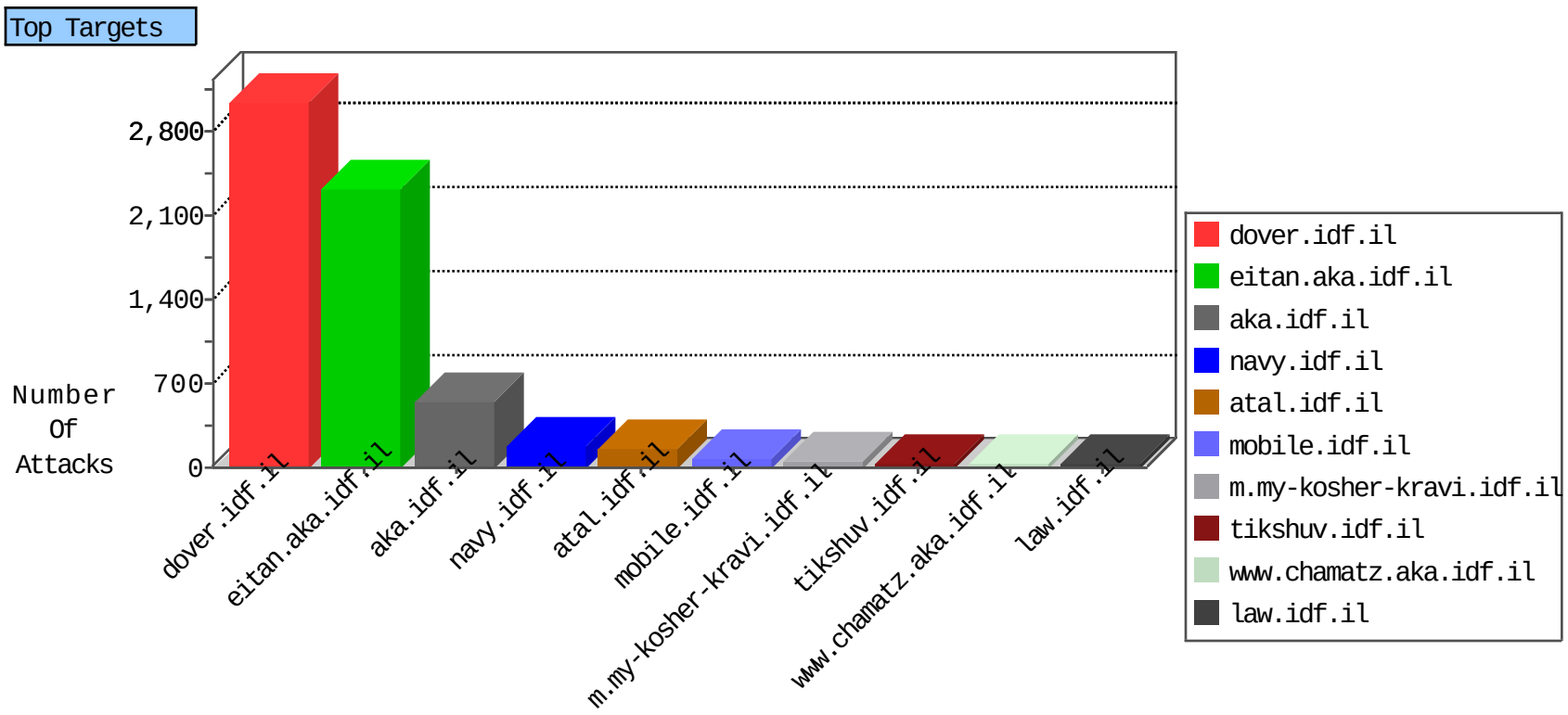
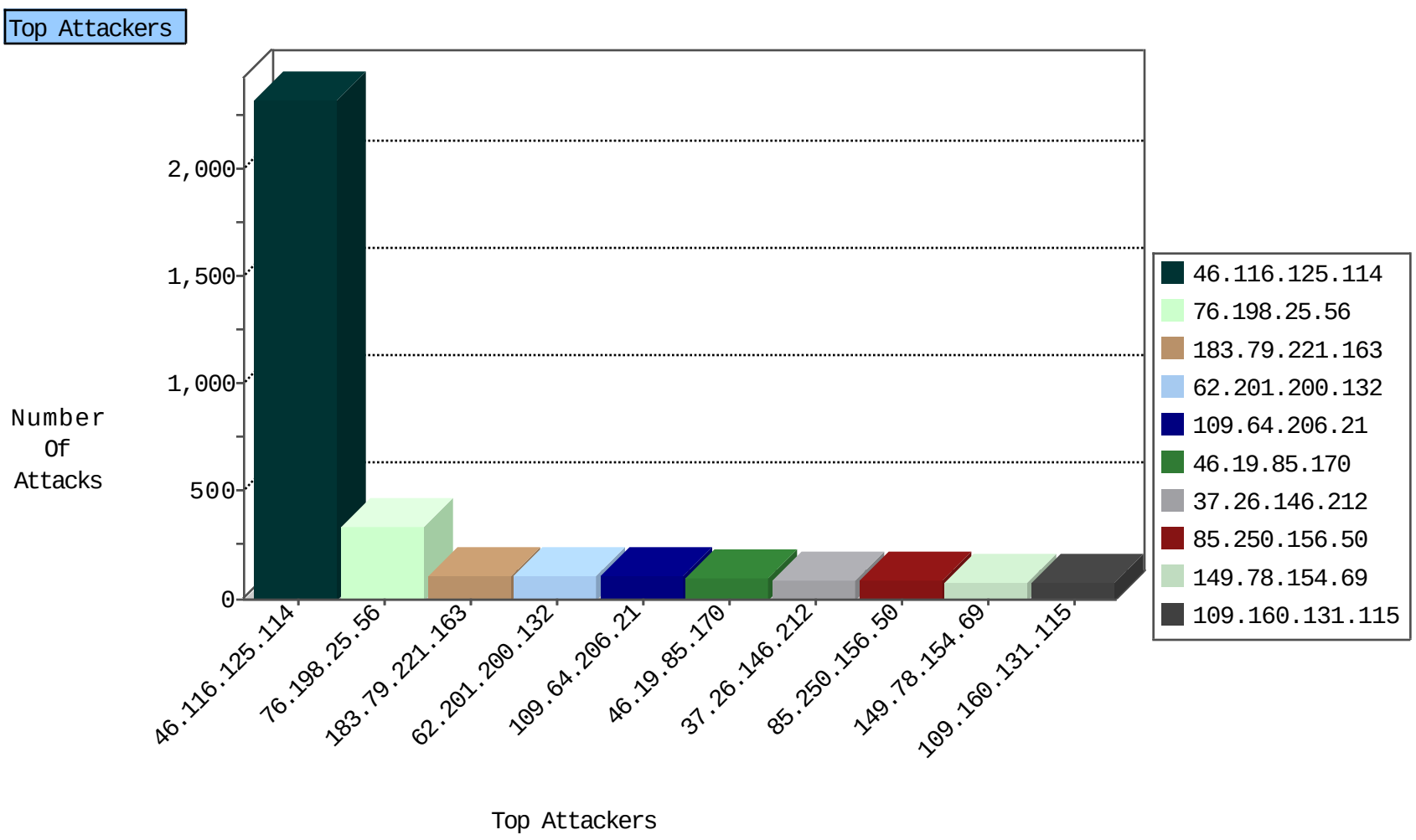
10-22-2015-23:04:00 to 10-23-2015-00:04:00

IDF Under Attack
Daily Report





10-22-2015-23:04:00 to 10-23-2015-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	38
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
109.67.29.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.54.53.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
79.177.134.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
80.246.136.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
213.151.51.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.49.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.142.105.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.26.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.136.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
89.138.209.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.154.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
213.57.60.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
80.246.136.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.145.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
173.71.48.158	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.149.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.136.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
76.216.154.170	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.154.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.64.184.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.64.184.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.54.145.205	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.66.24.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.64.184.47	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
37.142.116.214	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

10-22-2015-23:04:00 to 10-23-2015-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-22-2015-23:04:00 to 10-23-2015-00:04:00

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	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.173	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
95.86.122.250	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN NMAP -f -sS	1
188.68.224.151	147.237.77.205	Poland	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
82.192.68.46	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
209.41.67.92	147.237.8.50	United States	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
188.68.224.151	147.237.77.205	Poland	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

10-22-2015-23:04:00 to 10-23-2015-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.201.200.132	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
109.64.206.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
37.26.146.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
85.250.156.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
109.160.131.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
76.216.154.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
46.121.30.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
37.202.79.32	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
46.19.86.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
2.54.187.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.1.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
100.100.44.17		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
99.224.238.30	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
37.26.149.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
109.75.78.5	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.120.171.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
100.100.4.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
46.185.198.27	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
183.79.221.163	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
76.198.25.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
173.71.48.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
80.246.130.92	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.102.254.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.121.211.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
87.69.82.108	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
67.68.241.150	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
213.89.8.161	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.12.137.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.171	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.125.114	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2324
76.198.25.56	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 76.198.25.56	Block	294
183.79.221.163	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	70
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
176.12.140.74	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	42
82.118.24.206	Sweden	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 82.118.24.206	Block	42
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main0926.html	Block	14
178.62.222.234	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Multiple Illegal HTTP Version from 46.19.85.170	Block	14
95.35.193.35	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.35.193.35	Block	14
82.118.24.206	Sweden	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-admin/	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17754	Block	14
192.114.91.233	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
141.212.122.96	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	14
46.120.129.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
93.172.171.237	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
31.154.155.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
207.46.13.171	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	14
76.198.25.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/6_s3_	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Multiple Malformed URL from 46.19.85.170	Block	14
95.35.193.35	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	14
84.110.145.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	14
206.144.84.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=zwasxt9kp6jr1aucpufzqzwzcjy-	Block	14
157.55.39.194	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	14
66.102.9.13	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
93.172.171.237	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 93.172.171.237	None	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	14
213.57.211.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
77.126.232.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
188.120.148.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.170	Block	14
95.35.193.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/admin.php	Block	14
85.64.90.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.199	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
95.35.193.35	Israel	147.237.77.233	atal.idf.il	Admin Blocking	Block	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version deflate, sdch	Block	14
82.118.24.204	Sweden	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp/wp-admin/	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method : in URL gzip,	Block	14
95.175.35.73	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper	Block	14
87.68.241.23	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	14

10-22-2015-23:04:00 to 10-23-2015-00:04:00