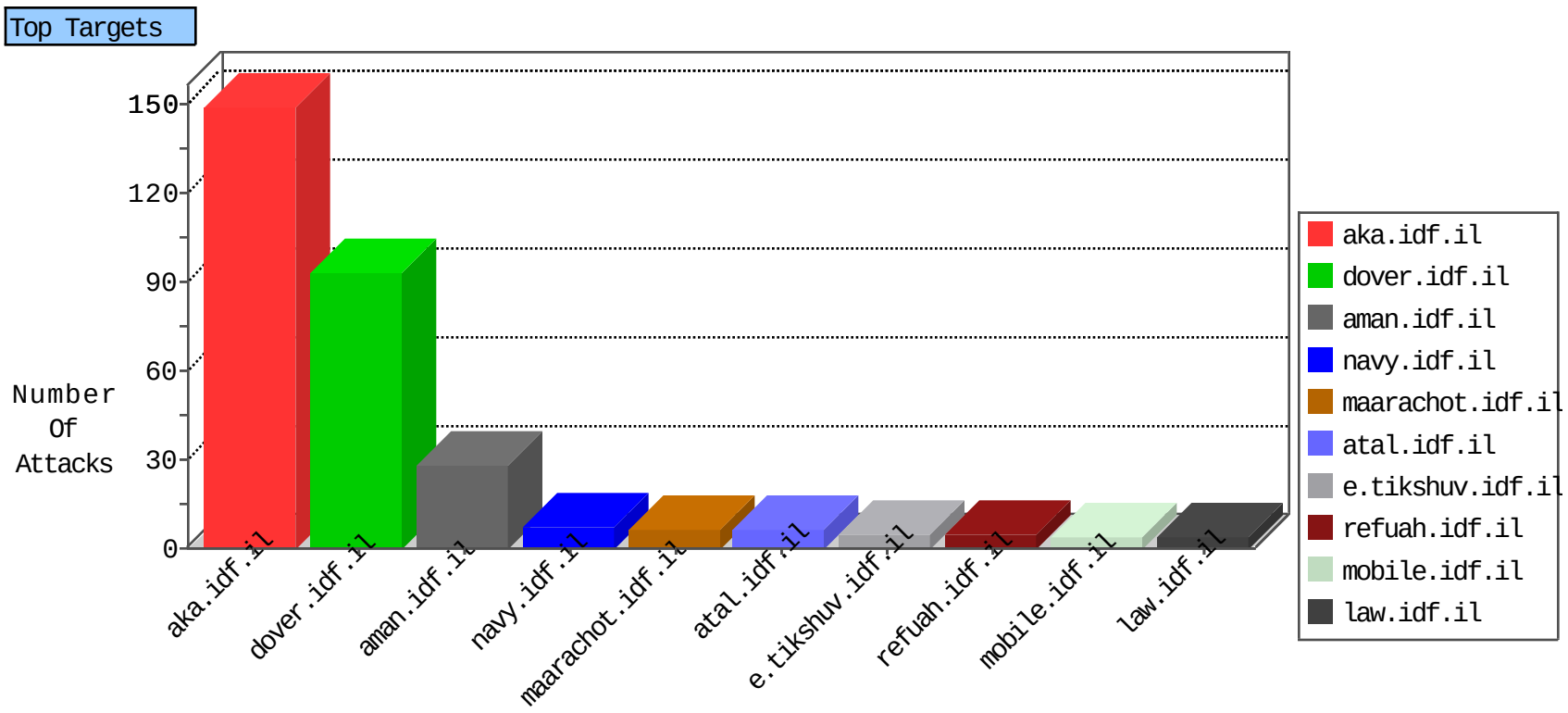
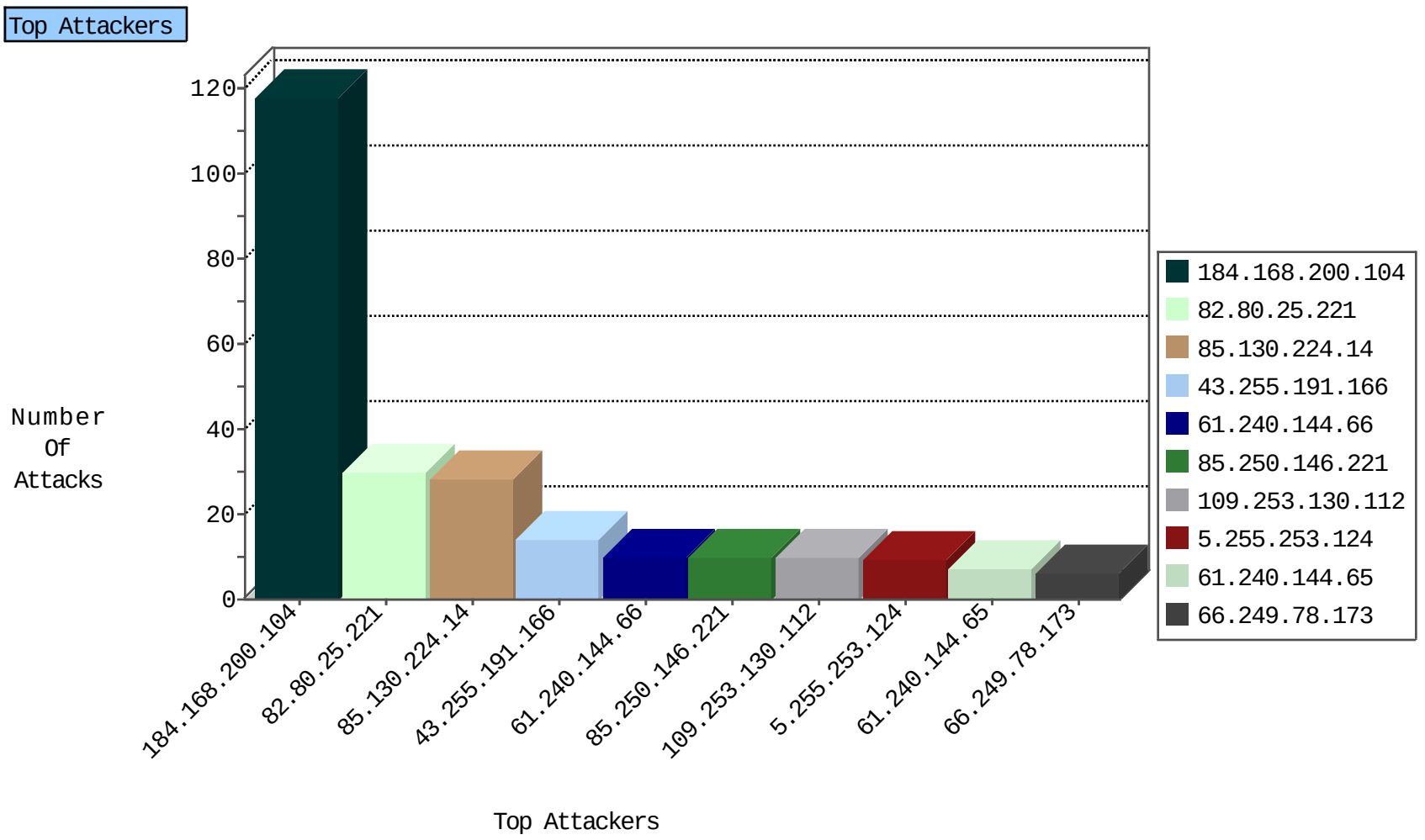
03-31-2015-05:03:05 to 03-31-2015-06:03:05

IDF Under Attack
03-31-2015-05:03:05

Top Targets



Top Attackers



03-31-2015-05:03:05 to 03-31-2015-06:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.130.224.14	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
213.163.65.66	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
84.109.240.90	Israel	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1

03-31-2015-05:03:05 to 03-31-2015-06:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
39.209.132.176	Indonesia	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	2
39.209.132.176	Indonesia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.77.121	e.navy.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
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.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
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-31-2015-05:03:05 to 03-31-2015-06:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
184.168.200.104	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
61.240.144.65	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.166	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
103.249.81.154	India	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.166	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.41.39.125	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
27.50.132.60	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.77.235	sviva.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
43.255.191.166	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.166	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.166	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
119.9.22.11	Australia	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.166	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
103.249.81.154	India	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.60	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.166	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.166	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
119.9.22.11	Australia	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

03-31-2015-05:03:05 to 03-31-2015-06:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.130.112	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
85.130.224.14	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
85.130.224.14	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
178.140.114.104	Russian Federation	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	4
46.116.162.84	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.190.137	Israel	147.237.72.166	aka.idf.il		Bad TCP sequence	monitor	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.133.15	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
80.246.133.15	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.120.54.105	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
109.253.157.15	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.130.147	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
24.13.233.255	United States	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.83	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
80.246.130.147	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.23	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
87.68.76.179	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.190.137	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.190.137	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	alert	1
74.82.47.34	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
50.198.201.34	United States	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1

03-31-2015-05:03:05 to 03-31-2015-06:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.168.200.104	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
184.168.200.104	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 184.168.200.104	Block	23
212.143.186.38	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
2.54.45.26	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
157.55.39.2	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.2	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0115-2.stm	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1506-en/dover.aspx+idf units	Block	1
84.228.245.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparIshi in aka.idf.il/main/sachar/	None	1
66.249.78.97	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
109.160.244.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/theproj/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/ general.aspx	Block	1
85.250.17.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
79.177.104.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-welcome.stm	Block	1
176.12.137.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.174.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
66.249.78.137	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.2	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/×’×ŸÂ¿Â½×ŸÂ¿Â½	Block	1
79.182.129.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
212.199.16.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wepdwukmtgwmty4mzg3mgqyaquex19db250cm9sc1jlcxvpcmvqb3n0qmfja0tlev9ffgeffmn0bdawjgn0bdawjhjiqwxsu2l0zxn6lpiyitir+hqfctxhgpc/da6cxa==/	Block	1
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
176.12.146.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.200.12.54	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2001/may/15.stm	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/poland/poland.stm	Block	1
80.246.133.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.48	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
108.250.225.28	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

03-31-2015-05:03:05 to 03-31-2015-06:03:05