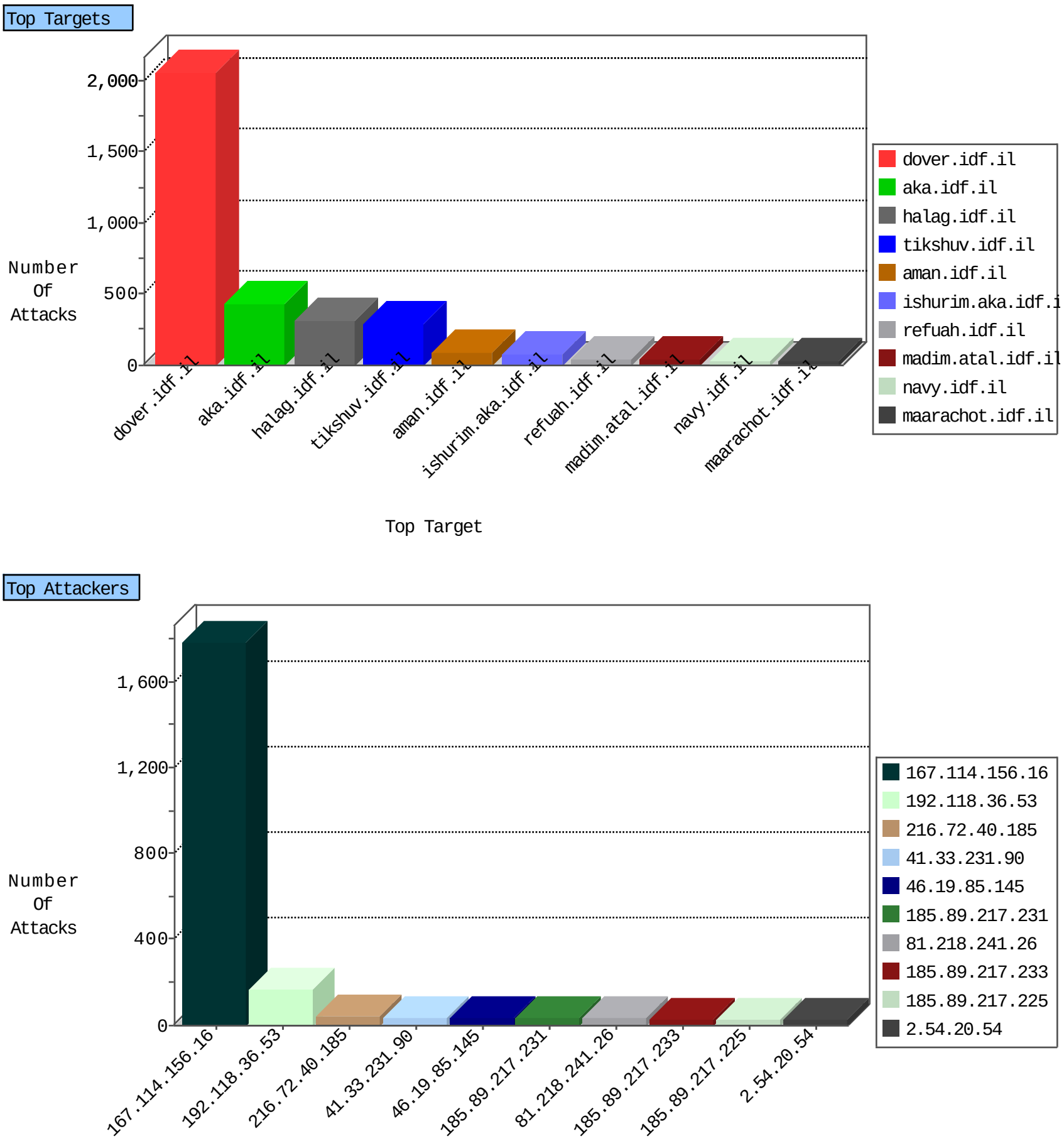
01-12-2016-09:04:04 to 01-12-2016-10:04:04

IDF Under Attack Daily Report



01-12-2016-09:04:04 to 01-12-2016-10:04:04

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	3009
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1115
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
185.35.62.80	Switzerland	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.101	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.231	Switzerland	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-09:04:04 to 01-12-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-12-2016-09:04:04 to 01-12-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	13
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
2.52.159.67	147.237.72.166	Israel	aka.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
193.104.41.54	147.237.8.28	Moldova, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.138.240.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.212.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.42	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.177	Moldova, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.80.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1

01-12-2016-09:04:04 to 01-12-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.89.217.231		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	31
185.89.217.225		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	26
85.158.139.101	United Kingdom	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	25
185.89.217.227		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	24
185.89.217.228		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	24
185.89.217.234		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	24
185.89.217.226		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	23
185.89.217.232		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	23
185.89.217.233		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	23
185.89.217.229		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	22
185.89.217.230		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	21
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	21
185.89.217.224		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	18
62.0.197.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.10	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
79.177.221.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.58.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.245	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.177.208.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
31.154.4.18	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	13
31.154.4.18	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.235		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
62.0.206.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.87.78.105	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.158.138.19	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
81.218.193.212	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
62.0.206.1	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
2.52.40.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.235.103.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
81.218.22.216	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.170	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
132.76.10.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

01-12-2016-09:04:04 to 01-12-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.36.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
212.25.83.133	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	9
176.13.16.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
31.168.152.32	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	4
93.173.12.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
109.253.129.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.95.226.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.26.147.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.146.82	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
176.13.20.23	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
84.95.226.189	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.230.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
212.76.98.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjh7l3k4qpkahwbwhqkhvl7dfoqfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
37.59.123.142	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
134.213.135.146	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/http:/www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
207.46.13.40	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/skin/pukiwiki.css.php	Block	1
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giy	Block	1
109.64.55.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.35.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
81.218.44.27	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
219.94.192.47	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.192.47	Block	1
37.26.147.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.192.33	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-19503-he	Block	1
2.52.51.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ; in URL __atuvc=1	Block	1
176.13.23.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.254.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.57.205	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/1133-he/dover.aspx	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
142.4.0.72	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
31.13.112.119	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.252.56	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.67.252.56 (Protocol violation (SSL_CONN_CLIENT_FINISH))	None	1

01-12-2016-09:04:04 to 01-12-2016-10:04:04