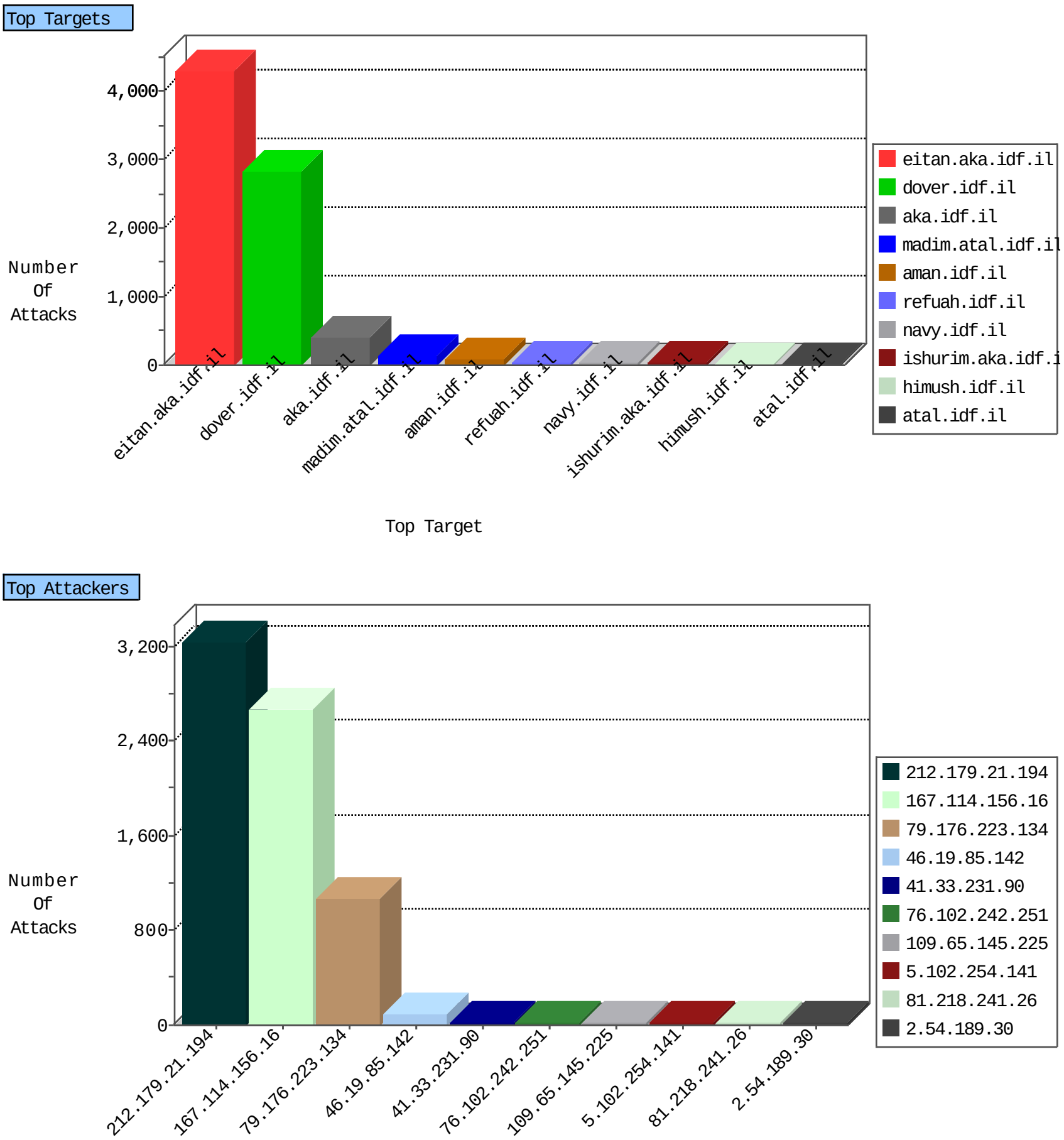
12-03-2015-16:04:04 to 12-03-2015-17:04:04

IDF Under Attack Daily Report



12-03-2015-16:04:04 to 12-03-2015-17:04:04

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	3358
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
121.224.91.182	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	4
119.123.146.16	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	3
39.115.45.16	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
124.130.148.254	China	147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	2
59.172.176.47	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
113.64.53.224	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
116.21.163.117	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
84.23.52.242	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
49.71.192.155	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
175.136.133.219	Malaysia	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.56.238	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-03-2015-16:04:04 to 12-03-2015-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-03-2015-16:04:04 to 12-03-2015-17:04:04

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
93.172.46.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.118.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.138.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.23.176.210	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.27.105.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.186.125.104	147.237.0.17	Pakistan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
84.94.181.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.13.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.254.217.114	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
128.199.41.249	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

12-03-2015-16:04:04 to 12-03-2015-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	894
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.14	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
76.102.242.251	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
76.102.242.251	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	11
79.176.29.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.250	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.180.162.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
143.112.32.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.229.11.88	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.102.254.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.229.11.88	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
93.173.250.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.54.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.129.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.155.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.60.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.138.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.164.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
145.108.40.164	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.123.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.29.100	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.15.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
100.100.95.92		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
100.100.103.55		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.161.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
42.118.11.178	Vietnam	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.189.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
197.37.49.160	Egypt	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
100.100.86.195		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.34.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.217.19.193	Switzerland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
157.55.39.147	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.118.27.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.186.42.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.143.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.56.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.217.19.193	Switzerland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.80.182	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

12-03-2015-16:04:04 to 12-03-2015-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	2518
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	678
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	174
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
5.102.254.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
212.179.28.34	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	6
212.179.49.226	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 212.179.49.226	Block	5
79.183.62.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.62.10	Block	4
5.29.145.204	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
79.183.62.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
2.54.144.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.117.183.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.117.183.158	Block	3
109.64.185.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.117.183.158	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
192.117.183.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
5.29.141.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.163.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.131.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/5/size220x0/1615.jpg.	Block	2
84.94.25.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.145.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
84.108.194.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.146.159	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
157.55.39.147	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
79.181.173.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
79.183.165.249	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.atal.idf.il/xmlrpc.php	Block	1
173.252.90.100	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.178	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
109.65.145.225	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
23.25.225.221	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.65.145.225	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
212.179.49.226	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
157.55.39.46	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	1
2.54.138.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
87.69.241.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.67.186.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
65.182.127.13	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.145.225	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
82.81.45.133	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.120.125.55		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.247	United States	147.237.76.30	himush.idf.il	Unknown Parameter v in www.chimush.atal.idf.il/cdn/1515/applications/adcnet/main-apc-min.css	None	1
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.145.225	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
213.57.91.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
76.102.242.251	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
157.55.39.28	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/news/news.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.52.140	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1

12-03-2015-16:04:04 to 12-03-2015-17:04:04