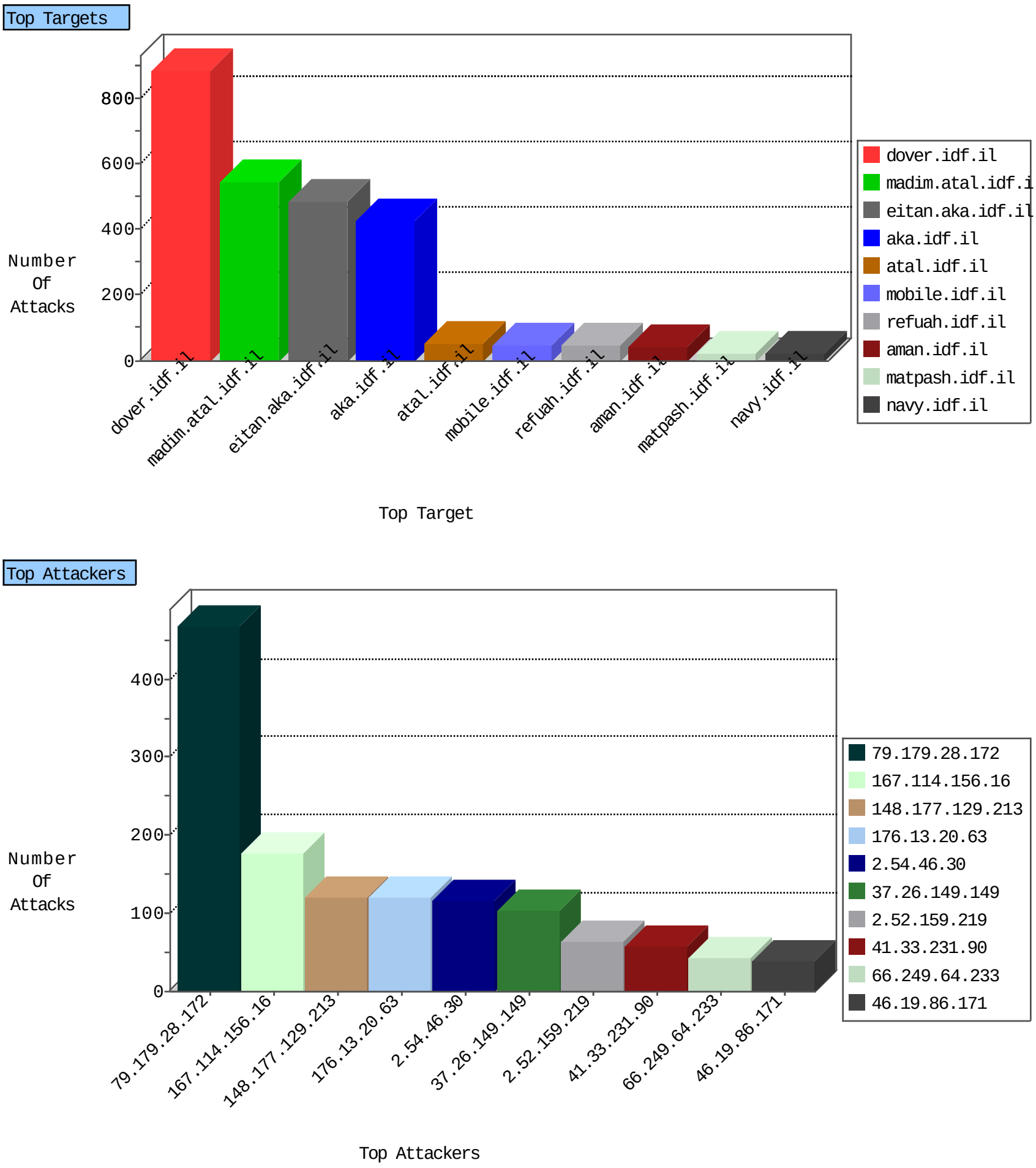
11-23-2015-13:04:03 to 11-23-2015-14:04:03

IDF Under Attack Daily Report



11-23-2015-13:04:03 to 11-23-2015-14:04:03

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	HTTP-POST-Segmented-DoS	dest-reset	9797
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3898
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
37.78.36.254	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
212.179.64.162	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

11-23-2015-13:04:03 to 11-23-2015-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.130	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.128.35.131	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
84.228.86.176	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-23-2015-13:04:03 to 11-23-2015-14:04:03

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	2
46.151.55.35	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.106.226.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
110.244.29.89	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.154.19.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.86.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.0.16	Poland	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
88.247.194.10	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.109.32.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.100.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.255.43.24	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
183.62.78.18	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
65.255.43.24	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
180.153.104.125	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.207.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.92.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.87.201.199	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.149.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.174.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.192.68.46	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.21.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.62.78.18	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
65.255.43.24	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
180.153.104.125	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1

11-23-2015-13:04:03 to 11-23-2015-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.28.172	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	459
148.177.129.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
46.19.86.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
168.63.200.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
194.31.58.8	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.107.198		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.182.13.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	14
100.100.2.112		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
197.45.84.172	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.108.147.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.107.198		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
125.88.8.235	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.26.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
194.203.215.201	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
79.181.106.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
155.254.215.191	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.0.156.161	Norway	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.1.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.43.203		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
86.180.133.92	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.7	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.114.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
80.246.136.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
62.0.84.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.177.125.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.117.36.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.30.25.170	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.172.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.1.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.88.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

11-23-2015-13:04:03 to 11-23-2015-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
2.54.46.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
176.13.20.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
2.52.159.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
176.13.20.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
2.54.46.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.150.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
80.246.139.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
176.12.151.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
79.179.28.172	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
176.12.143.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.159.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
109.105.167.126	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.105.167.126	Block	6
194.90.240.21	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	5
194.187.81.32	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	4
104.227.190.115		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.76.114.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20698-he/dover.aspx&sa=u&ved=0ahukewjjpiuiuqbjahxiubokht7fab4qfggvmaq&usg=afqjcnegcv2el-yxic5u3qhu4f6yetxf-g	Block	3
81.218.251.251	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.251.251	Block	3
37.142.158.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
185.120.126.43		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.162.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.65.202.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.64.112.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	2
66.249.93.187	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
2.52.2.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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	2
84.108.171.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/givus	Block	2
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.0.80.200	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	2
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
212.179.64.162	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.180.35.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
176.13.22.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.35.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.251.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.2.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
141.212.122.96	United States	147.237.77.170	maarachot.idf.il	Distributed Malformed URL	Block	1
80.246.133.203	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.25.103.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.183.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.126.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.114.23.210	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894- he/matpash.aspx	Block	1

11-23-2015-13:04:03 to 11-23-2015-14:04:03