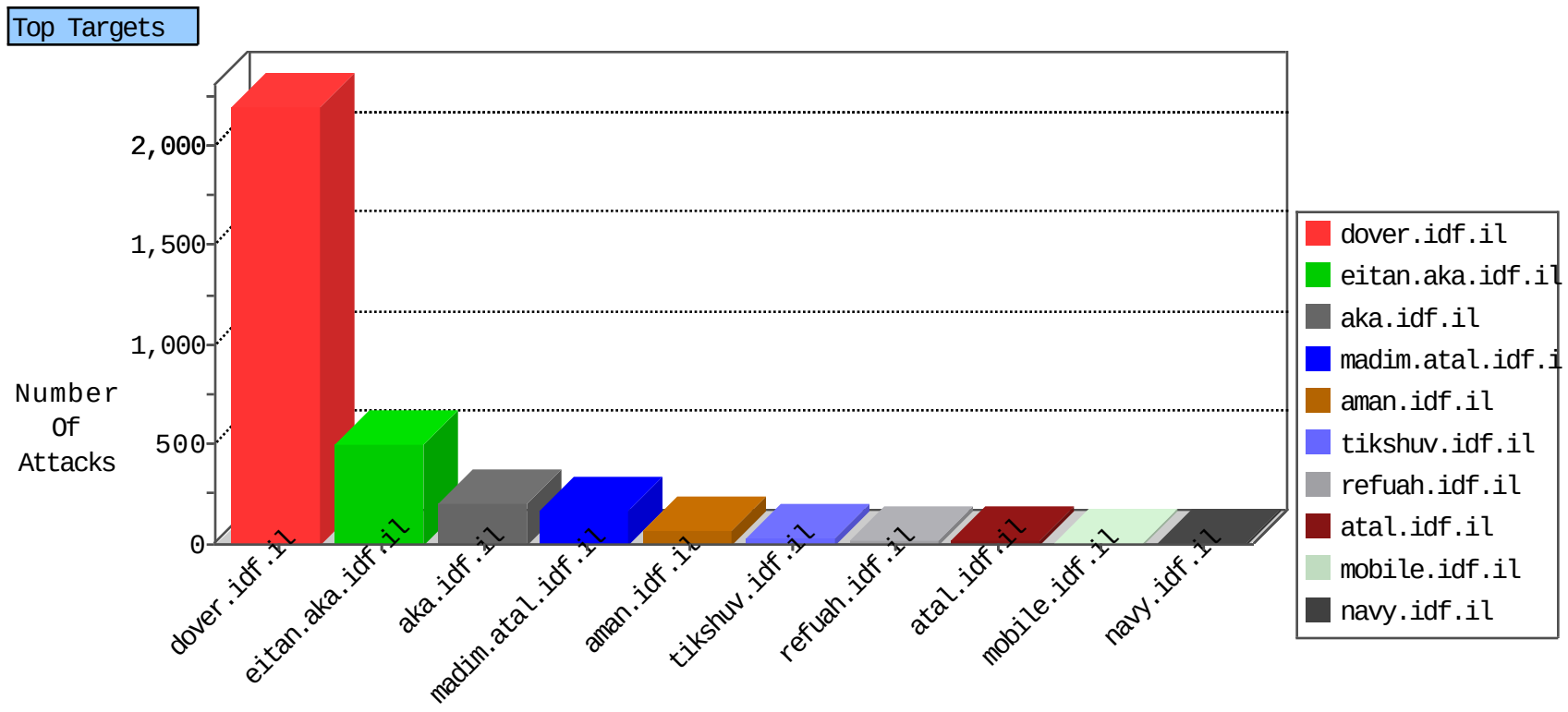
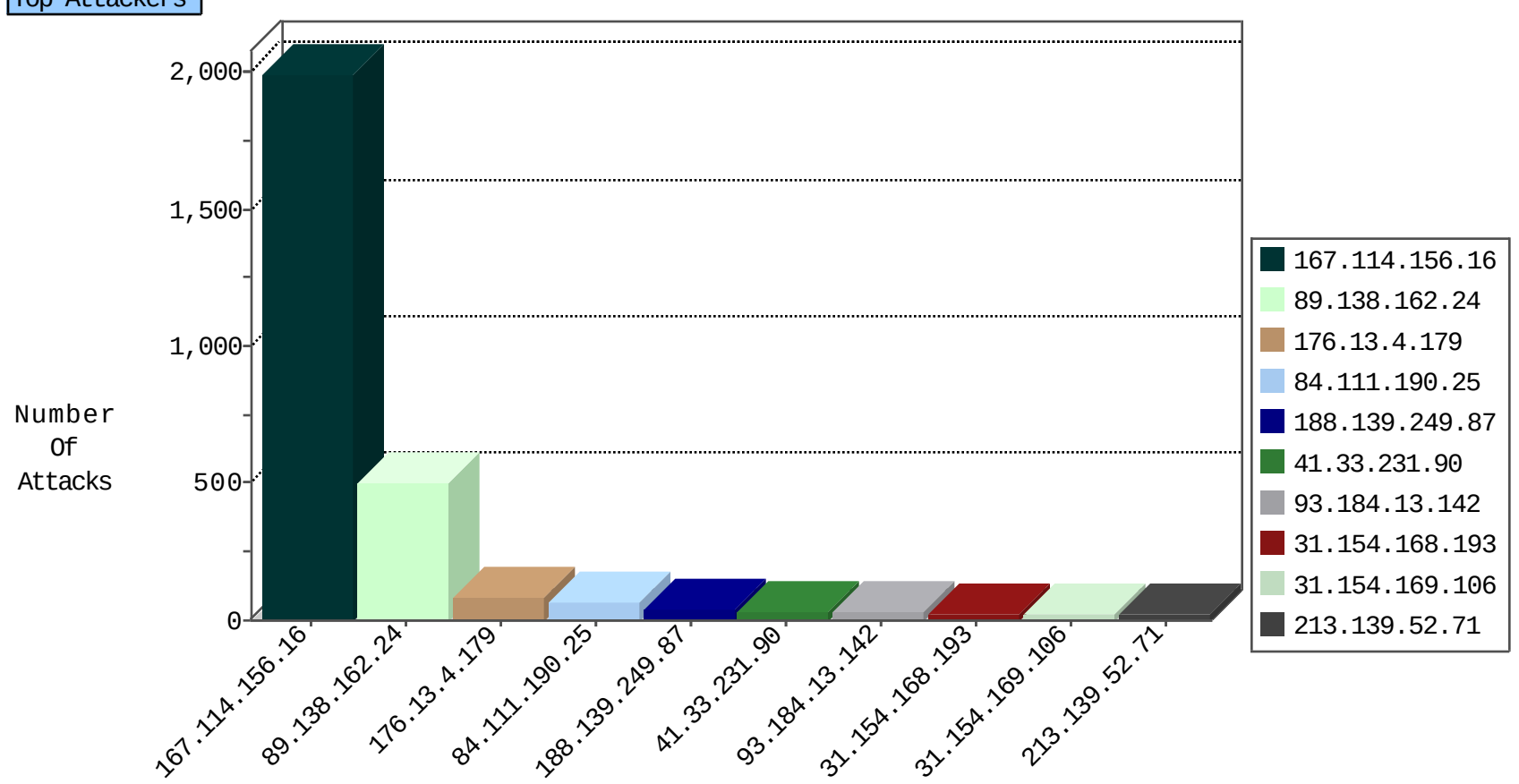
12-06-2015-23:04:00 to 12-07-2015-00:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-06-2015-23:04:00 to 12-07-2015-00:04:00

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	3645
66.249.65.37	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	24
200.109.66.194	Venezuela	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	3
118.193.21.98	China	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

12-06-2015-23:04:00 to 12-07-2015-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-06-2015-23:04:00 to 12-07-2015-00:04:00

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
109.67.54.251	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.64.69	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.6	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.200	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
222.186.56.115	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.30.215	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
60.29.182.175	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.215	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
60.29.182.175	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.215	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.113	147.237.76.200	Ukraine	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
60.29.182.175	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.146.220.220	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.0.19	Cote D'Ivoire	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
187.161.117.121	147.237.72.217	Mexico	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.117.40.23	147.237.77.216	Russian Federation	dover.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
222.186.56.115	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
60.29.182.175	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.215	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
60.29.182.175	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.215	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.113	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
60.29.182.175	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.170.241	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.146.220.220	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.0.19	Cote D'Ivoire	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
74.117.209.135	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
187.161.117.121	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.160.184.241	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1

12-06-2015-23:04:00 to 12-07-2015-00:04:00

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	34
31.154.169.106	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	23
188.139.249.87	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
188.139.249.87	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
213.57.128.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
213.57.133.11	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.85.125	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
31.154.168.193	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
31.154.168.193	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
149.78.28.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.181.118.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
93.184.13.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
66.249.93.228	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.162.24	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.184.13.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.176.225.29	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.129.216	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.59		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
199.30.25.150	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.121.54	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.120.126.59		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.130.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
93.184.13.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.78.78.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
213.57.130.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.32.179.11	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
91.200.12.137	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
77.127.163.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.13.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.120.71	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.26	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	3
95.35.148.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.229.35.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.145.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.137.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.8.204.26	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.181.208.243	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
66.249.93.231	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.143.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.130.171.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.78.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3

12-06-2015-23:04:00 to 12-07-2015-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.162.24	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	497
176.13.4.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
84.111.190.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 213.139.52.71	Block	5
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 213.139.52.71	Block	5
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 213.139.52.71	Block	4
176.228.64.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.125.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	2
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 213.139.52.71	Block	2
2.54.30.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	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
89.139.7.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Malformed URL safari/537.36	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	1
83.10.57.57	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
185.120.126.59		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2422.jpg	Block	1
41.253.72.136	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 0.2490.86 in URL safari/537.36	Block	1
109.160.237.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.244.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
213.8.204.56	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
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	1
176.13.0.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english	Block	1
83.10.57.57	Poland	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
149.78.28.88	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
89.138.83.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.146.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.135.241	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.179.135.241 (Open Mode)	None	1
207.46.13.131	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/sitemap.aspx	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
83.130.123.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
195.62.53.168	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to /css/css	Block	1
157.55.39.149	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic	Block	1
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
207.46.13.134	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/recruitinformation	Block	1
79.181.118.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.117.40.23	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/manager/html	Block	1

12-06-2015-23:04:00 to 12-07-2015-00:04:00