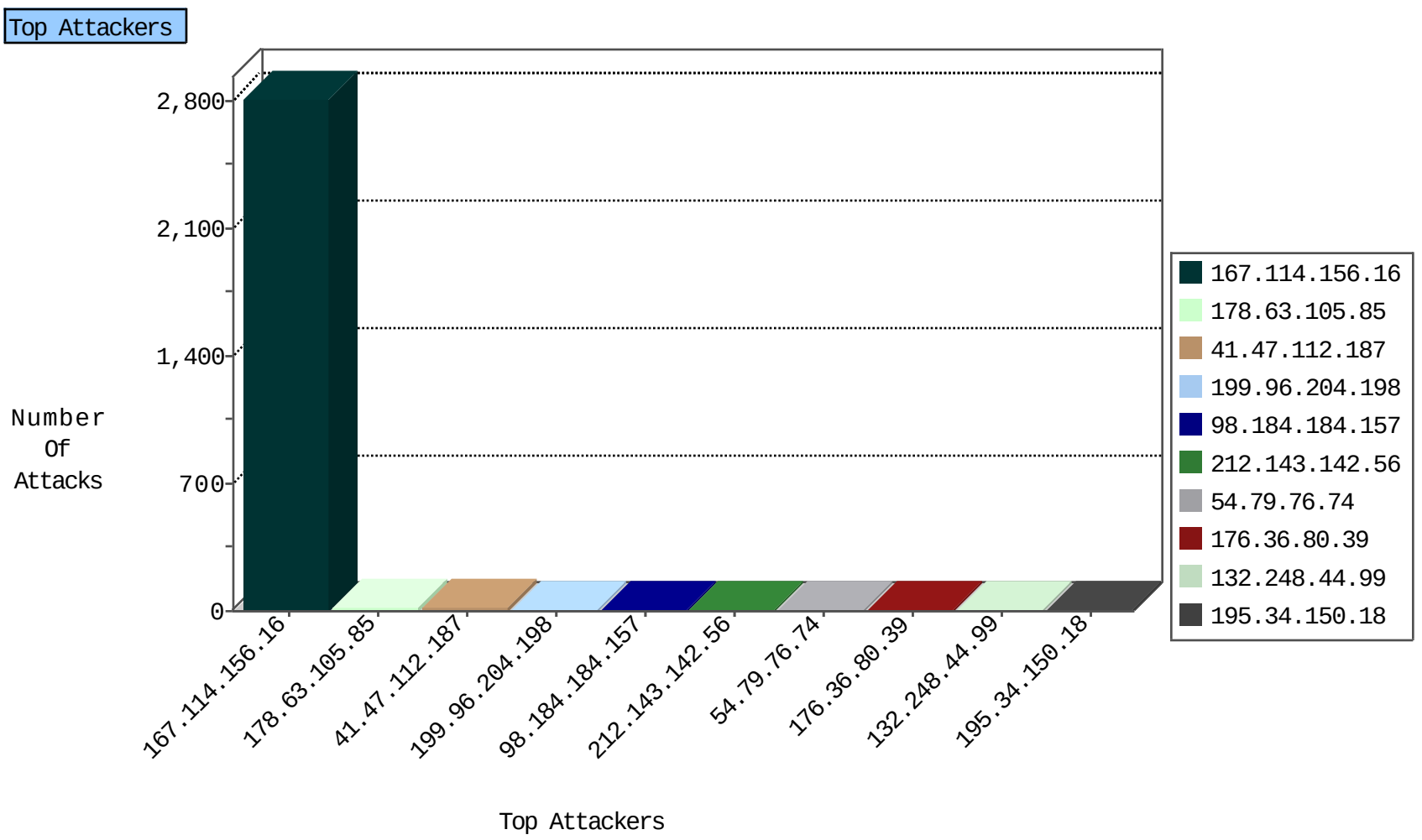
03-14-2016-02:04:03 to 03-14-2016-03:04:03

IDF Under Attack Daily Report





03-14-2016-02:04:03 to 03-14-2016-03:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3881
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	2

03-14-2016-02:04:03 to 03-14-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.36.80.39	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
176.36.80.39	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	3
199.30.24.233	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.53	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.90	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.141	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-14-2016-02:04:03 to 03-14-2016-03:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
199.98.17.225	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
77.44.73.85	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
208.71.68.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
208.71.68.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
199.98.17.225	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.98.87.187	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
208.71.68.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1

03-14-2016-02:04:03 to 03-14-2016-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.47.112.187	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
199.96.204.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	3
77.66.60.75	Denmark	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.140.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
141.212.122.78	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.154.130	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.210.70	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.68	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.110.35.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.154.243.14	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.47.112.187	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.79	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
65.55.210.70	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
141.212.122.69	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.110.35.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
197.134.178.45	Egypt	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
141.212.122.160	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
132.248.44.99	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.77	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.229.32.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
41.47.112.187	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.175	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.96	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.124	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
84.229.32.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
159.226.95.66	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
132.248.44.99	Mexico	147.237.0.33	idf.il	drop		drop	1
220.255.145.53	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

<table>
<tr><th>Attacker Address</th><th>Attacker Country</th><th>Target Address</th><th>Site</th><th>Signature</th><th>Device Action</th><th>Count</th></tr>
<tr><td>54.79.76.74</td><td>Australia</td><td>147.237.72.166</td><td>aka.idf.il</td><td>Multiple Unauthorized URL Access from 54.79.76.74</td><td>Block</td><td>5</td></tr>
<tr><td>220.255.145.53</td><td>Singapore</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>2</td></tr>
<tr><td>212.179.21.194</td><td>Israel</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>2</td></tr>
<tr><td>220.255.103.232</td><td>Singapore</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>2</td></tr>
<tr><td>203.127.96.198</td><td>Singapore</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Malformed URL t…₪´¿„ˆnz3„g:ש6°,ÿסצ¸ ¸oף=]]62#[[€¡e¨™•f|ט<„[[61#]]מ ¶[[#25]]lÊ[[#17]]¸€ü</td><td>Block</td><td>1</td></tr>
<tr><td>66.249.64.190</td><td>Israel</td><td>147.237.72.166</td><td>aka.idf.il</td><td>Multiple Unauthorized URL Access from 66.249.64.190</td><td>Block</td><td>1</td></tr>
<tr><td>179.7.213.26</td><td>Peru</td><td>147.237.77.216</td><td>dover.idf.il</td><td>PHP Attempt</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀ œ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ</td><td>Block</td><td>1</td></tr>
<tr><td>46.19.85.62</td><td>Israel</td><td>147.237.77.233</td><td>atal.idf.il</td><td>Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>NULL Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀ œ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ</td><td>Block</td><td>1</td></tr>
<tr><td>69.197.169.202</td><td>United States</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Unauthorized URL Access to www.idf.il/894-he/shared/usercontrols/headerupper/</td><td>Block</td><td>1</td></tr>
<tr><td>179.7.213.26</td><td>Peru</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Unauthorized URL Access to www.idf.il/xmlrpc.php</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Illegal Byte Code Character in Parameter Name ₪[[†׳#18[[]]#15ˆ„¿´₪…t ni]] nz3„g:ש6°,ÿסצ¸ ¸oף=]]62#[[€¡e¨™•f|ט<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü</td><td>Block</td><td>1</td></tr>
<tr><td>213.143.50.51</td><td>Spain</td><td>147.237.72.166</td><td>aka.idf.il</td><td>Untraceable SSL Sessions: Open Mode</td><td>None</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀ œ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ</td><td>Block</td><td>1</td></tr>
<tr><td>82.80.63.208</td><td>Israel</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Multiple Unauthorized URL Access from 82.80.63.208</td><td>Block</td><td>1</td></tr>
<tr><td>195.154.207.160</td><td>France</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Unauthorized URL Access to www.idf.il/templates/homepage/shared/usercontrols/headerupper/</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Illegal Byte Code Character in Query String ₪[[†׳#18[[]]#15„3znˆ„¿´₪…t no]] g:ש6°,ÿסצ¸ ¸oף=]]62#[[€¡e¨™•f|ט<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü</td><td>Block</td><td>1</td></tr>
<tr><td>54.79.76.74</td><td>Australia</td><td>147.237.72.166</td><td>aka.idf.il</td><td>Unauthorized URL Access to aka.idf.il/wp-admin/</td><td>Block</td><td>1</td></tr>
<tr><td>219.74.38.152</td><td>Singapore</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>1</td></tr>
<tr><td>105.198.243.139</td><td>Egypt</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Untraceable SSL Sessions: Open Mode</td><td>None</td><td>1</td></tr>
<tr><td>82.80.63.208</td><td>Israel</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Unauthorized URL Access to www.idf.il/french/</td><td>Block</td><td>1</td></tr>
<tr><td>203.127.96.196</td><td>Singapore</td><td>147.237.77.216</td><td>dover.idf.il</td><td>Distributed Unauthorized URL Access on www.idf.il/error.htm</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Illegal Byte Code Character in URL t…₪´¿„ˆnz3„g:ש6°,ÿסצ¸ ¸oף=]]62#[[€¡e¨™•f|ט lÊ[[#17]]¸€ü]]#25[[¶מ]]#16[[„<</td><td>Block</td><td>1</td></tr>
<tr><td>66.249.64.180</td><td>Israel</td><td>147.237.0.34</td><td>tikshuv.idf.il</td><td>Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/</td><td>Block</td><td>1</td></tr>
<tr><td>141.212.122.64</td><td>United States</td><td>147.237.77.19</td><td>law-forum.idf.il</td><td>Unauthorized URL Access to /x</td><td>Block</td><td>1</td></tr>
<tr><td>98.184.184.157</td><td>United States</td><td>147.237.76.42</td><td>refuah.idf.il</td><td>Abnormally Long Request method</td><td>Block</td><td>1</td></tr>
</table>