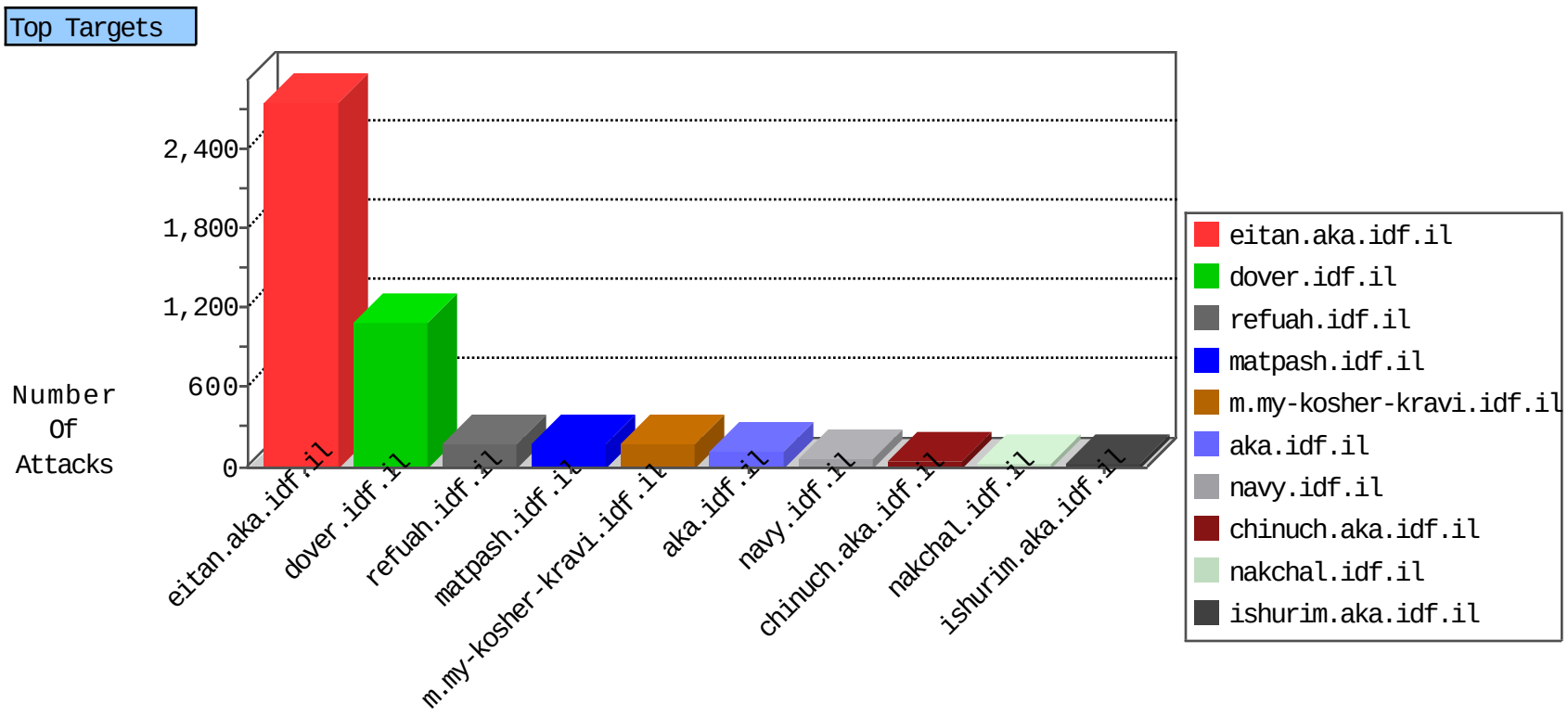
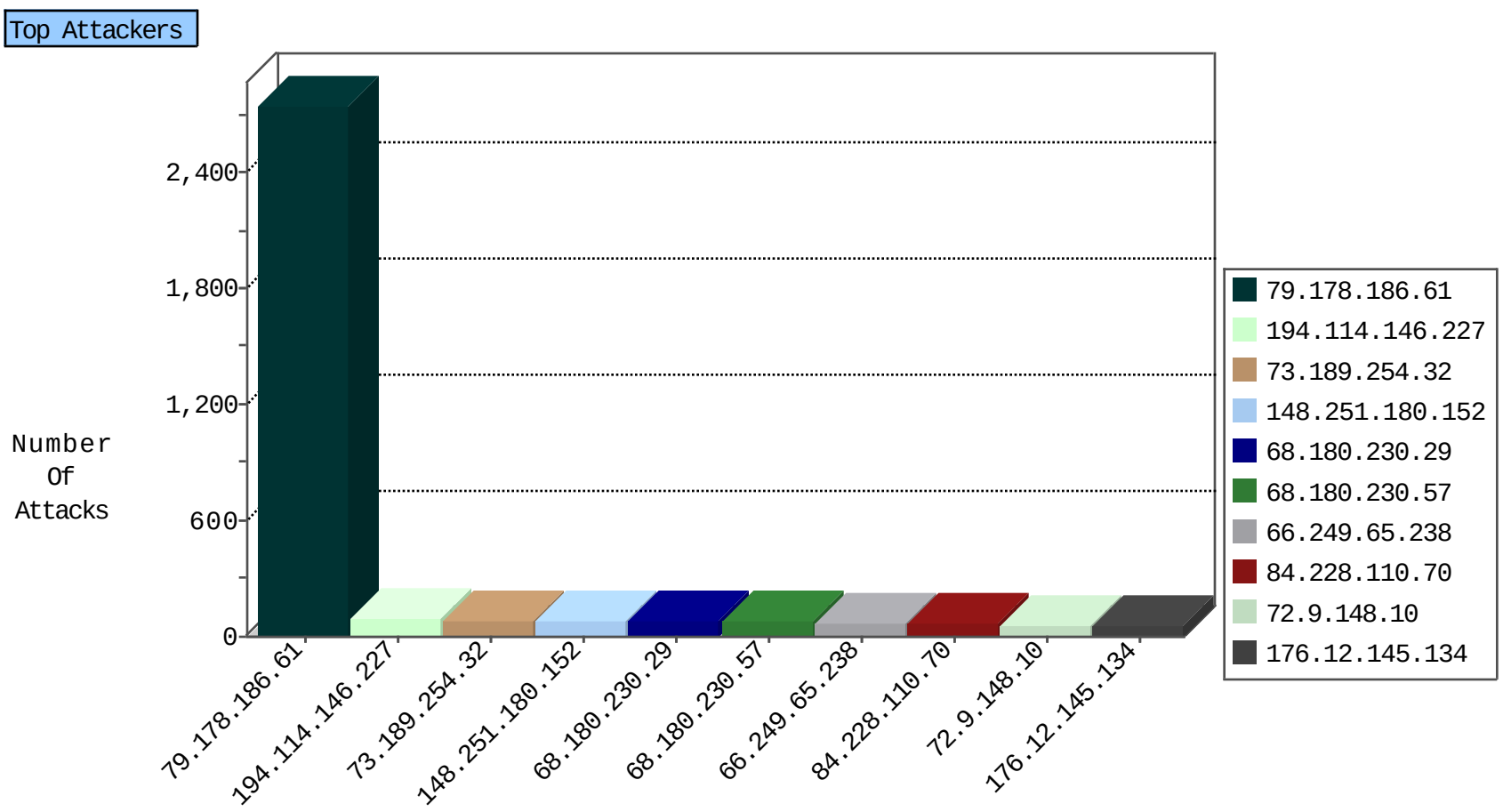
10-24-2015-08:04:08 to 10-24-2015-09:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-24-2015-08:04:08 to 10-24-2015-09:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	73
2.54.20.84	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
109.160.224.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
173.52.85.106	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
93.172.42.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
65.55.210.10	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.82.201.17		147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.94.23.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.228.110.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.41.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.60.24.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.149.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.177.102.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
83.139.146.6	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
45.32.68.116		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

10-24-2015-08:04:08 to 10-24-2015-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
171.8.55.230	China	147.237.72.156	aman.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

10-24-2015-08:04:08 to 10-24-2015-09:04:08

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	2
218.205.176.50	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
218.205.176.50	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
189.254.90.133	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
111.202.238.1	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
218.205.176.50	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.176.50	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.205.176.50	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
111.202.238.1	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
218.205.176.50	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
111.202.238.1	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1

10-24-2015-08:04:08 to 10-24-2015-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.186.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	747
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	88
73.189.254.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
37.142.147.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	48
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
84.228.110.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
31.154.147.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
89.139.50.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
5.29.203.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.7.226	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
173.52.85.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.160.224.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.123.190		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.75.172		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.94.23.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.46.39.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.55.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.200.30.154	United Kingdom	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
93.172.42.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.166.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
96.40.153.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.20.84	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
80.246.133.198	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
77.125.252.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.74.113		147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.148.30.0	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.186.61	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.186.61	Block	1988
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	84
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	84
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	56
176.12.145.134	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	56
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	56
176.12.147.59	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	42
84.228.110.70	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1153-he/dover.aspx	Block	28
148.251.180.152	Germany	147.237.77.176	matpash.idf.il	PHP Attempt	Block	28
131.253.25.249	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	28
176.13.1.193	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
157.55.39.11	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/cometous/	Block	14
81.223.254.34	Austria	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	14
176.13.3.57	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
148.251.180.152	Germany	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 148.251.180.152	Block	14
77.237.154.221	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	14
188.165.15.233	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspx-title=over	Block	14
68.148.30.0	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	14
176.13.3.57	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.3.57	None	14
148.251.180.152	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 148.251.180.152	Block	14
79.178.186.61	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
62.210.88.201	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	14
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
176.13.11.223	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.120.223.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
182.118.70.199	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/sa_swfobject.js	Block	14
148.251.180.152	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-admin/admin-ajax.php	Block	14
81.223.254.34	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to /robots.txt	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	14
148.251.180.152	Germany	147.237.77.176	matpash.idf.il	Admin Blocking	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8904-he/refuah.aspx	Block	14
54.179.134.216	Singapore	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	14

10-24-2015-08:04:08 to 10-24-2015-09:04:08