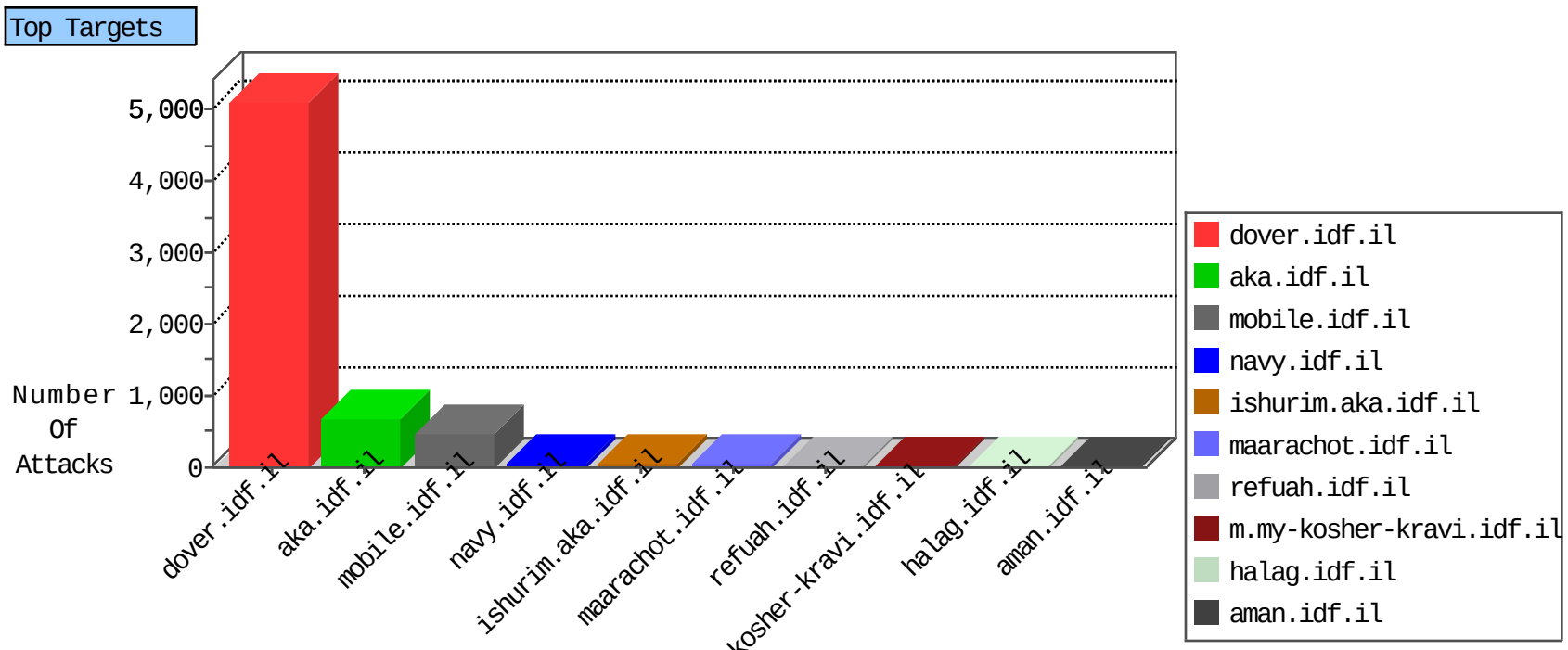
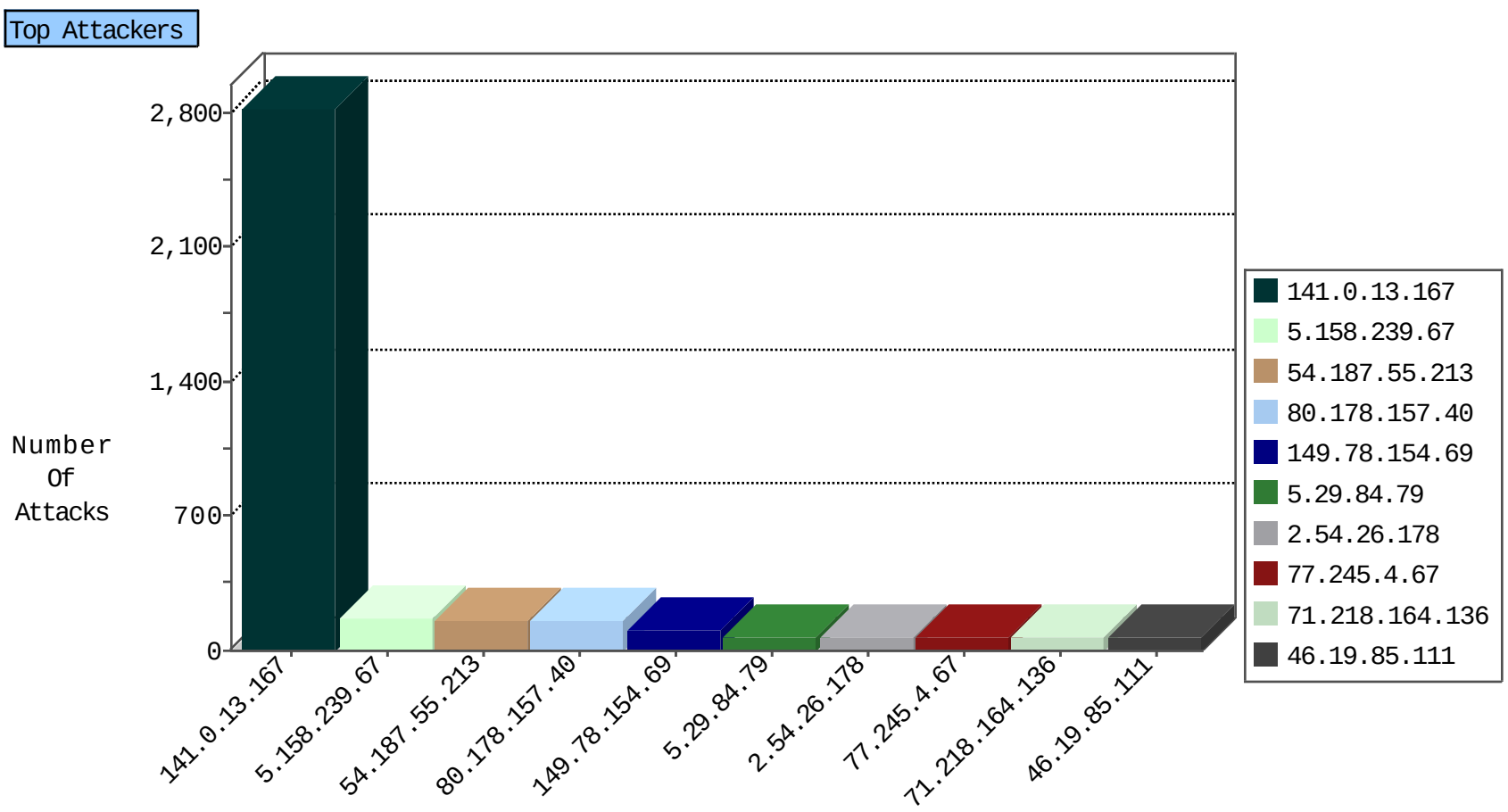
11-01-2015-07:04:04 to 11-01-2015-08:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-01-2015-07:04:04 to 11-01-2015-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.0.13.167	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8381
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3890
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	328
220.181.108.113	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	310
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	136
176.12.140.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	44
185.32.179.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
79.183.16.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
46.19.86.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.52.163.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
79.178.104.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.2.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
37.26.147.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.85.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.67.32.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
5.29.84.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
89.138.84.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.46.39.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
76.173.132.231	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.162.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
37.26.149.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.19.85.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.8.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.174.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.136.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
76.173.132.231	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.12.142.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.148.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.33.112.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.13.13.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.2.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
5.22.130.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.13.17.184	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
165.72.200.11	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.14.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.145.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.148.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.139.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.52.39.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-01-2015-07:04:04 to 11-01-2015-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-01-2015-07:04:04 to 11-01-2015-08:04:04

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	4
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
2.54.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
46.19.86.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.204.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.7.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.46.13.32	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
188.165.15.241	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.252.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
36.72.195.123	147.237.76.44	Indonesia	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.58.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.226.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-01-2015-07:04:04 to 11-01-2015-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.13.167	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2767
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
77.245.4.67	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
71.218.164.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
5.29.84.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
76.173.132.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
46.121.18.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.181.17.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
80.178.204.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.186.35.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	30
81.218.196.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.52.163.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.54.26.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
93.173.183.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.102.169.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
139.162.206.220	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.42.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.139.102	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.183.16.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.32.179.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
87.69.94.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
40.77.167.71	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
176.12.136.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.52.39.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	14
204.237.0.104	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.192.68.46	Netherlands	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	12
131.253.25.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.195.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.69.55.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.2.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	150
5.158.239.67	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	90
5.158.239.67	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.158.239.67	Block	75
176.13.17.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
2.54.26.178	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	45
2.54.131.3	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	30
80.246.130.184	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
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
176.13.17.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
2.54.41.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	30
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/chamatz/search/searchresults.asp	None	15
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	15
176.12.142.176	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation DocumentNumber in mobile.idf.il/sachar/login	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	15
176.13.12.105	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.12.105	None	15
109.67.32.222	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
185.32.179.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	15
176.12.151.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
2.54.185.28	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
87.68.77.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×’×™××•×¡	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	15
176.13.14.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
31.168.151.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	15
2.52.130.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	15
113.102.135.55	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	15
77.125.73.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
66.249.67.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
212.150.174.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
176.13.5.205	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
2.54.185.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
89.138.64.94	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109916.pdf	Block	15
46.120.156.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
77.127.245.79	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 105 cookies	Block	15
176.13.7.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
2.54.185.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
89.139.21.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	15
157.55.39.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	15
217.132.52.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
176.13.12.105	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	15
109.67.32.222	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteykatava/	Block	15