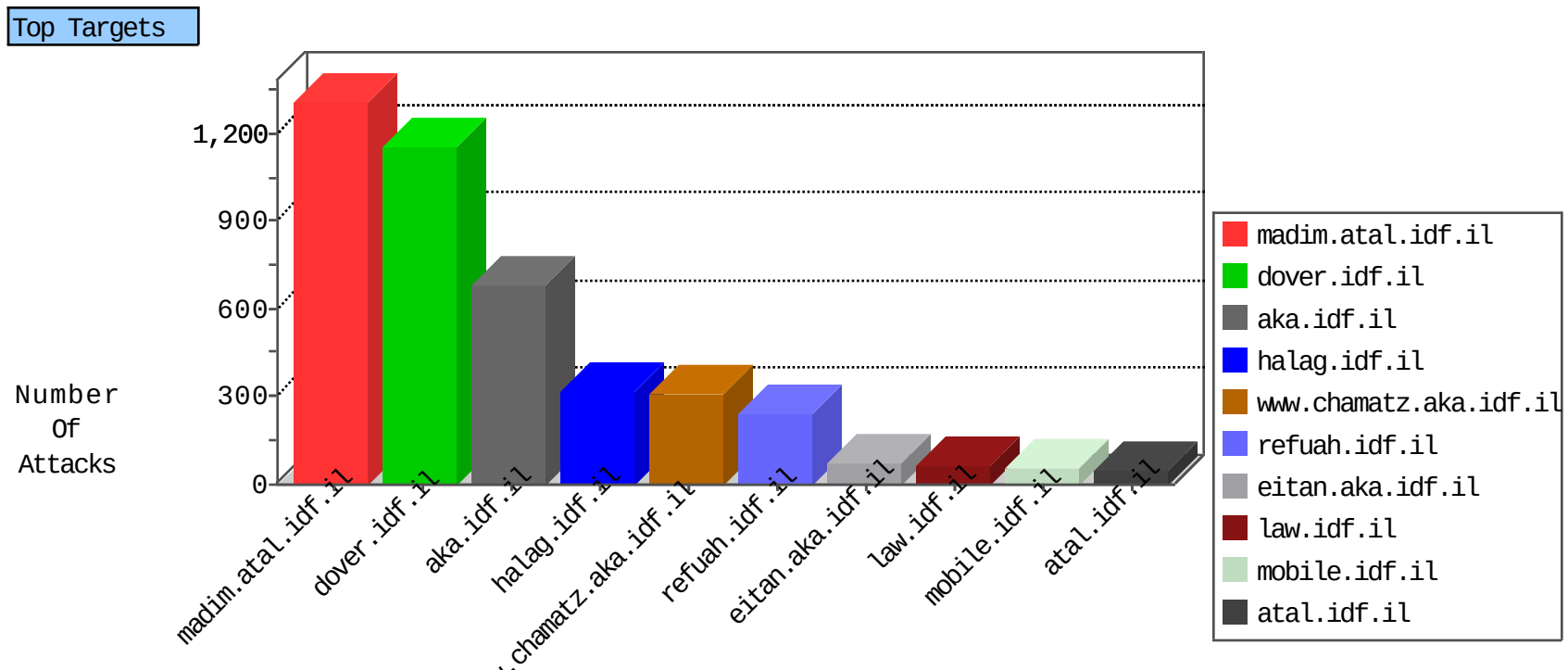
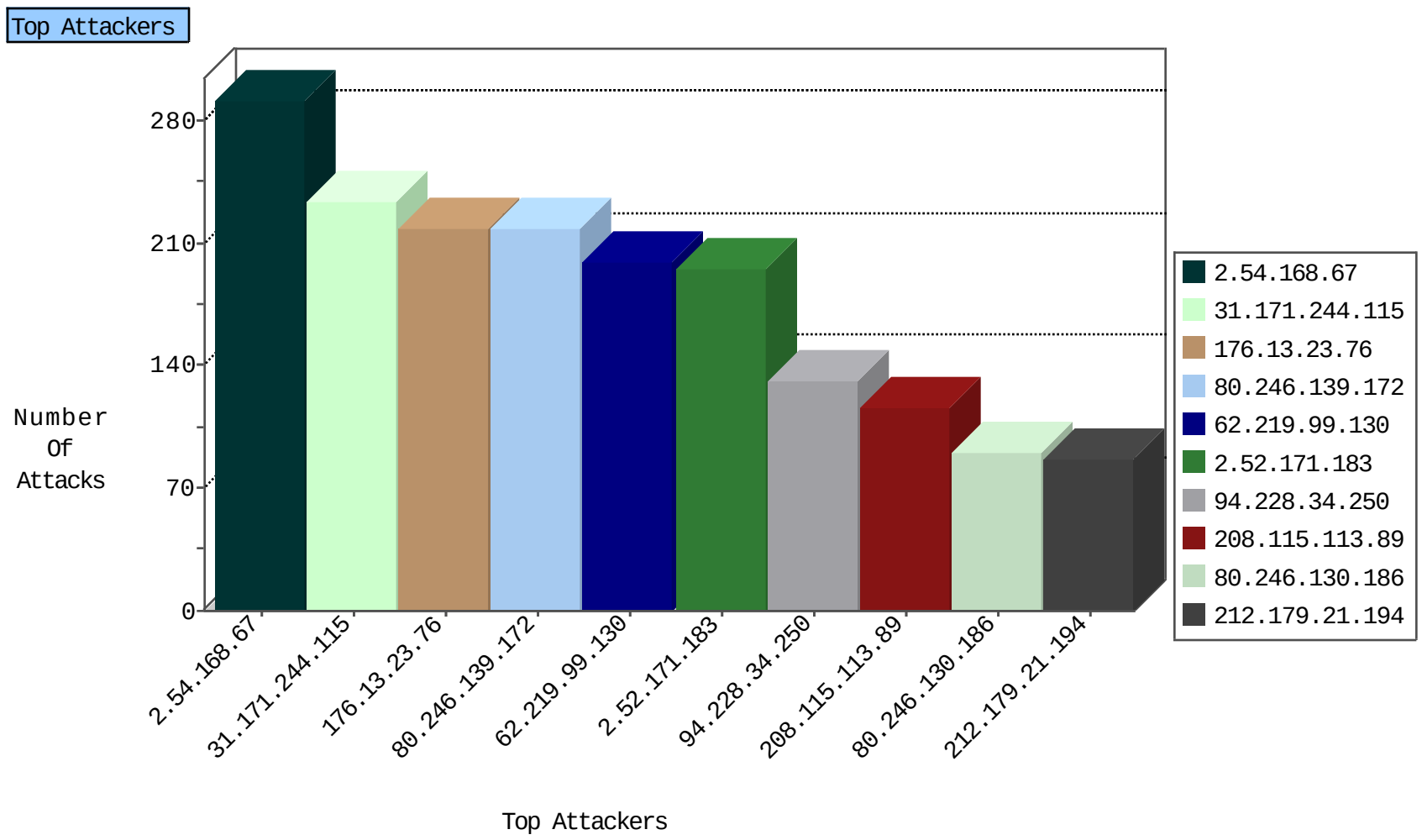
11-24-2015-11:04:07 to 11-24-2015-12:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-24-2015-11:04:07 to 11-24-2015-12:04:07

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	TCP handshake violation, first packet not syn	drop	19164
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3561
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
204.42.253.130	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
66.249.66.96	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.130	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-24-2015-11:04:07 to 11-24-2015-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.124.109.87	New Zealand	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
168.63.12.166	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
83.168.248.11	Sweden	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
2.54.17.116	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
168.63.12.166	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
82.80.193.244	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.172.144.215	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
168.63.12.166	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.139	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
198.154.238.249	United States	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
83.168.248.11	Sweden	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

11-24-2015-11:04:07 to 11-24-2015-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.62	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	30
83.168.248.11	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	21
168.63.12.166	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	17
202.124.109.87	147.237.72.166	New Zealand	aka.idf.il	SQL Injection - Select From	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.19.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.217.27.17	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.29.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.65.37	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.17.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.115.113.89	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
23.95.248.139	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
195.160.240.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.237.168.157	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.12.127.94	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.181.173.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.0.130.116	147.237.77.216	Sudan	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1

11-24-2015-11:04:07 to 11-24-2015-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.171.244.115	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	234
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
80.246.130.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
80.246.133.3	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
84.228.29.115	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
69.41.14.215	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	36
69.41.14.155	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	36
84.228.108.104	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
185.32.179.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
178.128.235.185	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
212.0.130.116	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
99.89.32.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	28
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.64.135.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.57.133.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
87.68.73.0	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.85.167	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	19
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.54.21.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.6.36		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
74.125.57.73	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
172.56.12.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.199.34.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
91.144.30.96	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
88.191.108.74	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.179.28.215	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
176.13.23.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
138.134.192.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
100.100.6.36		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.23.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.168.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	151
176.13.23.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	125
80.246.139.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
2.54.168.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
2.52.171.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
80.246.139.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	94
176.13.23.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
2.52.171.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	89
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
2.54.55.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
176.13.6.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
2.54.168.67	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	20
185.32.179.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.168.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	6
91.205.155.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.105.98.166	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.105.98.166	Block	5
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
87.139.239.188	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	4
46.19.85.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	4
176.13.10.57	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	3
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.88.143.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.143.163	Block	3
176.13.14.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.22.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.188.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.12.150.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.13.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.139.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.2.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.159	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
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
8.37.234.158	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 8.37.234.158	Block	2
176.13.6.66	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.17.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.43.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.64.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.156.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.182.10	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 2.54.182.10	Block	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/do	Block	1
149.78.112.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
212.199.34.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1