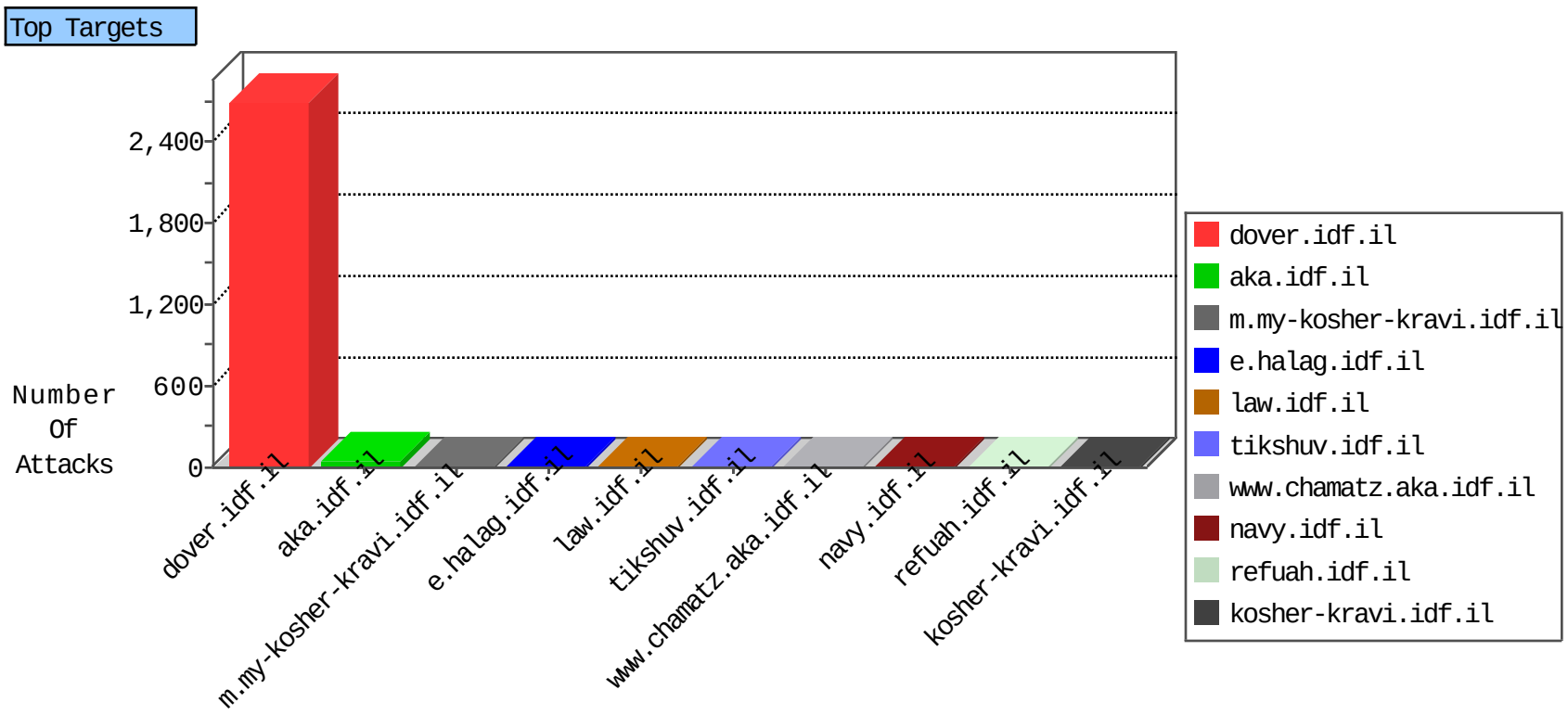
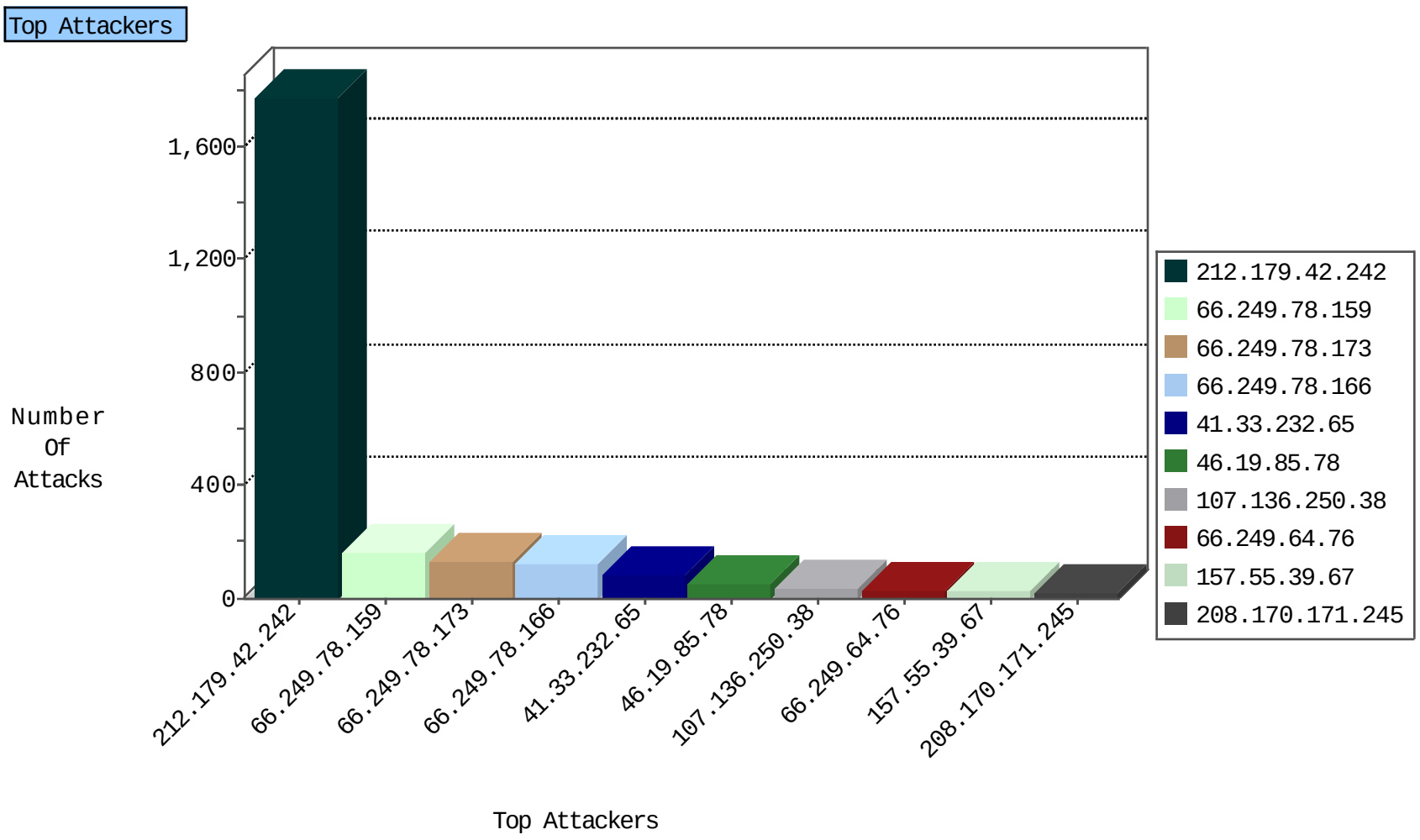
04-16-2015-03:03:02 to 04-16-2015-04:03:02

IDF Under Attack
04-16-2015-03:03:02

Top Targets



Top Attackers



04-16-2015-03:03:02 to 04-16-2015-04:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.79.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	728
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	385
66.249.79.157	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	40
110.67.63.245	Japan	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	4
66.249.79.5	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4

04-16-2015-03:03:02 to 04-16-2015-04:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.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
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
176.100.101.47	Russian Federation	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
178.43.182.190	Poland	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-16-2015-03:03:02 to 04-16-2015-04:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
84.111.234.58	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
101.226.2.99	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
91.217.90.19	Ukraine	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.231.101.67		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
103.27.236.108	Vietnam	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
101.226.2.99	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.210	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
91.217.90.19	Ukraine	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
213.158.233.62	Norway	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
103.231.101.67		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
103.231.101.67		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1

04-16-2015-03:03:02 to 04-16-2015-04:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.42.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1777
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	150
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	126
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	116
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
46.19.85.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
107.136.250.38	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
157.55.39.67	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
208.170.171.245	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
69.120.218.190	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
73.17.19.29	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
197.196.82.140	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
220.255.1.132	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
24.9.117.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
207.46.13.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.55.39.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.83.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.146	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.86.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
69.171.237.115	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
84.111.234.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
124.6.181.194	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
100.34.152.11	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.31	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
67.68.131.195	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
70.90.233.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.103	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
68.225.15.192	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
24.37.20.202	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
88.71.238.69	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.67	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-ar	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
207.46.13.78	United States	147.237.72.166	aka.idf.il	Unknown Parameter </script in www.aka.idf.il/ishurim/main/url	None	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/general.aspx	Block	1
66.249.64.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.79.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/chief of staff.stm	Block	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
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	1
66.249.79.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
213.158.233.62	Norway	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.158.233.62	Block	1
157.55.39.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/engl	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/110-he/patzar.aspx	Block	1
66.249.79.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-ar	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
194.187.168.22	Poland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
12.216.216.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
85.65.177.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.79.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8674-he/navy.aspx	Block	1
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
157.55.39.180	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.211	None	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	Block	1
62.210.69.5	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/continuation/english/index1.stm	Block	1
66.249.79.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16054-en/dover.asp	Block	1
176.100.101.47	Russian Federation	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.67.48	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 66.249.67.48	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.sviva.gov.il	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	1
64.183.55.214	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8653-he/navy.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
184.105.139.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.67.48	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/news/news.in.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteychayal	Block	1
66.249.79.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1