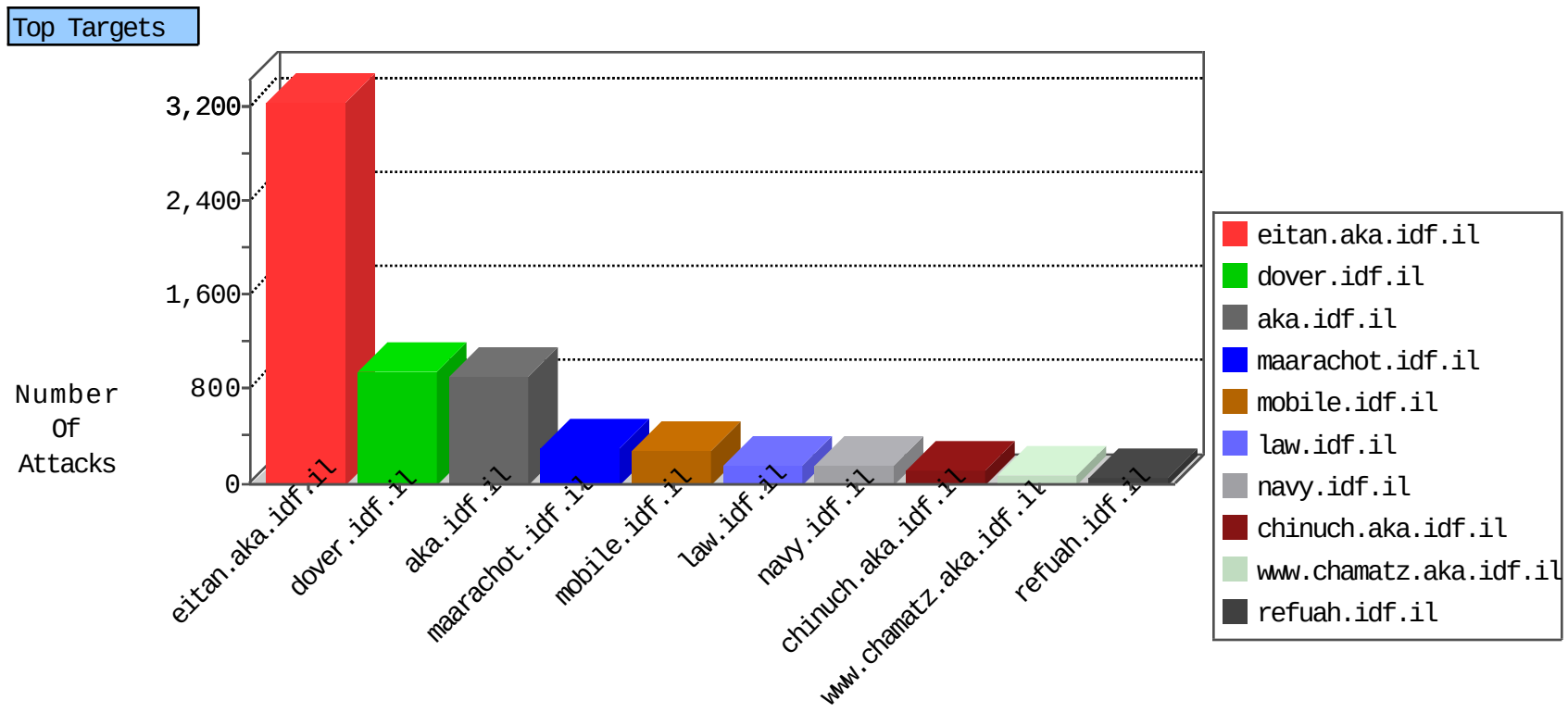
11-01-2015-02:04:04 to 11-01-2015-03:04:04

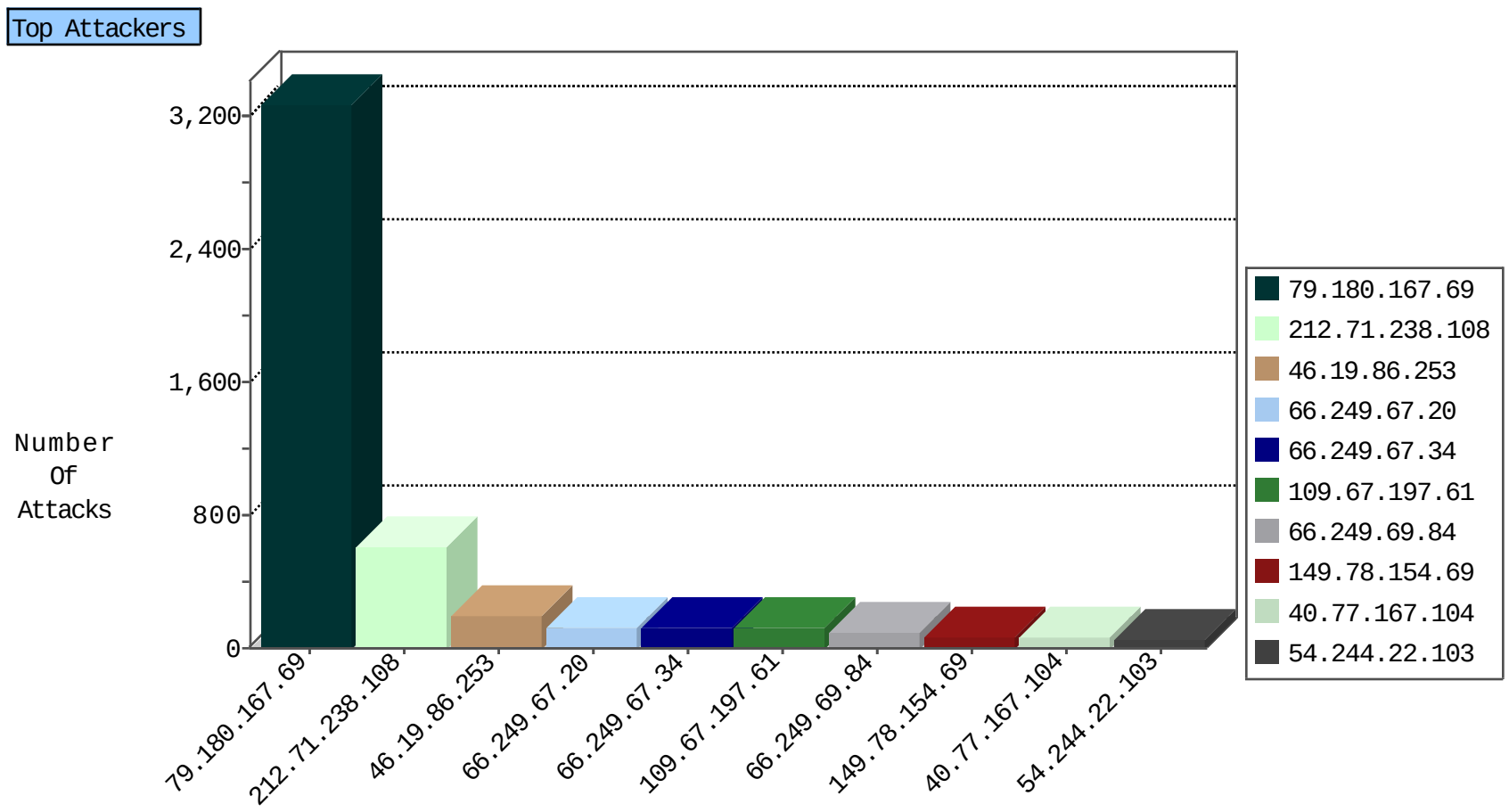
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-01-2015-02:04:04 to 11-01-2015-03:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.71.238.108	United Kingdom	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	27584
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	15210
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	14184
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6657
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4935
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4198
66.249.65.22	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4046
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3886
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3498
149.88.6.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2919
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2912
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1552
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1062
196.221.216.51	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1040
66.249.75.2	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	825
79.186.22.229	Poland	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	791
66.249.81.189	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	757
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	718
66.102.8.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	709
54.244.22.103	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	663
66.249.75.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	530
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	343
220.181.108.96	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	265
66.249.75.114	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	212
176.12.151.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	61
66.249.65.18	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	10
66.249.75.60	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	9
66.102.8.233	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
46.19.86.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
80.74.107.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.88.6.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
66.249.88.101	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
176.12.151.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.226.110.21	Switzerland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
31.168.28.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.71.238.108	United Kingdom	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
162.193.58.178	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.102.8.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.88.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.138.41.161	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.81.184	Russian Federation	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
176.13.22.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-01-2015-02:04:04 to 11-01-2015-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12

11-01-2015-02:04:04 to 11-01-2015-03:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.71.238.108	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	47
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.92	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	147.237.76.44	China	e.refuah.idf.il	GPL SCAN nmap TCP	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.151.54.209	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.215.130.20	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
212.83.155.0	147.237.0.19	France	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
177.129.252.200	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.71.238.108	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

11-01-2015-02:04:04 to 11-01-2015-03:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.167.69	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	543
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
176.12.151.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
74.90.192.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
40.77.167.33	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.18.82	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
219.74.38.178	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
131.253.25.187	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.67.13	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
131.253.25.135	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.6.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
131.253.25.162	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.137.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.10.99.206	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
203.127.96.198	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.167.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.12.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.183.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.27	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
203.127.96.244	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

11-01-2015-02:04:04 to 11-01-2015-03:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.102.8.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.167.69	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2700
46.19.86.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	165
109.67.197.61	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.67.197.61	Block	120
40.77.167.104	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	60
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	30
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112402.pdf	Block	15
66.249.64.4	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	15
183.60.243.187	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 183.60.243.187	Block	15
79.180.167.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/iturim/i	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/jquery/jquery-ui.js	Block	15
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	15
77.237.146.28	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/107835.pdf	Block	15
183.60.243.187	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/cgi-mod/header_logo.cgi	Block	15
66.249.65.26	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	15
5.28.183.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/jquery/global.js	Block	15
66.249.67.45	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
79.137.225.218	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/a2billing/customer/iridium_threed.php	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
183.245.117.200	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	15
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1923.pdf	Block	15
79.183.118.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
31.168.126.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/webresource.axd	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	15
46.19.85.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
176.10.99.206	Switzerland	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.178.222.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
207.46.13.84	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	15
85.64.206.93	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
37.26.147.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1930-he/cogat.aspx	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
176.10.99.206	Switzerland	147.237.72.166	aka.idf.il	Unknown Parameter userPass'word in www.aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	None	15
79.180.167.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.167.69	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
207.46.13.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar/	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
37.26.148.214	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	15
109.64.153.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	15
66.249.67.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10