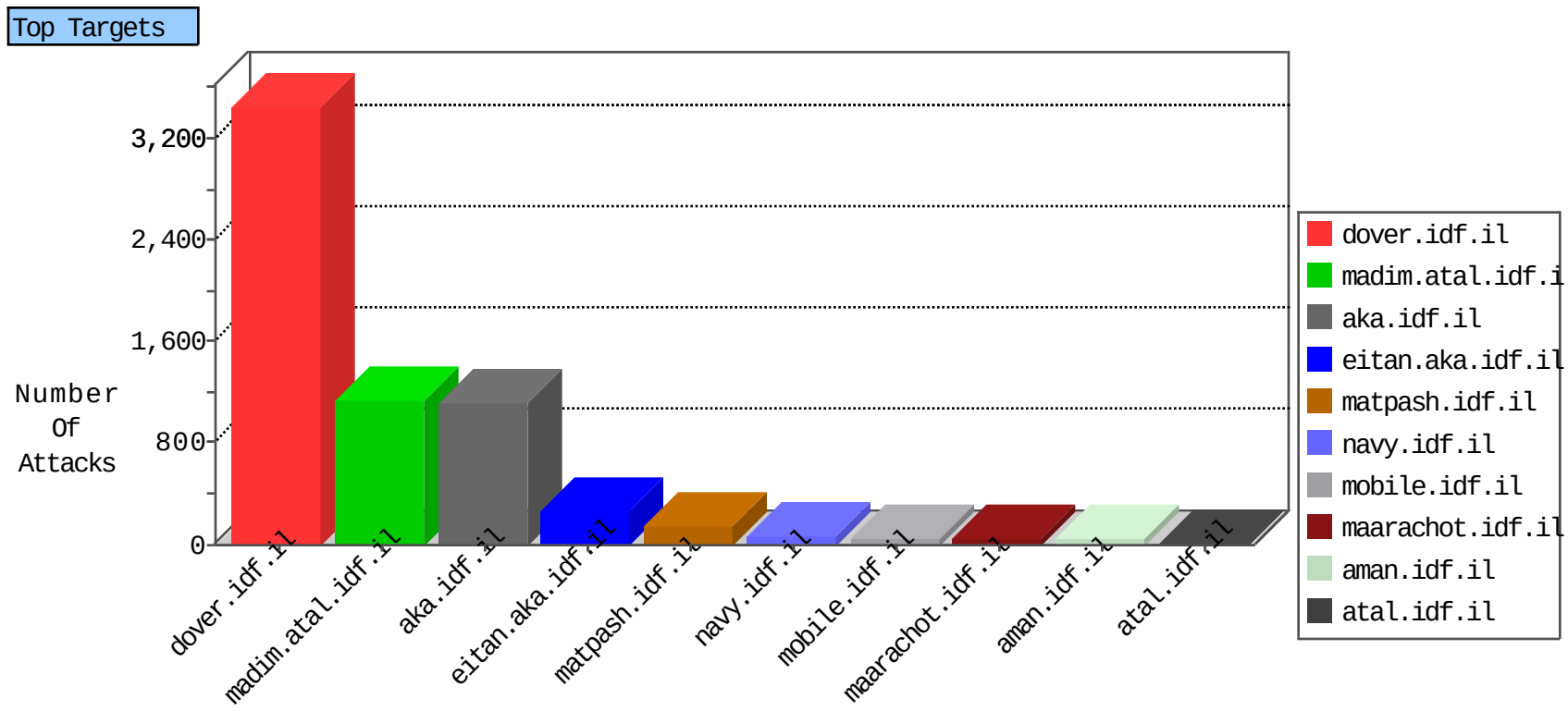
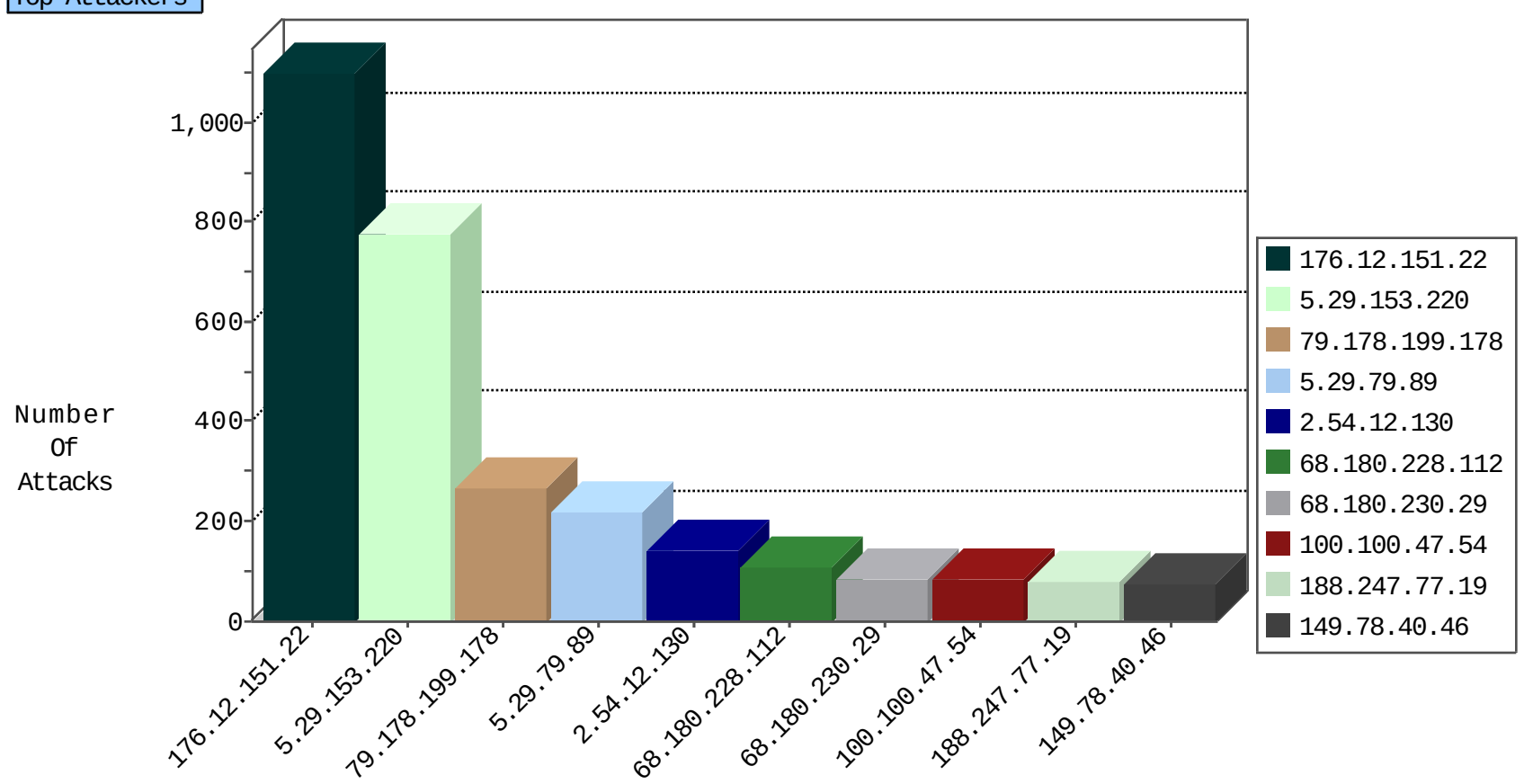
10-25-2015-23:04:06 to 10-26-2015-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-23:04:06 to 10-26-2015-00:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3582
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	151
149.88.182.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	102
82.41.239.181	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	66
79.178.17.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.19.86.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.36.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
87.69.78.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.2.247	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	19
185.32.179.185	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	13
5.29.112.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.91.194.128	Iraq	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
95.86.88.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.246.136.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.127.208.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.102.245.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
192.114.91.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.78.40.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.201.24.82	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.124.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.160.210.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.29.32.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.49.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
176.13.2.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
108.36.196.168	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.86.73.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.177.36.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.67.139.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.183.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.88.168.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.228.165.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.169.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
178.34.162.213	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	3
2.54.145.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.64.49.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.146.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.139.165.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.169.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.109.229.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.52.128.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.127.246.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.169.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.181.102.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
141.212.121.206	United States	147.237.76.39	mobile.meitav.idf.i	Block_Udp_All_Nets	drop	1
46.19.85.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-25-2015-23:04:06 to 10-26-2015-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.74.107.118	Israel	147.237.72.166	aka.idf.i	C1000004: HTTP: options method (Microsoft)	Block	2
180.250.149.158	Indonesia	147.237.77.74	law.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	2

10-25-2015-23:04:06 to 10-26-2015-00:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	60
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.87.76.23	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
41.140.253.9	147.237.0.16	Morocco	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
41.140.253.9	147.237.0.16	Morocco	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
223.4.212.53	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
186.136.89.102	147.237.76.31	Argentina	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.153.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
71.105.83.208	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
58.63.4.40	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.140.253.9	147.237.0.16	Morocco	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.212.53	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.177.185.79	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
96.90.100.123	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.148.142.253	147.237.77.216	Spain	dover.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-23:04:06 to 10-26-2015-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
2.54.12.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
188.247.77.19	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
46.19.86.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
149.78.40.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
79.180.1.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
80.178.213.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
80.246.133.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
141.0.13.124	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.66.190.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
149.88.200.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.86.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
207.228.78.15	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
100.100.47.54		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
85.65.244.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.52.49.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
89.139.29.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
162.219.230.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
93.91.194.128	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
82.41.239.181	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
45.48.113.61		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
85.168.11.224	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
108.56.149.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.10.101.28	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
149.88.182.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
108.36.196.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.47.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
5.29.112.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
95.86.88.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.64.129.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
172.56.23.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
213.165.45.2	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.11.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

10-25-2015-23:04:06 to 10-26-2015-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.151.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1101
79.178.199.178	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.199.178	Block	266
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
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	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	44
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	42
109.67.139.118	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	41
109.65.124.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	28
46.189.28.215	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
83.244.51.147	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	28
37.60.42.229	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	28
181.229.112.165	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	28
37.60.42.229	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 37.60.42.229	Block	28
91.208.99.2	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	14
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
185.32.179.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
109.186.175.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
80.74.107.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	14
2.54.5.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
173.252.120.114	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/captcha.ashx	Block	14
109.64.153.81	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
69.171.230.116	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	14
46.120.154.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
207.46.13.5	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
157.55.39.186	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
82.166.22.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	14
66.249.67.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	14
2.54.166.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
213.229.125.138	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	14
157.55.39.186	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.186	Block	14
64.19.78.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
157.55.39.186	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/×³Ö³Â¯Ö²Â¿Ö²Â½×³Ö³Â¯Ö²Â¿Ö²Â½×³Â§×³Ö³Â¯Ö²Â¿Ö²Â½×³Ö³Â¯Ö²Â¿Ö²Â½	Block	14
88.15.247.66	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
184.168.200.148	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	14
109.67.209.14	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
80.74.107.118	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.74.107.118	Block	14
66.49.225.162	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	14
157.55.39.186	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	14

10-25-2015-23:04:06 to 10-26-2015-00:04:06