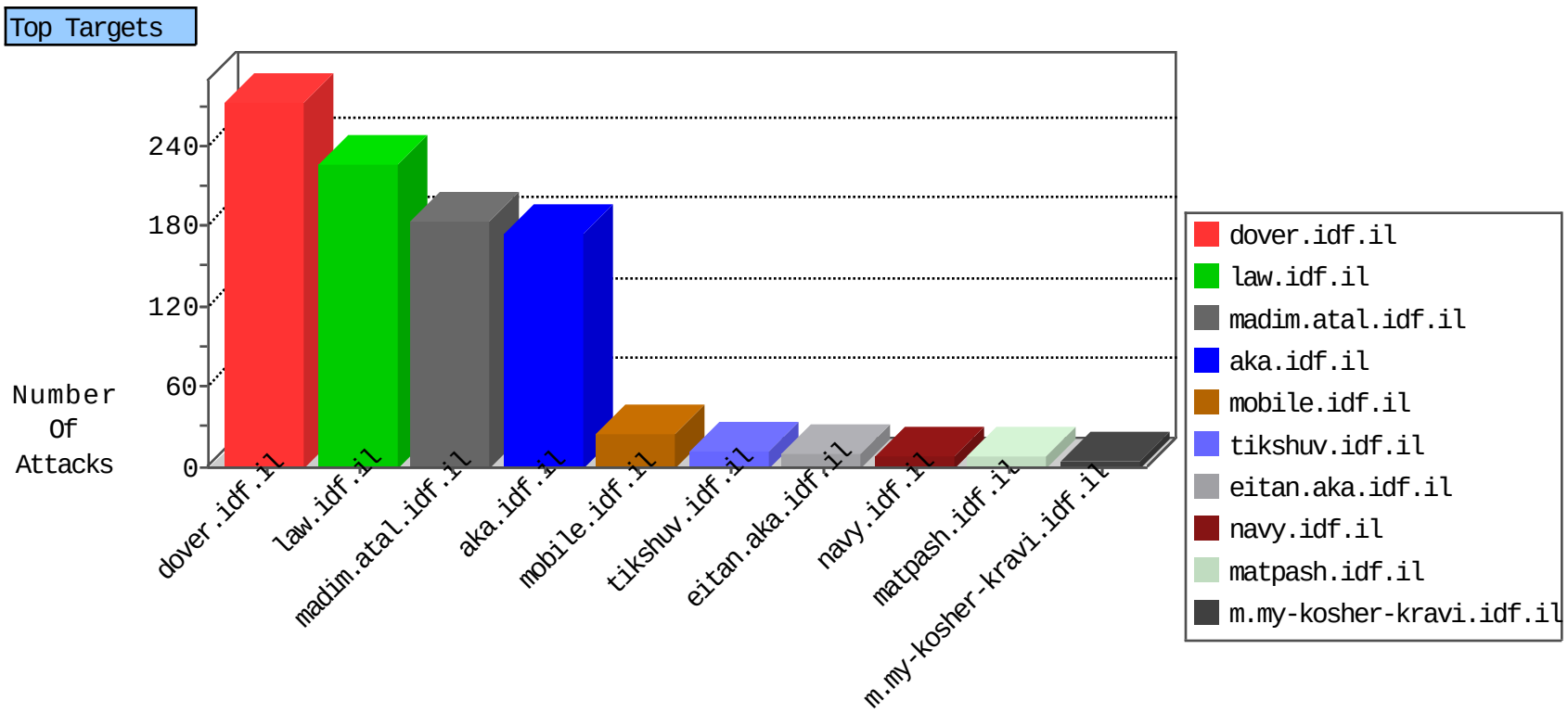
04-24-2016-01:04:11 to 04-24-2016-02:04:11

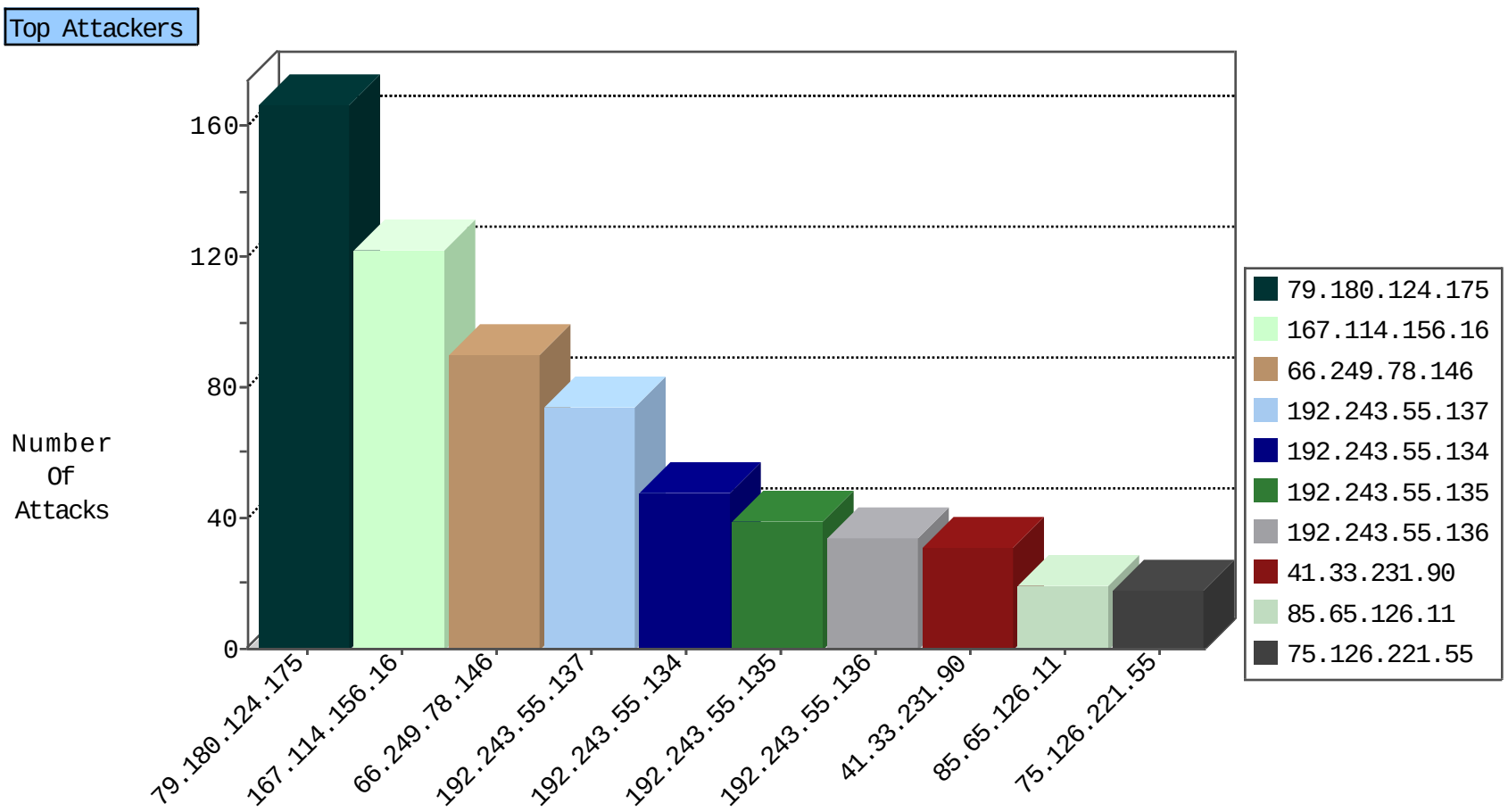
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-24-2016-01:04:11 to 04-24-2016-02:04:11

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	9713
69.30.202.229	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.197.250	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
216.176.185.42	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
173.208.197.252	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
69.30.202.230	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
5.196.199.231	France	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
69.30.202.228	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
173.208.197.252	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

04-24-2016-01:04:11 to 04-24-2016-02:04:11

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.161.9.8	Russian Federation	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1

04-24-2016-01:04:11 to 04-24-2016-02:04:11

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
58.218.204.211	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.195	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.195	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.196.199.232	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.152.155	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.59.33.61	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
113.59.33.61	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
109.72.215.18	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.195	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.139	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
113.59.33.61	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.72.215.18	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
72.13.164.90	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

04-24-2016-01:04:11 to 04-24-2016-02:04:11

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
75.126.221.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
85.65.126.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
87.70.0.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
37.237.186.59	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.183.154.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.53.180.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.32.179.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
40.77.167.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
95.86.104.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.0.116.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
37.142.208.84	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
46.19.85.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.114.146.42	Azerbaijan	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-24-2016-01:04:11 to 04-24-2016-02:04:11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.124.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
37.26.148.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.15.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.181.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.65.126.11	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.65.126.11 (Open Mode)	None	2
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
208.54.80.155	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
87.71.125.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
173.208.197.252	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
85.26.63.207	Belgium	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
95.86.66.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/departmentslobby/mobile	Block	1
69.30.202.229	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
199.30.24.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.26.63.207	Belgium	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
8.18.121.192	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/rights/asp/info.asp	None	1
150.70.173.55	Japan	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
69.30.202.230	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
66.249.66.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
50.116.28.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.65.126.11	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17748-en/dover.aspx.	Block	1

04-24-2016-01:04:11 to 04-24-2016-02:04:11