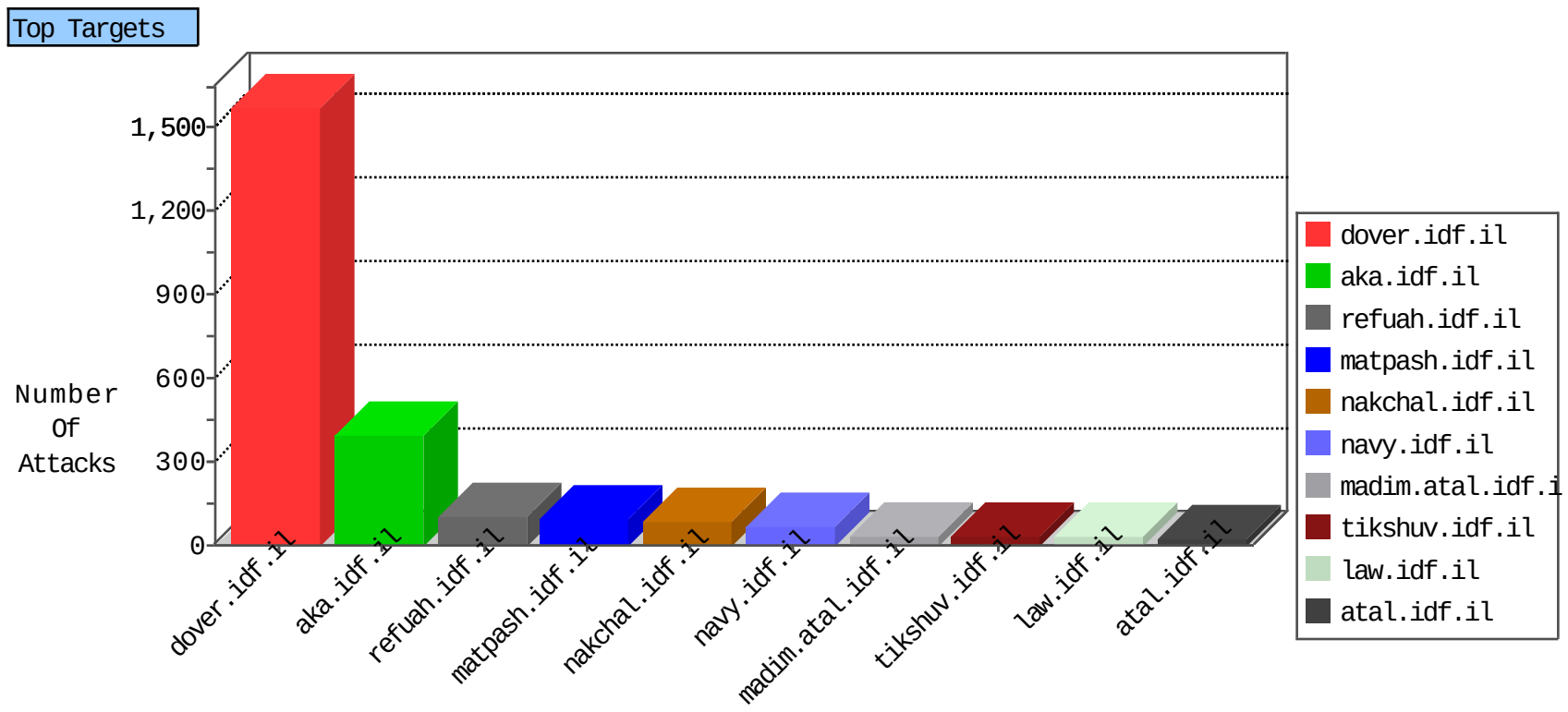
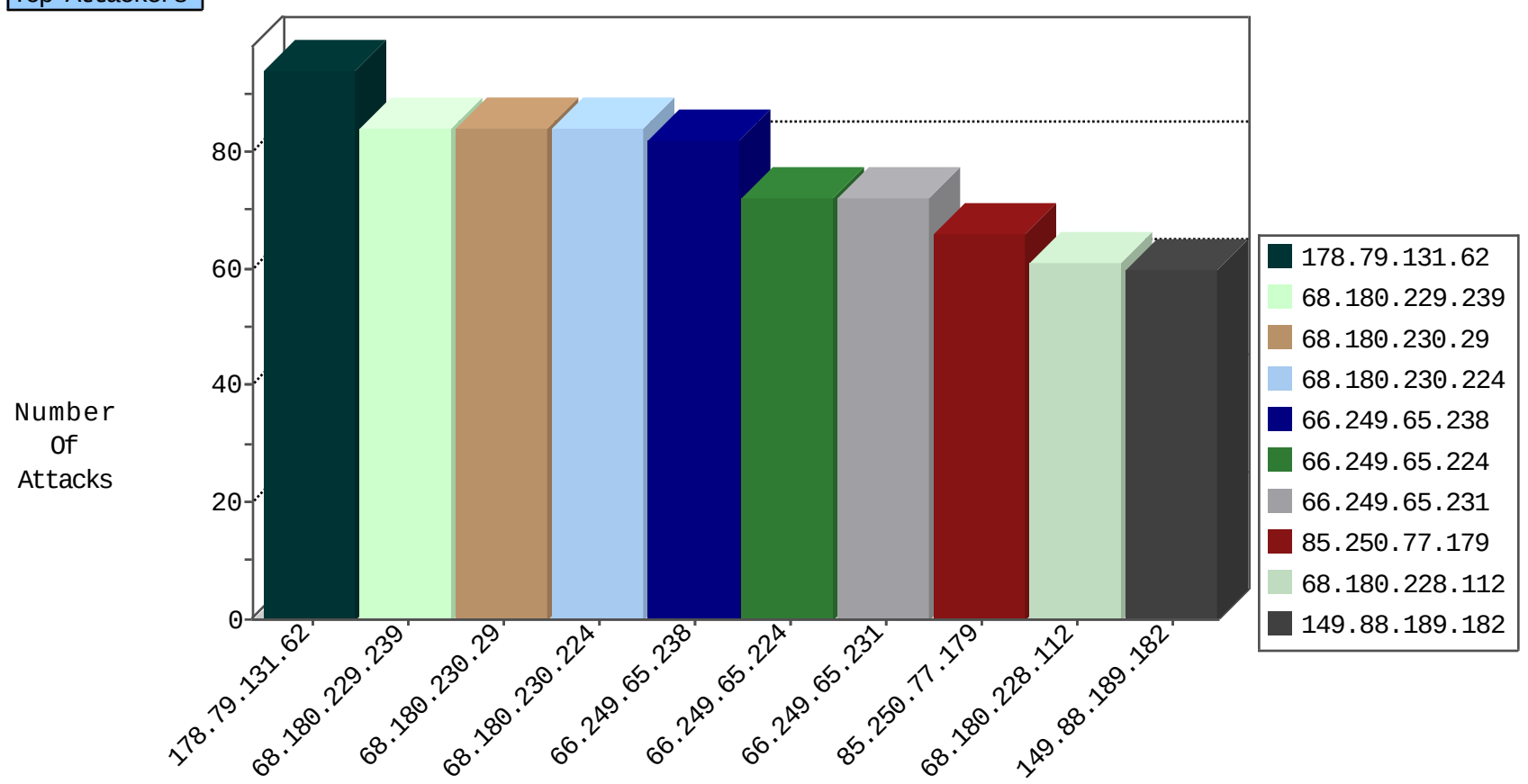
10-24-2015-10:04:04 to 10-24-2015-11:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-24-2015-10:04:04 to 10-24-2015-11:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.39.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
77.127.224.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
62.90.107.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
87.68.244.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.173.217.40	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.117.198.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.215.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.186.3.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.117.113.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.148.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.66.173.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.109.28.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.182.221.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.94.151.16	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
80.246.136.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.8.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.145.210.177	Europe	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.65.160.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.8.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-24-2015-10:04:04 to 10-24-2015-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.215.237	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-24-2015-10:04:04 to 10-24-2015-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
113.59.33.61	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.92.25.103	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.199.8.151	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.93.198.54	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
5.148.157.229	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

10-24-2015-10:04:04 to 10-24-2015-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.79.131.62	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
85.250.77.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
176.228.71.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
149.88.189.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.181.48.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.85.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.250.113.161	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
79.173.217.40	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.239.0.18	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
142.4.213.25	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.183.12.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	18
79.183.12.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.182.0.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
100.100.14.100		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.123.190		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.109.102.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.85.82		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.245.242.72	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.127.224.239	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	9
79.179.116.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.39.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.230.12.190	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	8
79.182.219.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	7
37.26.148.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
209.159.138.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.108.15		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.196	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.102.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
77.127.224.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	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
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×"×?×ª×¨	Block	84
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	84
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	84
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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	28
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	28
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8906-he/refuah.aspx	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
54.179.134.216	Singapore	147.237.72.156	aman.idf.il	Unauthorized URL Access to /	Block	14
109.67.102.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	14
79.181.99.134	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	14
178.255.215.87	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
84.94.161.105	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5484-he/patzar.aspx	Block	14
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
54.179.134.216	Singapore	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	14
141.212.122.160	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	14
79.181.208.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
182.118.70.168	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery/jquery-1.7.1.js	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	14
88.247.16.34	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
74.82.47.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	14
195.154.226.90	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.88.189.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
79.183.12.86	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
182.118.70.199	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/webresource.axd?d	Block	14
88.247.16.34	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	14
77.126.233.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl107 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
81.176.228.190	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	14
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.65.231	Block	14
54.179.134.216	Singapore	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	14
109.66.10.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
79.179.110.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	14
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
151.80.31.134	Italy	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/	Block	14
81.209.177.189	Europe	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14