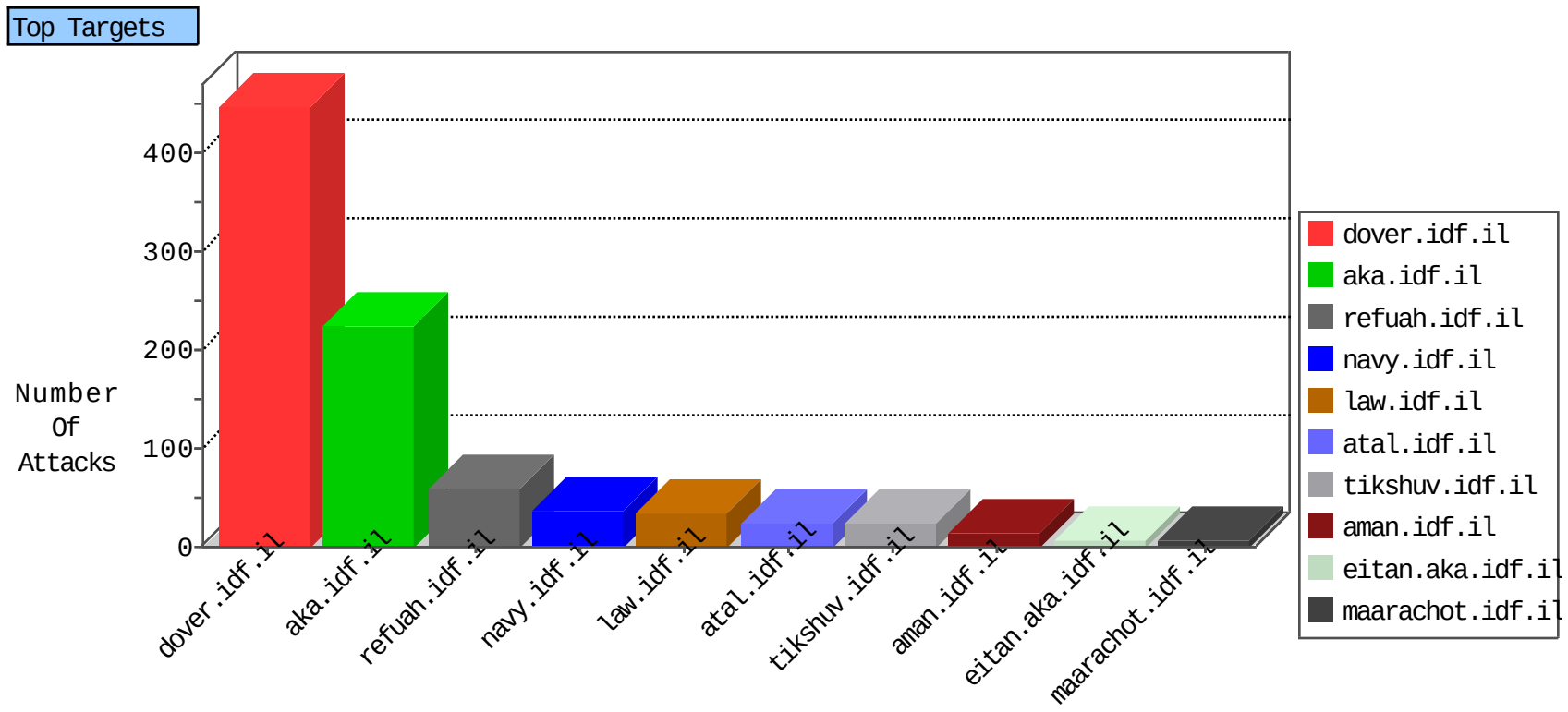
04-26-2016-01:04:08 to 04-26-2016-02:04:08

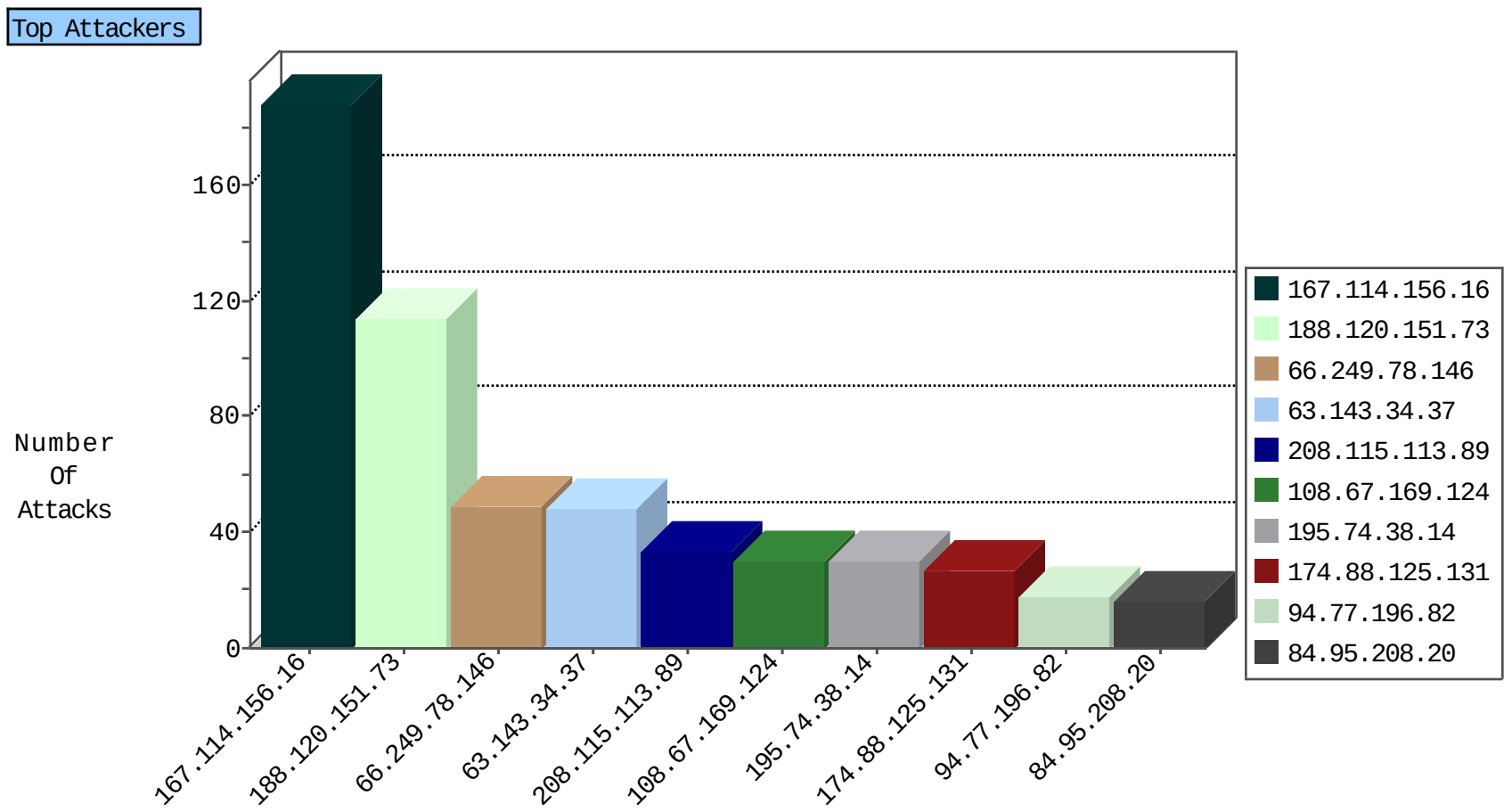
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-26-2016-01:04:08 to 04-26-2016-02:04:08

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	6661
66.249.66.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1490
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1324
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
217.112.96.194	Italy	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
45.63.20.231	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-26-2016-01:04:08 to 04-26-2016-02:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.143.34.37	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
195.74.38.14	Sweden	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
63.143.34.37	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
209.173.241.141	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.201.148.210	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.31.44.6	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
64.87.23.55	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.74.38.14	Sweden	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-26-2016-01:04:08 to 04-26-2016-02:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
63.143.34.37	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	36
195.74.38.14	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	18
108.67.169.124	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	18
216.201.148.210	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	6
64.87.23.55	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	4
99.46.81.205	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.216.176.244	147.237.77.170	Latvia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
40.76.60.52	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.237.168.43	147.237.77.216	Iraq	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
104.2.249.244	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
13.92.122.143	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
99.46.81.205	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
99.46.81.205	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
202.29.86.129	147.237.0.15	Thailand	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.179	Latvia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
40.76.60.52	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
104.2.249.244	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.122.143	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.122.143	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
99.46.81.205	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
99.46.81.205	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.205	Latvia	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-01:04:08 to 04-26-2016-02:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.120.151.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
174.88.125.131	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.234.228.90	Germany	147.237.77.233	atal.idf.il	drop	SAM rule	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
27.111.71.66	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.203.74.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
97.74.24.187	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
86.101.97.96	Hungary	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.2.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.175	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
79.181.24.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.169.130.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.184.55	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
83.130.103.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.172.120.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
148.251.176.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
174.88.125.131	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
149.202.98.161	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
174.88.125.131	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
85.130.184.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.130.184.55	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.183.176.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
174.88.125.131	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.85.73	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
174.88.125.131	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

04-26-2016-01:04:08 to 04-26-2016-02:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.97.116.135	Block	5
176.13.9.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.13.139.30	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
64.251.27.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /robots.txt	Block	1
157.55.39.126	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
84.13.139.30	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
64.251.27.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /robots.txt	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
77.125.86.125	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
180.76.15.33	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9022-he/refuah.aspx	Block	1
86.101.97.96	Hungary	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
81.223.254.34	Austria	147.237.77.233	atal.idf.il	Unauthorized URL Access to /robots.txt	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
212.76.102.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
86.188.230.218	United Kingdom	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1

04-26-2016-01:04:08 to 04-26-2016-02:04:08