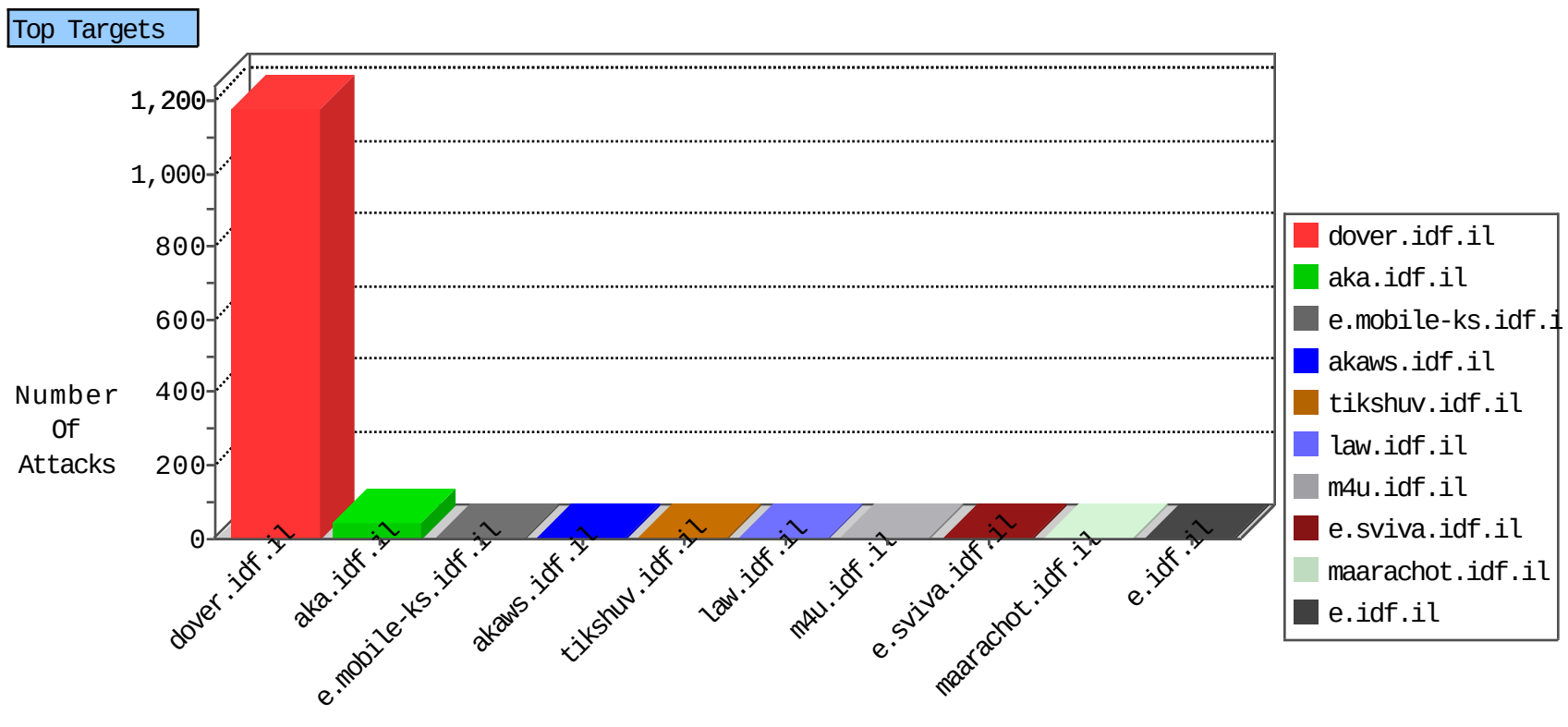
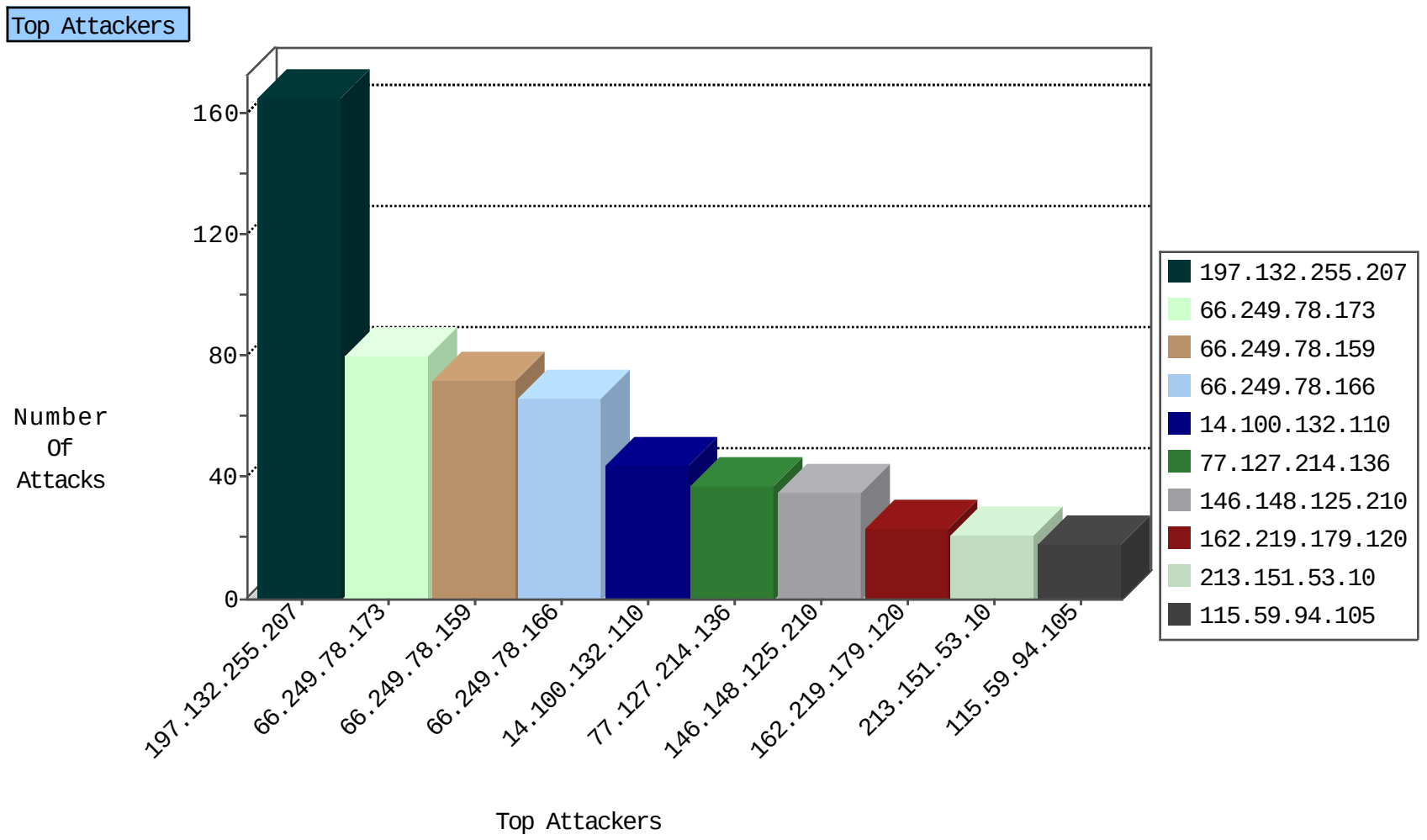
04-17-2015-02:03:04 to 04-17-2015-03:03:04

IDF Under Attack
04-17-2015-02:03:04

Top Targets



Top Attackers



04-17-2015-02:03:04 to 04-17-2015-03:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
123.30.128.71	Vietnam	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-17-2015-02:03:04 to 04-17-2015-03:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
146.148.125.210		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	31
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	2
115.59.94.105	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.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
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.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
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.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
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
202.62.121.142	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-02:03:04 to 04-17-2015-03:03:04

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	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
84.228.117.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
91.238.134.92	Poland	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
218.7.37.194	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
167.88.41.228		147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.16.232.231	India	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
111.13.30.109	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.16.232.231	India	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-17-2015-02:03:04 to 04-17-2015-03:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.132.255.207	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	156
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	62
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
14.100.132.110	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
77.127.214.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
162.219.179.120	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
213.151.53.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
107.216.251.40	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
41.251.222.202	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
64.251.59.210	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
76.218.90.230	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
45.102.24.252		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.40.162.253	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
74.71.12.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.67.157	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
84.228.117.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
157.55.39.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
115.59.94.105	China	147.237.77.216	dover.idf.i	SAM rule	drop	drop	10
104.155.59.203		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
69.171.230.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
188.120.148.214	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
173.252.79.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
69.171.230.116	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
173.252.79.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
69.171.230.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
209.133.111.211	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.85.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.64.72	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.168.198.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
69.171.230.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
173.252.79.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
202.62.121.142	Fiji	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
198.142.230.132	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
198.142.230.137	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
69.171.230.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
178.62.106.169	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.87.83.121	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
198.142.230.138	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
198.142.230.129	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

04-17-2015-02:03:04 to 04-17-2015-03:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.190.92.127	Germany	147.237.77.216	dover.idf.il	PHP Attempt	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
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
158.222.14.10		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/megurim/news/	None	1
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 93.190.92.127	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
58.22.77.143	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp/trackback/	Block	1
178.123.176.153	Belarus	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
66.249.67.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.73.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
61.135.190.70	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/webresource.axd	Block	1
178.255.215.128	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0405-1.stm	Block	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20065-he/idfgdover.aspx	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//scriptresource.axd	Block	1
188.138.17.205	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/shalishut/site/general.aspx	None	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/miluim/templates/inner.asp	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/list.aspx	None	1
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1

04-17-2015-02:03:04 to 04-17-2015-03:03:04