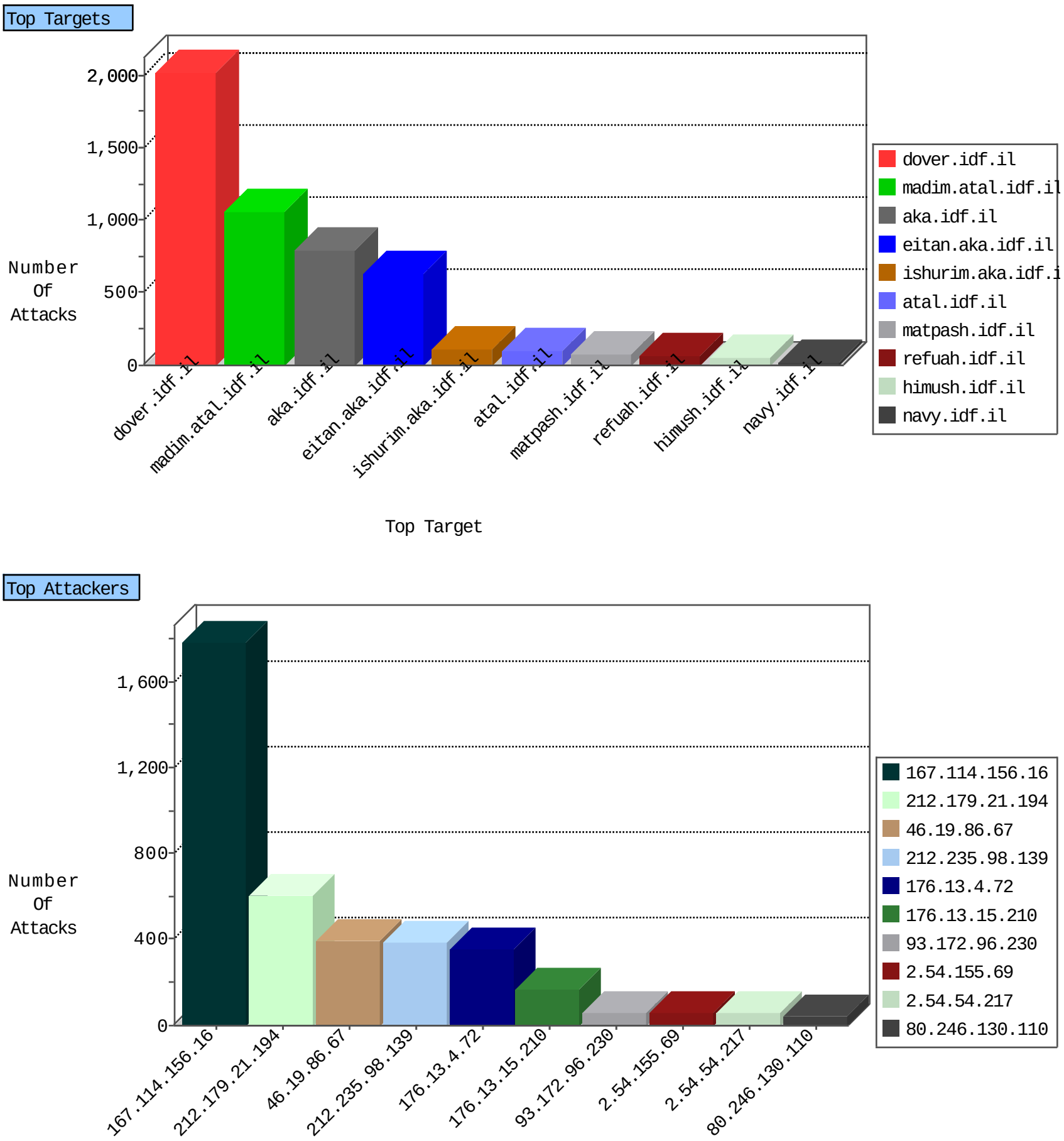
12-06-2015-09:04:01 to 12-06-2015-10:04:01

IDF Under Attack Daily Report



12-06-2015-09:04:01 to 12-06-2015-10:04:01

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	3326
79.178.48.152	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.8	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
118.193.21.98	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-06-2015-09:04:01 to 12-06-2015-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-06-2015-09:04:01 to 12-06-2015-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.68.85.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.42.38.207	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.42.38.207	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
212.199.112.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.223	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
5.42.38.207	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.38	Cote D'Ivoire	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
62.38.250.31	147.237.72.14	Greece	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
176.13.7.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.206.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.95.44.69	147.237.76.42	Canada	refuah.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.95.44.69	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
5.42.38.207	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
5.42.38.207	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.226	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.42.38.207	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.166.98.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.42.38.207	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
217.194.197.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.193.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.42.38.207	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.143.3.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.38.250.31	147.237.72.14	Greece	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
5.42.38.207	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
188.120.132.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.149.161.186	147.237.72.167	China	ishurim.aka.idf.il	GPL SCAN nmap TCP	1
174.95.44.69	147.237.76.176	Canada	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
174.95.44.69	147.237.72.217	Canada	e.idf.il	ET SCAN Potential SSH Scan	1
5.42.38.207	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
174.95.44.69	147.237.8.27	Canada	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
5.42.38.207	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.226	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
5.42.38.207	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

12-06-2015-09:04:01 to 12-06-2015-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	384
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	178
66.249.93.215	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	42
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
46.19.85.129	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
62.219.161.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
80.246.130.110	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
82.205.107.144	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
83.244.52.202	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
80.246.130.110	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
37.26.147.226	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
82.166.53.161	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	18
2.54.12.41	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
77.247.178.53	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
109.66.188.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
2.54.54.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.54.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
109.66.188.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.54.54.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.54.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.54.54.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
79.179.129.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.180.248.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.54.24.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.69.48.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.125	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
66.249.93.219	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.149	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.137.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
108.171.128.161	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.41	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.12.41	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.147.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.36.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.189.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.16.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

12-06-2015-09:04:01 to 12-06-2015-10:04:01

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	Distributed Too Many of the Same Response Code (404)	Block	392
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	257
176.13.4.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	235
176.13.4.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.15.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
176.13.15.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
2.54.155.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.96.230	Block	41
82.80.219.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	32
132.73.110.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/homas/site/resources/services/wsmaterials.asmx/getcompaniesbyprefix	Block	17
176.13.4.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	12
80.179.184.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.34.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.4.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	5
80.246.138.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.1.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.67.181.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyu	Block	4
37.26.147.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
82.205.107.144	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
213.57.109.5	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/1133-22638-he/dover.aspx.	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
80.246.136.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.102.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.181.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.12.138.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.51.120.142	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	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
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/sendtofriend/sendtofriend.js	Block	1
195.154.168.82	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
178.154.243.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/15749.jpg	Block	1
2.52.157.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.219.164	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
212.117.180.21	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.255.253.167	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
176.12.141.20	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

12-06-2015-09:04:01 to 12-06-2015-10:04:01