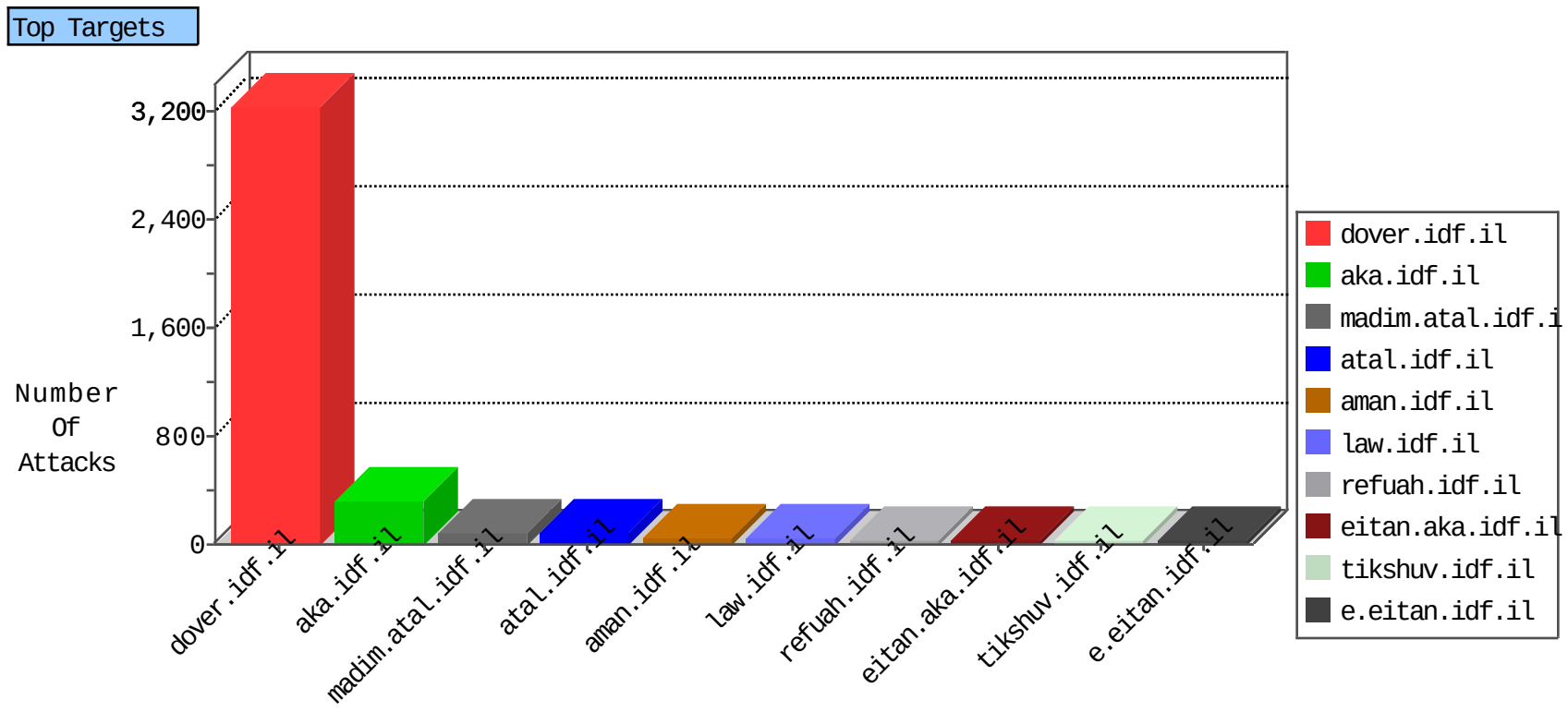
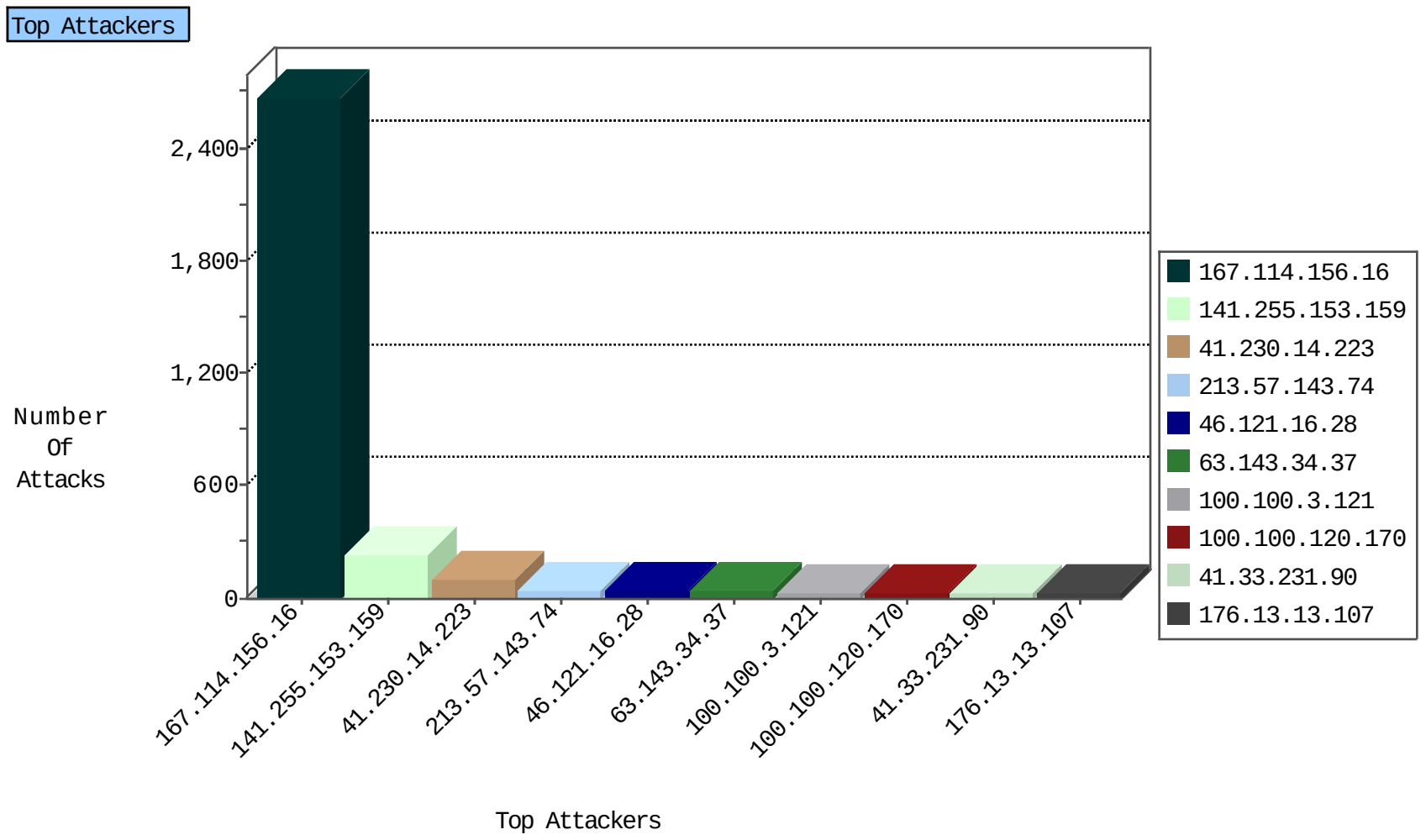
12-02-2015-22:04:09 to 12-02-2015-23:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015-22:04:09 to 12-02-2015-23:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.153.159	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	5372
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3513
79.179.196.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

12-02-2015-22:04:09 to 12-02-2015-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.251.25.176	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
63.143.34.37	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
63.143.34.37	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
64.251.25.176	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.168.193.34	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
91.142.253.133	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
91.142.253.133	Netherlands	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
184.168.193.34	United States	147.237.0.34	tikshuv.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
151.80.31.103	Italy	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.226.9	France	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
62.210.226.9	France	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

12-02-2015-22:04:09 to 12-02-2015-23:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
63.143.34.37	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	23
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
91.142.253.133	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	7
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
64.251.25.176	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	2
109.66.146.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.49.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
222.186.21.72	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
2.54.28.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.178.78.138	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.80.162.188	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
79.182.229.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.72	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.72	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
220.178.78.138	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

12-02-2015-22:04:09 to 12-02-2015-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.100.120.170		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.3.121		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
46.121.16.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
213.57.143.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
100.100.3.121		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
77.125.120.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.104.89		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.121.16.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.121.16.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.7.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
176.13.7.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
194.88.154.138	Poland	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.139.101	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.195.107	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.124.100		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.110.85	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.104.89		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.186.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.11.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.148.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.89.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.33.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.136.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.54.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.40.182.148	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.254.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.121.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	68
176.13.13.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.165.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	9
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.186.60.132	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.60.132	Block	5
5.29.46.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	4
207.46.13.103	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.103	Block	4
2.54.149.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
173.254.55.58	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	3
109.66.171.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.146.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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	2
173.254.55.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	2
109.186.60.132	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.12.144.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.40.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.60.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
46.121.89.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method em2lzq in URL	Block	1
173.254.55.58	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.254.55.58	Block	1
79.178.129.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templ@es/home.asp	Block	1
109.67.178.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/3/423.pdf	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.147.170	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
95.86.105.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewi50l2shb7jahvc8q4khetkaxgqfggwmai&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
46.116.131.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.106.227.129	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 176.106.227.129	Block	1
82.166.57.237	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
77.125.103.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
157.55.39.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/20_10_03_strike_eng.asf	Block	1
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templ@es/homepage/homepage.aspx	Block	1
109.64.177.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18189-he/dover.aspx	Block	1
213.57.206.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.204.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.253.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2802.jpg	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
79.178.171.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter answerid in www.aka.idf.il/sachar/login/	None	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter amp;moduletogoto in www.aka.idf.il/giyus/login/	None	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