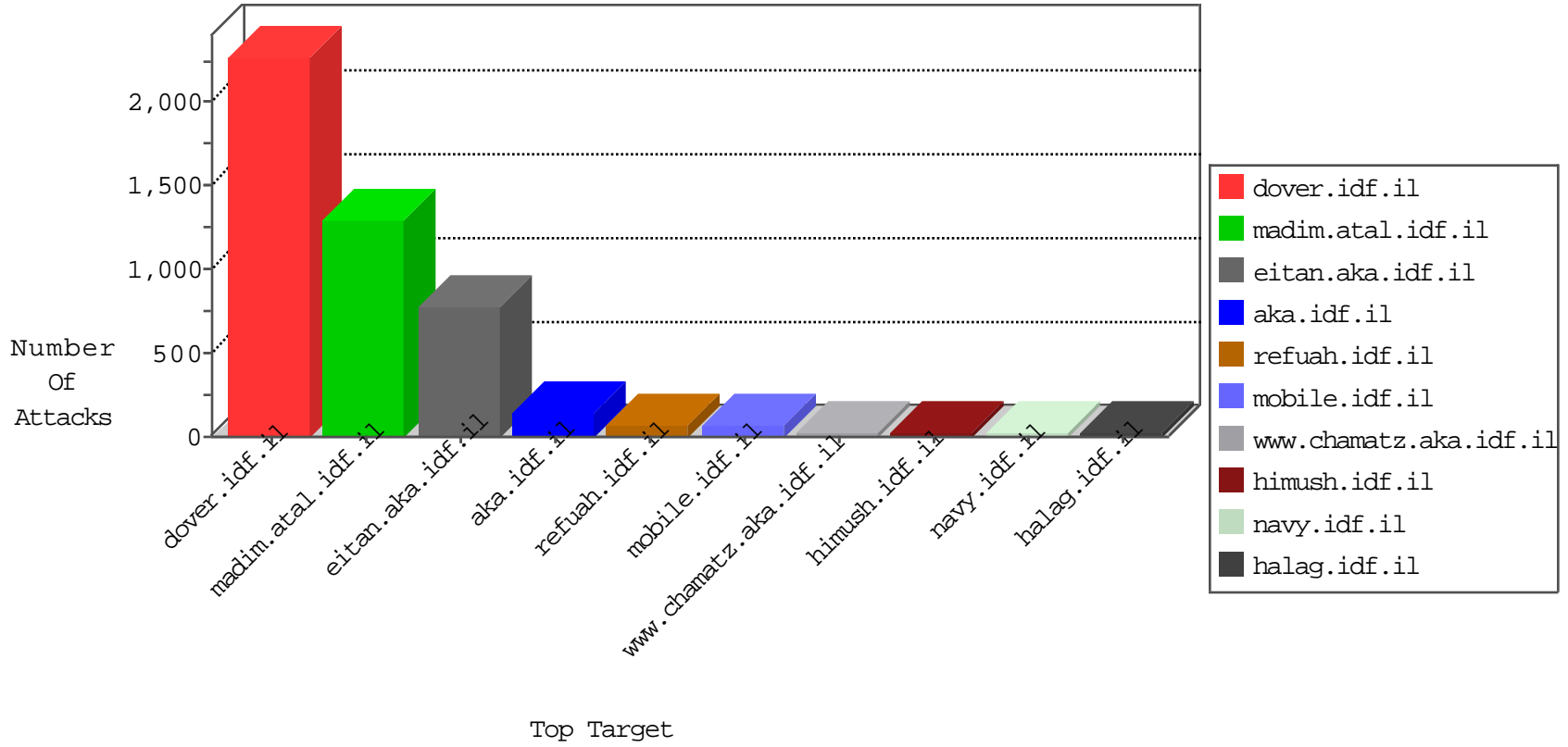


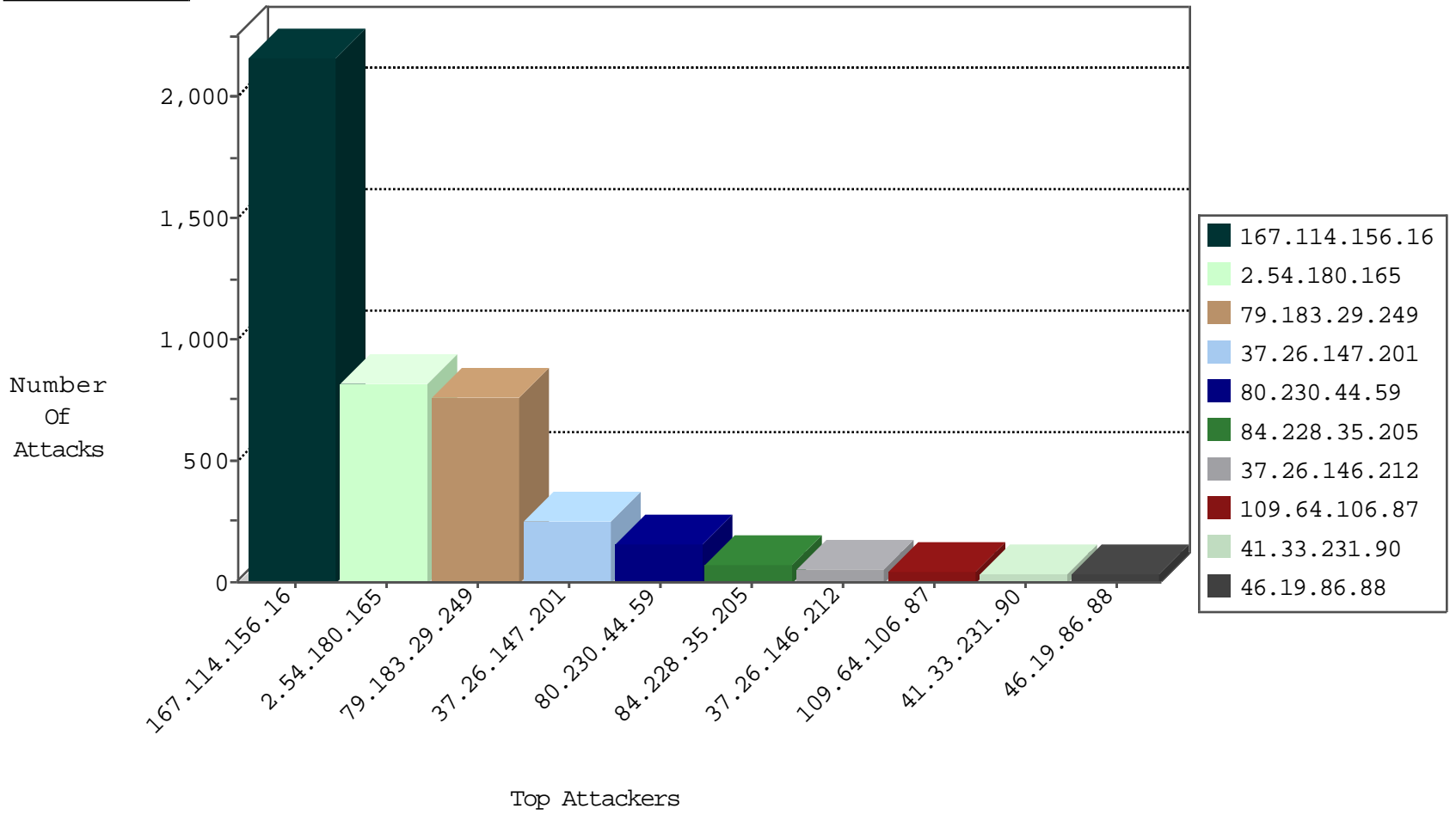
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3388
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	584
83.24.156.120	Poland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.122	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.122	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	5
37.26.147.201	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
177.126.223.156	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
177.126.223.156	147.237.76.176	Brazil	test.ncoore.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
177.126.223.156	147.237.76.86	Brazil	navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.72.166	Brazil	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.77.233	Brazil	atal.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.77.179	Brazil	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
177.1.4.155	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
177.126.223.156	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
177.126.223.156	147.237.76.148	Brazil	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.72.217	Brazil	e.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
46.151.55.35	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
177.126.223.156	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN Potential SSH Scan	1
177.126.223.156	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
177.126.223.156	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.29.249	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	654
84.228.35.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
109.64.106.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.86.83	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.121.108.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.126.171.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.126.211	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.102.9.83	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.65.109	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.83	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.143.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
76.126.183.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.43.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.130.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.191.126	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
201.246.34.220	Chile	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
188.120.148.187	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.134.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.54	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
177.64.167.150	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.181.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.39.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.126.211	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.66.193.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
117.213.16.250	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.108.158.145	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.141.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.44.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.126.211	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.181.191.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.216.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.125.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.254.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
147.235.8.69	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
212.235.34.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.65.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.4.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.120.75.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.180.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	478
2.54.180.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	230
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
2.54.180.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
80.230.44.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
79.183.29.249	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.29.249	Block	105
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
80.230.44.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	21
85.250.4.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 85.250.4.76	Block	6
80.230.44.59	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.230.44.59	Block	5
109.64.106.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.6.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.169	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
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	2
86.193.124.162	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.210.182.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
85.130.190.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.78	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
79.181.191.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.21.179	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
96.44.179.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
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	1
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.29.249	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14181-he/dover.aspx	Block	1
188.220.148.81	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
104.162.2.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.171.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
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	1
65.55.210.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot20122010.aspx	Block	1
188.220.148.81	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
107.77.76.17	United States	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	1
84.228.35.205	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
79.120.72.222	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8687-he/refuah.aspx	Block	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/tziudrefueigaza14062011.aspx	Block	1
199.30.24.32	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1