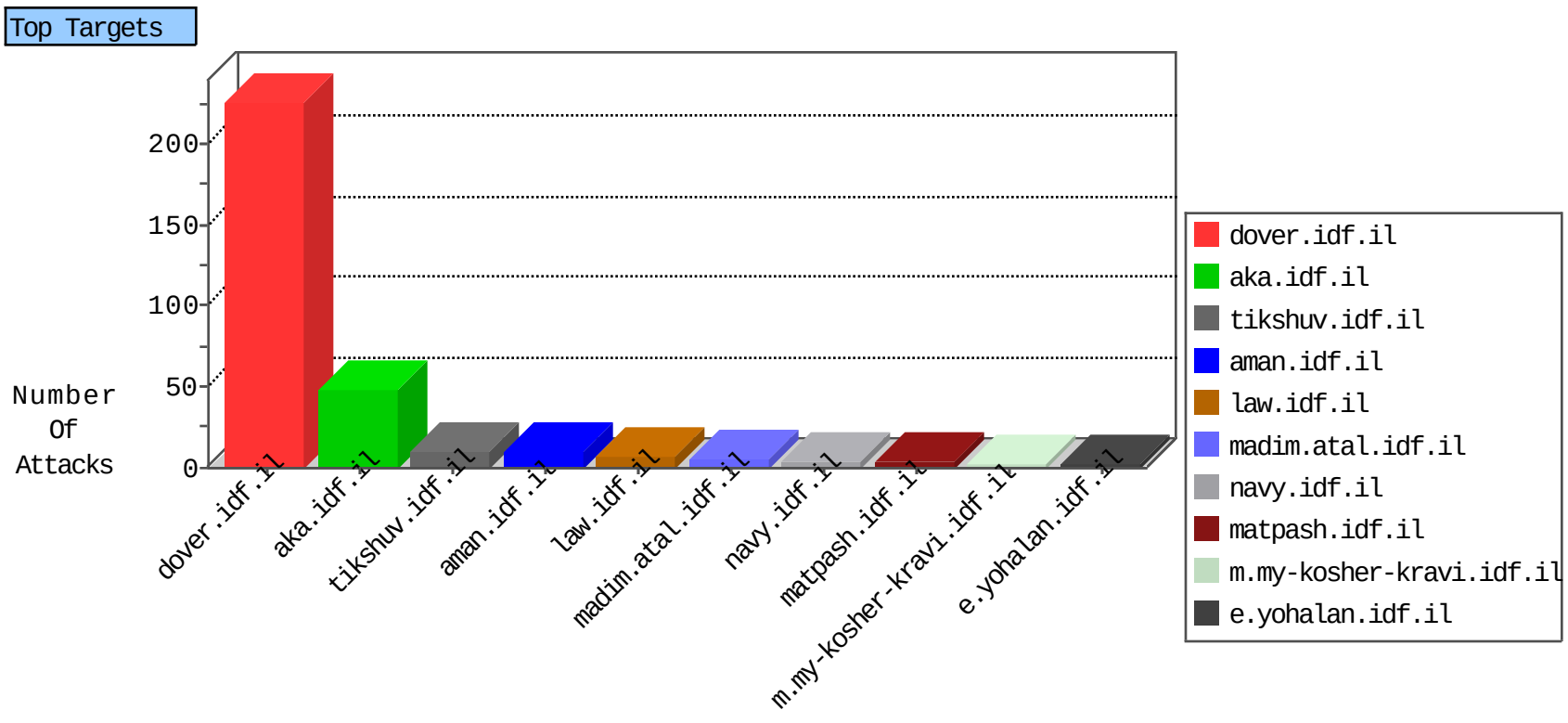
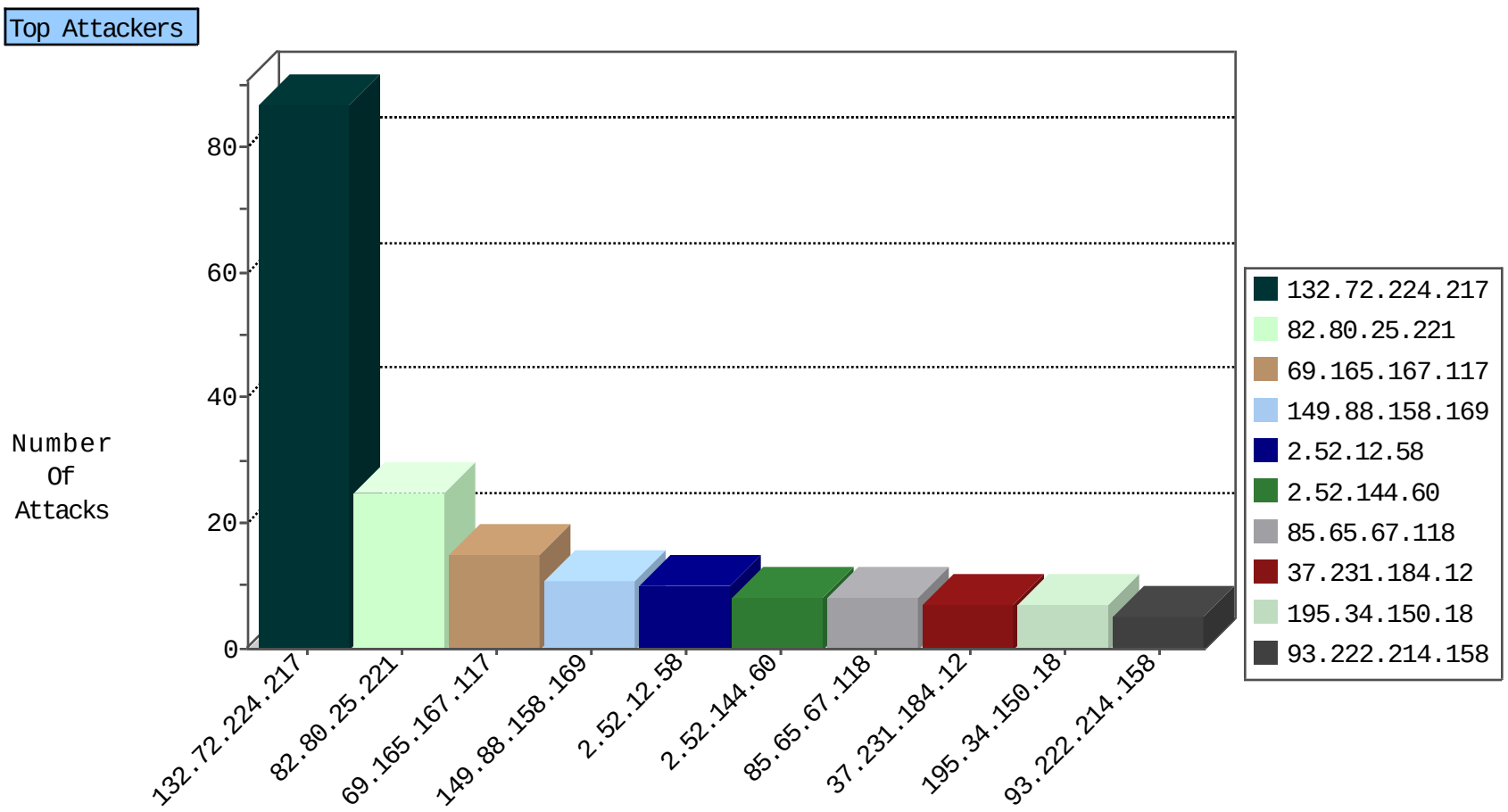
04-25-2015-13:03:04 to 04-25-2015-14:03:04

IDF Under Attack
04-25-2015-13:03:04





Top Attackers

04-25-2015-13:03:04 to 04-25-2015-14:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7346
66.249.91.142	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7298
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	6722
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6409
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6253
66.249.75.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5832
66.249.69.74	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5051
220.181.108.181	China	147.237.0.19	madim.atal.idf.il	TCP handshake violation, first packet not syn	drop	4390
207.46.13.95	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	842
84.94.68.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	795
77.127.191.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	424
109.64.232.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	249
85.65.67.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
84.109.156.112	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.231.184.12	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.223.118.220	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
79.182.145.75	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.224.21.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.210.181.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.222.214.158	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
140.139.231.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.190.38.73	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.159.128.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.179.26.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-25-2015-13:03:04 to 04-25-2015-14:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-13:03:04 to 04-25-2015-14:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
132.72.224.217	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	87
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
69.165.167.117	Canada	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
79.178.145.177	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
69.165.167.117	Canada	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
79.182.2.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
69.165.167.117	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
66.249.75.117	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
82.166.91.43	Israel	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
61.160.224.130	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
14.104.185.8	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
14.104.185.8	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
69.165.167.117	Canada	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
62.210.8.164	France	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
82.166.91.43	Israel	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.130	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
14.104.185.8	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

04-25-2015-13:03:04 to 04-25-2015-14:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.12.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
2.52.144.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.231.184.12	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.145.209.47	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.222.214.158	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.180.134.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.116.178.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.210.189.96	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.88.20.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.22.129.203	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.65.142.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
89.139.48.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.116.221.177	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
114.4.142.174	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.177.210.168	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.133.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.184	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	1
95.173.171.236	Turkey	147.237.76.198	e.yohalan.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-25-2015-13:03:04 to 04-25-2015-14:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.88.158.169	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	4
93.173.32.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	3
77.126.234.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	3
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	3
178.137.85.64	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
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
46.120.160.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.86.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.228.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.165.167.117	Canada	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/cgi-bin/php	Block	1
178.222.21.60		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
109.120.157.179	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	1
77.126.105.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
66.249.81.245	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/894-he/himush.aspx	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
84.228.169.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
69.165.167.117	Canada	147.237.0.34	tikshuv.idf.il	Access to: /cgi-bin/php	Block	1
115.31.175.92	Thailand	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
69.165.167.117	Canada	147.237.0.15	kosher-kravi.idf.il	Multiple Malformed URL from 69.165.167.117	Block	1
46.120.160.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
87.69.17.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.165.167.117	Canada	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/project1/english/index.stm	Block	1
37.19.127.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
115.31.175.92	Thailand	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
80.230.84.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.165.167.117	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/cgi-bin/php	Block	1
157.55.39.170	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
46.120.209.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
69.165.167.117	Canada	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	1
46.19.86.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
69.165.167.117	Canada	147.237.0.19	madim.atal.idf.il	Distributed Malformed URL	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-6446-he/	Block	1

04-25-2015-13:03:04 to 04-25-2015-14:03:04