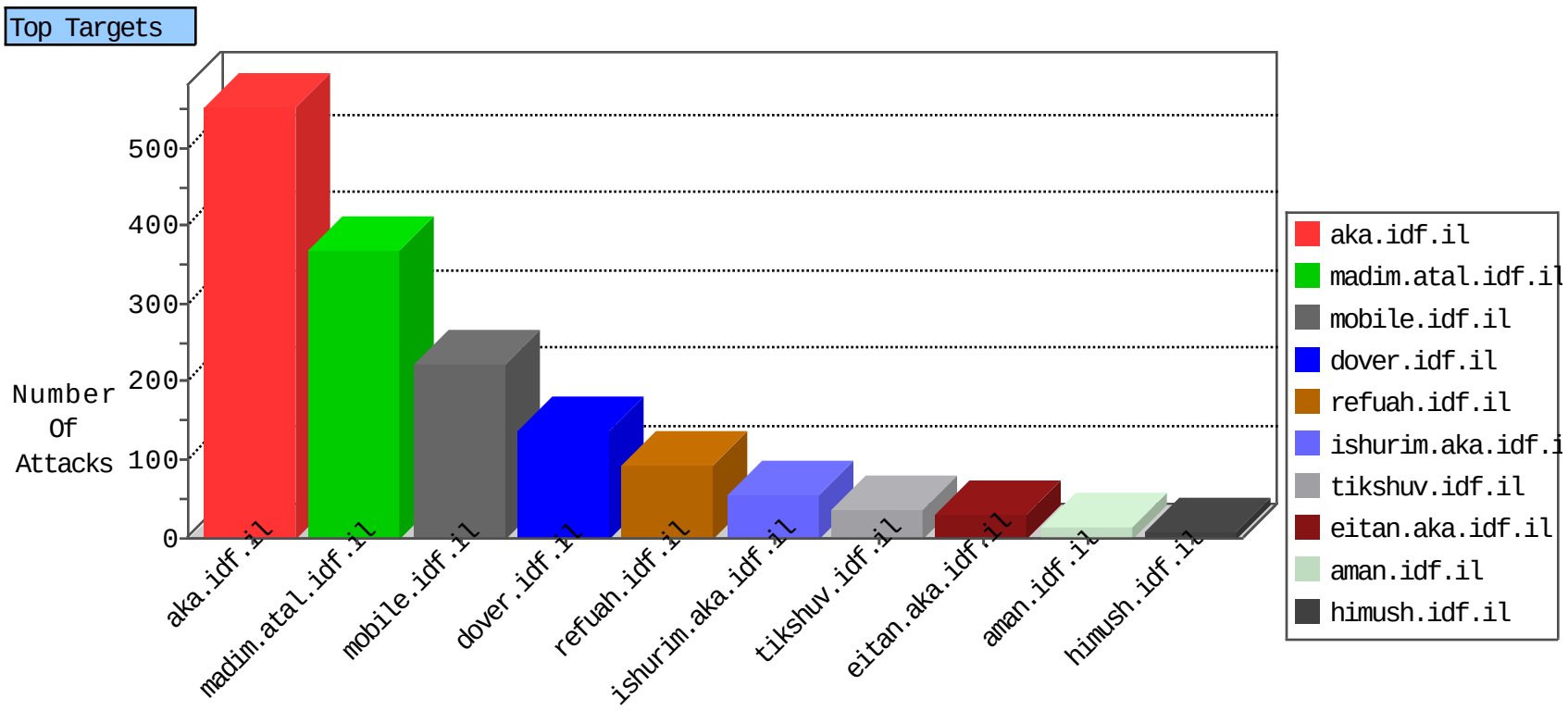
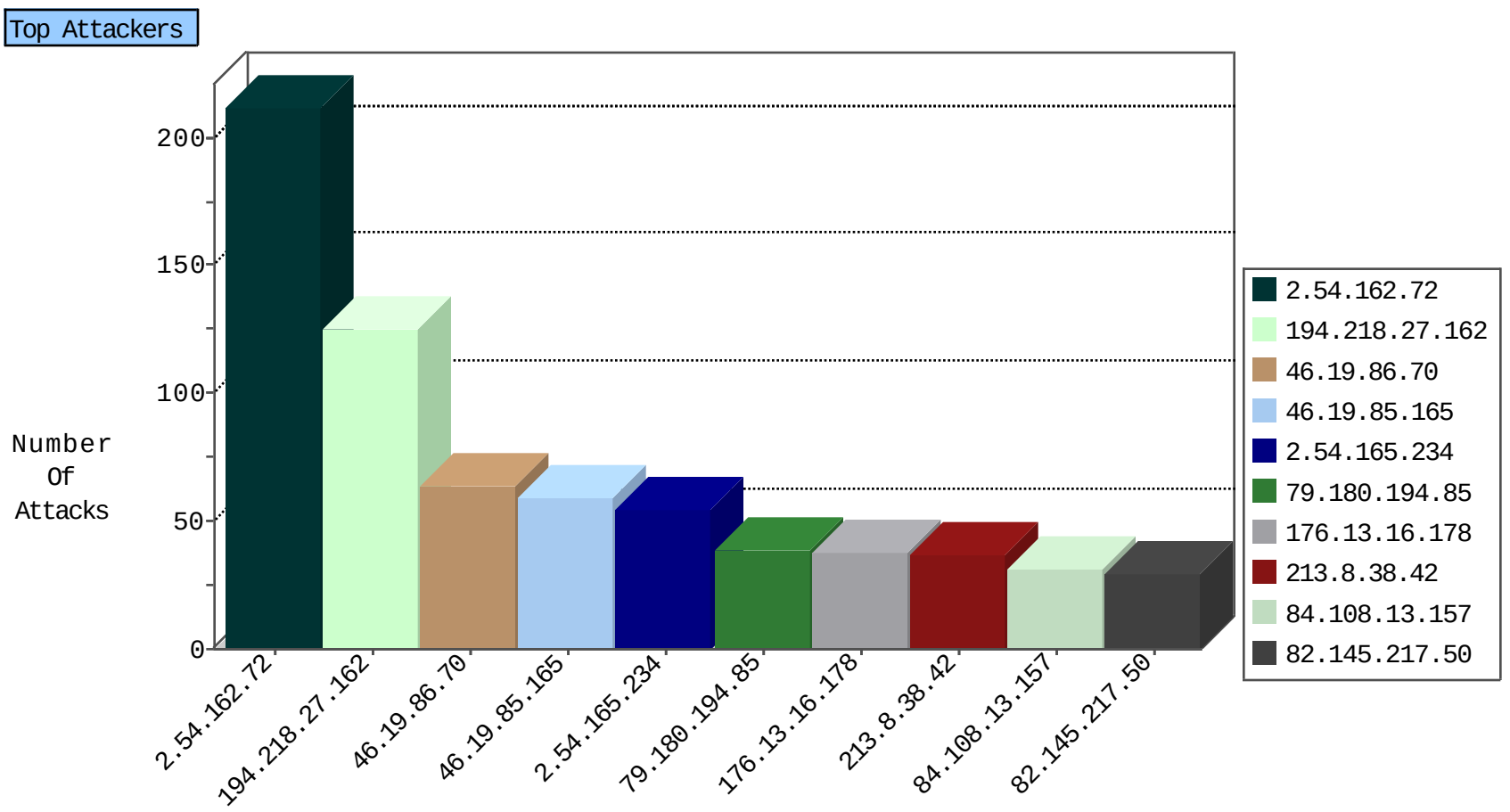
02-29-2016-11:04:02 to 02-29-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-11:04:02 to 02-29-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.217.50	Europe	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	29
82.145.219.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.162.158	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
159.104.163.19	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.102.239.27	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
159.104.163.20	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.17	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.18	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.22	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.145.217.189	Europe	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	1

02-29-2016-11:04:02 to 02-29-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.207.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
212.179.42.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
31.31.73.93	Czech Republic	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.214.249.146	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-29-2016-11:04:02 to 02-29-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
134.191.232.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.15.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.17.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.230.54.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.39.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.139.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.116.89.27	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.245.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.63.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.59.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
136.243.130.9	147.237.77.243	Germany	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.54.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.5.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
92.61.225.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.255.154.161	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.62.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.74.100.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.112.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.139.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.9.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-29-2016-11:04:02 to 02-29-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
2.54.165.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
213.8.38.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
79.180.194.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
176.13.16.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
84.108.13.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.58.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.22.131.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.95.61.247	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	13
79.183.142.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.228.78.15	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.132.68	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.194.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.14.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.179.21.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.37.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.219.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.12.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.36.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.99.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.140.255	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
37.26.146.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.139.8	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.49	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.179.8.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.132.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.139.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.74.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.20.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.204.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.146.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-11:04:02 to 02-29-2016-12:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.64.15.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.59.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.137.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.0.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-11:04:02 to 02-29-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.162.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	212
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
109.67.24.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.54.165.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
176.13.16.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
84.108.13.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
188.138.159.69	Moldova, Republic of	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
188.138.159.69	Moldova, Republic of	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.138.159.69	Block	5
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	4
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
31.168.219.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.37.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.34.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.206.77	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
46.19.85.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.219.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.0.252	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.0.252	Block	2
62.90.100.124	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.90.100.124	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.60	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
169.229.3.91	United States	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
79.177.177.217	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.92	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
37.26.146.209	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.13.47.139	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.13.47.139	Block	1
85.64.210.34	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at û0ë´^¼˜•N#012þô[[#3]]e[[#5]]©¶C[[#3]]ºàÏAªê}á[[#28]]Ÿ)–ìì	Block	1
176.13.18.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ס׳ג	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
85.64.210.34	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
52.48.17.30	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
86.32.225.87	Austria	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	1
169.253.194.1	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
85.64.210.34	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL [[ט#23\eœ]]ע˜x¸#*וו9¸‰t"^Ê'†¡^]]uÝ%zg•¨ü•]l^Ÿ“[[#0]]•q[[#30…ם§]]#12[[]]#2[[]]#18[[]]#26[[Žt(z[[#15]]{[[#27]]ɔ!‹…:dj£„qp”ž•u	Block	1
85.64.148.229	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.148.229	Block	1
46.19.86.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method ³a[[#25]]x¥c•af–},Lžæ‡»tŽ¸ÊßK	Block	1
95.13.47.139	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

02-29-2016-11:04:02 to 02-29-2016-12:04:02