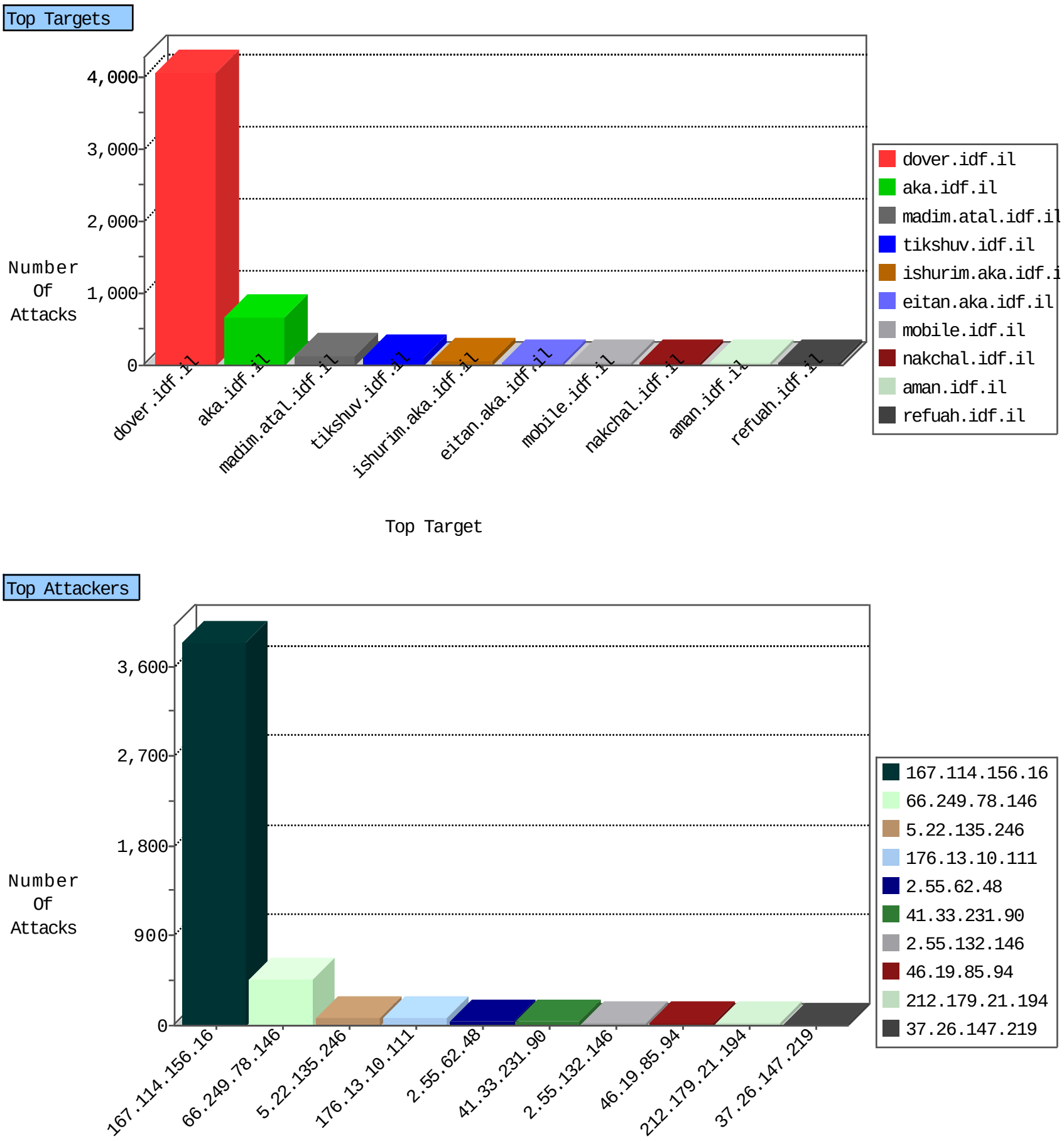
04-14-2016-09:04:03 to 04-14-2016-10:04:03

IDF Under Attack Daily Report



04-14-2016-09:04:03 to 04-14-2016-10:04:03

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	Block_Ip_Web_In	drop	3837
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
192.116.232.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
212.199.233.127	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
31.210.185.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
82.145.209.90	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
184.105.139.114	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
85.25.237.162	Germany	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.106	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
140.205.2.187	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.126	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1

04-14-2016-09:04:03 to 04-14-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.116.217.245	Russian Federation	147.237.0.34	tikshuv.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
185.106.92.47	Russian Federation	147.237.0.15	kosher-kravi.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	1

04-14-2016-09:04:03 to 04-14-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	469
82.80.180.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.135.246	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
213.8.159.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
180.153.151.102	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.130.220.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.111	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.117.154.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.28.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.153.151.102	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.253.157.0	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.239.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-14-2016-09:04:03 to 04-14-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.10.111	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
37.26.147.219	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.156.92	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
82.166.190.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
195.110.40.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.254	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.184	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.184	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.90.89.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.116.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.30.24.6	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.52.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
89.138.119.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.211	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.161	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.140.153	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.161	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
170.253.177.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
62.90.77.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.135.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.94.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.137.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.7.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.145.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.169.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
149.78.34.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.169.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.148.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.92.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.117.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.205.42	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
80.178.121.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.2.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.62.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
2.55.132.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
91.228.248.251	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
80.246.140.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.12.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.157.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 5.22.135.246	Block	4
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 5.22.135.246	Block	4
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Header Line from 5.22.135.246	Block	3
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 5.22.135.246	Block	3
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 5.22.135.246	Block	3
176.13.18.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 5.22.135.246	Block	3
109.253.209.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.228.248.251	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/8/	Block	3
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal HTTP Version from 5.22.135.246	Block	2
80.246.136.8	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 5.22.135.246	Block	2
75.17.232.116	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 5.22.135.246 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 5.22.135.246	Block	2
194.90.89.5	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 194.90.89.5	Block	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple NULL Character in Header Name from 5.22.135.246	Block	2
194.90.89.5	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	2
5.22.135.246	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.22.135.246 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple NULL Character in Url from 5.22.135.246	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.143.110.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/	Block	1
80.246.130.217	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/68320.doc	Block	1
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Name rx[[#12]]§»‡[[#7]]#,ÚÐ[[#6]][[#23]]ÆcŸkþ[[#23]]–D½V£Èt^[[#19]]Õ5•[v§¹ [[#19]]Ø•Ô•ö%Tw[[#12]]‡[[#2]]6[[#28]]'ïE±Ð•É[[#25]]¨uÌ[[#22]]Ì[[#18]]â[[#22]]$™[[#22]][[#20]][[#6]]äÅ[[#28]]¦F¨[[#7]]•IÓxn[[#0]]A©\ëó[[#11]]-„[[#0]]w[[#15]]ö3©Gë=Lpíóa[[#5]][[#18]][[#28]]¨¡•@’ÞÀ§{ÜâÆ[[#19]]ÌÄ	Block	1
147.236.232.252	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	NULL Character in URL y&[[#29]][˛[[#28]]¡”w}[[¥,|#8@]]51#[[oxj]]ѯmՈ3&µ̉ נ yךe˛ty6^[[#25]]k[[#26]]‹«Ư€cחr«˜ח›{v™ß„Þvק ®w[[#0]]Ú`4š![[#26]][[#17]][[#6]]y[[|#20)˛Úkq”tvv¶]]ɣ•[[41#]]“y[[#0]]$Þ˛כ x®[[#6]]“½ הk¾u+Ý[[ק#28[[]]#18ח˛‹„]]dɣÝ[[#23]]q[[#12]]˙¶[[#26]]b[[#21]], cצ×y'q§סךא	Block	1
85.250.50.254	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal HTTP Version [[#20]]a[[#8]]â @¤A¿°#!r?4ò„¸Â6DV[[#18]]Ž^R$ž ý–¨…(×¿ü´ @[[#19]]¶[[#8]]µ/³›[[#29]]Ëdø”[[#2]]}$+æ˜Q"Ó3SdšDøŒ[[#23]]_O”[[#26]]_‰ƒœÍÁ}[[#18]][[#17]]q‰Ž±û4n©ñ[[#21]]ð`Î[[#17]]-É•ÌÁ³%uÚ][[#7]]æM³rî 6œ>JµÑÂ„[[#12]]Ø¯[[#24]][[#7]]	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.i l	Unauthorized URL Access to 147.237.76.39/	Block	1
5.22.135.246	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.168	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ww.refua.atal.idf.il/Templates/SendToFriend/SendToFriend.aspx?&l=he&f=14 71 in URL	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/common/includes/globaltopbar/resources/styles/portalhea der.css.asp	Block	1
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1