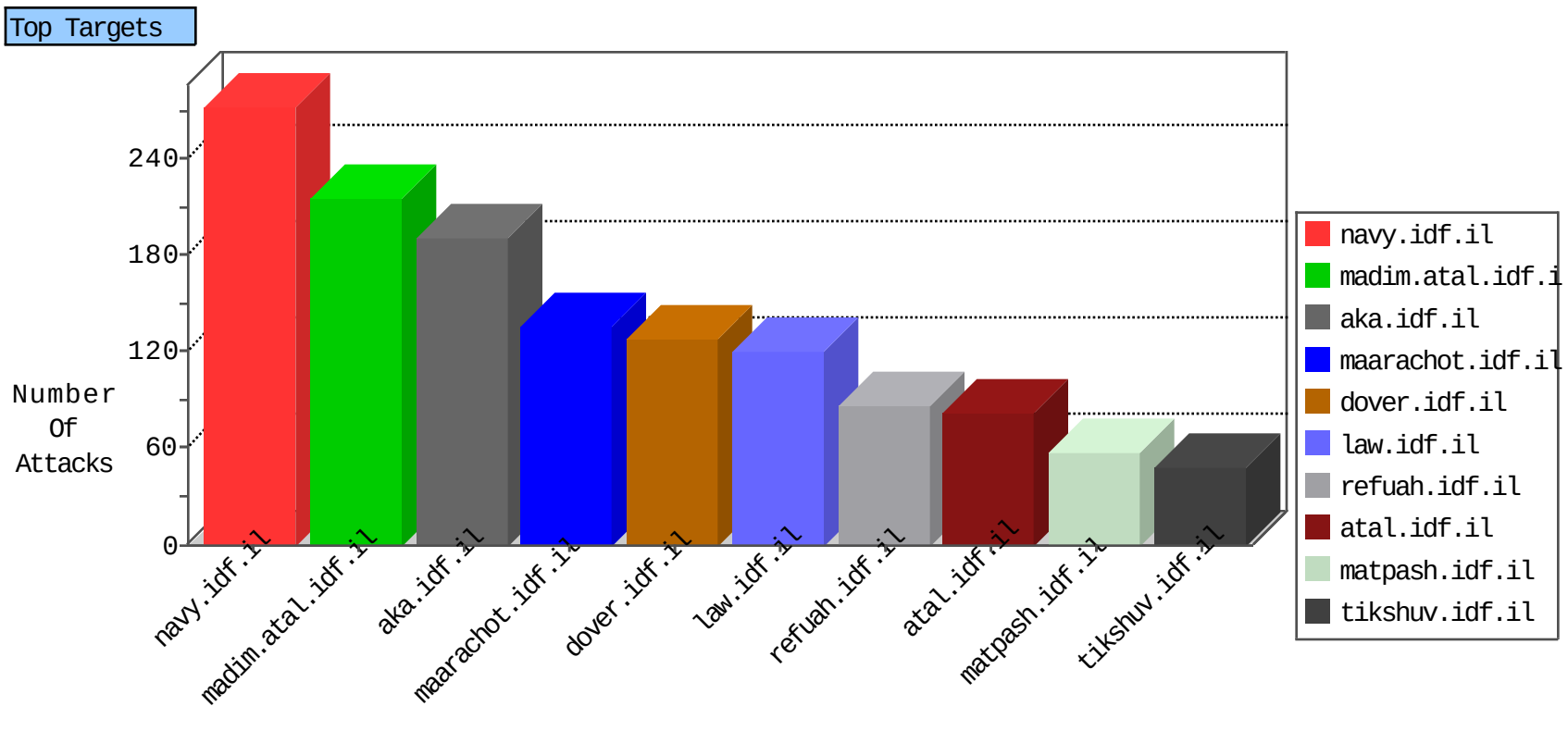
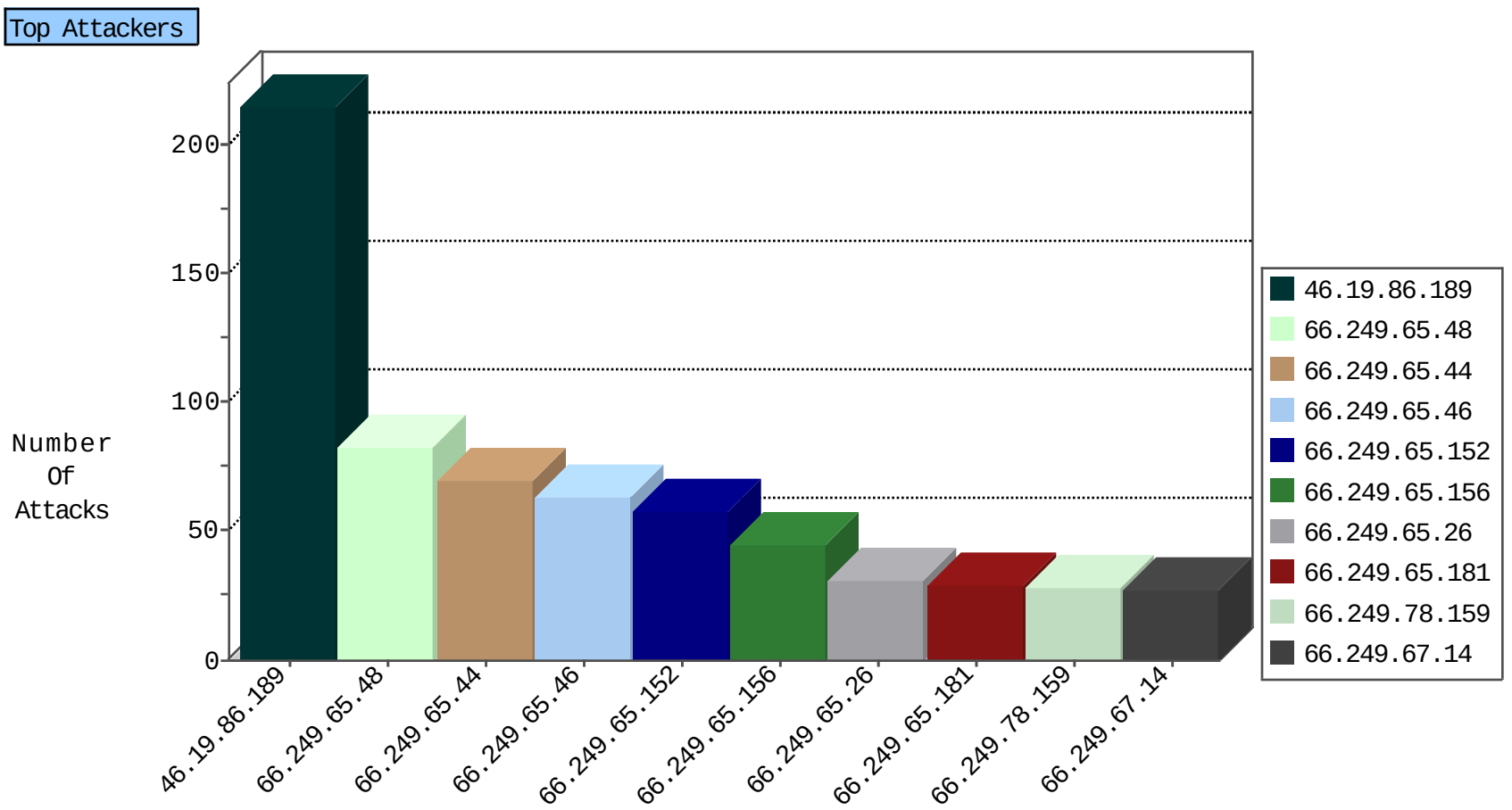
04-13-2015-18:03:04 to 04-13-2015-19:03:04

IDF Under Attack
04-13-2015-18:03:04

Top Targets



Top Attackers



04-13-2015-18:03:04 to 04-13-2015-19:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3241
84.110.60.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
87.68.9.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
66.249.65.48	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	72
66.249.65.44	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	69
66.249.65.46	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	63
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	58
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	45
66.249.65.26	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	30
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	28
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	27
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.65.30	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.65.39	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	17
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	15
66.249.65.28	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.93.172	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.65.43	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.65.3	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.65.48	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.65.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.65.1	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.65.36	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.65.41	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.65.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.65.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	7
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.73.238	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.65.50	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5

04-13-2015-18:03:04 to 04-13-2015-19:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.151.14	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
87.69.188.161	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
148.251.51.83	Germany	147.237.76.86	navy.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
31.223.189.33	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
72.10.140.218	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
80.246.140.21	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
2.54.36.167	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
14.200.122.207	Australia	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-13-2015-18:03:04 to 04-13-2015-19:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
212.199.196.143	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
182.74.92.201	India	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
182.74.92.201	India	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
182.74.92.201	India	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
84.108.15.124	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
31.210.187.143	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
5.29.134.150	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
182.74.92.201	India	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
182.74.92.201	India	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.125.223	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
84.108.119.182	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.179.27.240	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.240.115	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1

04-13-2015-18:03:04 to 04-13-2015-19:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	215
109.67.148.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
89.139.7.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	3
141.138.138.156	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
95.86.120.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
209.133.77.163	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
69.90.163.100	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
37.9.168.30	Slovakia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
5.9.152.78	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
162.144.87.219	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
79.179.183.166	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
149.78.164.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.253.141.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.52.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.116.164.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.229.33.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.120.133.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.120.133.41	Block	1
70.39.157.197	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.177.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
81.218.39.233	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1135-he/atal.aspx	Block	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
114.184.159.252	Japan	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.102.203.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
213.57.243.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.132.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/forms.aspx	None	1
188.120.133.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
70.39.157.198	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
148.251.51.83	Germany	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
82.166.221.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$ctl00$cphMain$contentMainArea$btnPrevPhase in www.aka.idf.il/homas/site/homasformphase2.aspx	None	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.90.163.100	Canada	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
132.64.37.35	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.9.168.30	Slovakia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
87.68.17.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.78	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/510-he/patzar.asph	Block	1
46.116.250.17	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
149.78.154.244	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.9.152.78	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
84.108.2.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.144.87.219	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
132.75.80.152	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	1
87.68.150.252	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/resource/userfollowresource/create/	Block	1
79.179.70.245	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1