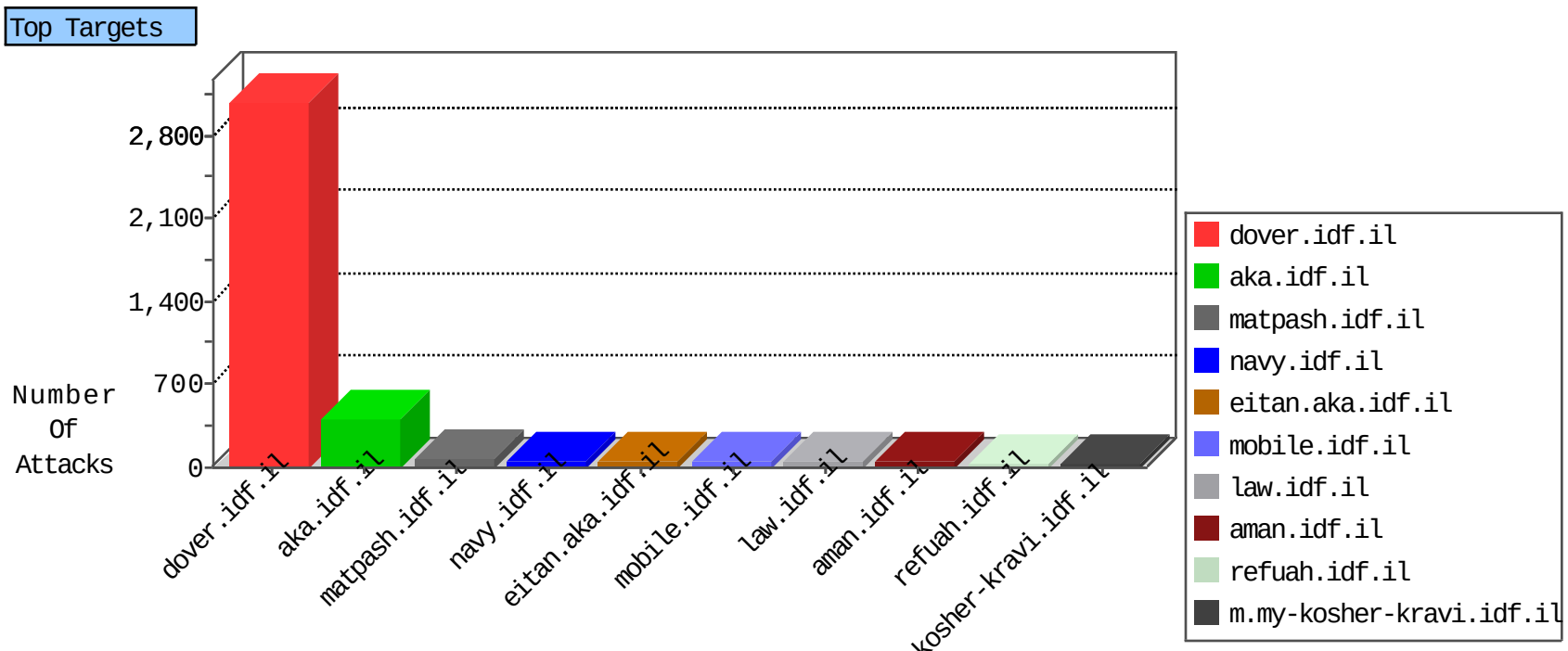
10-19-2015-07:04:09 to 10-19-2015-08:04:09

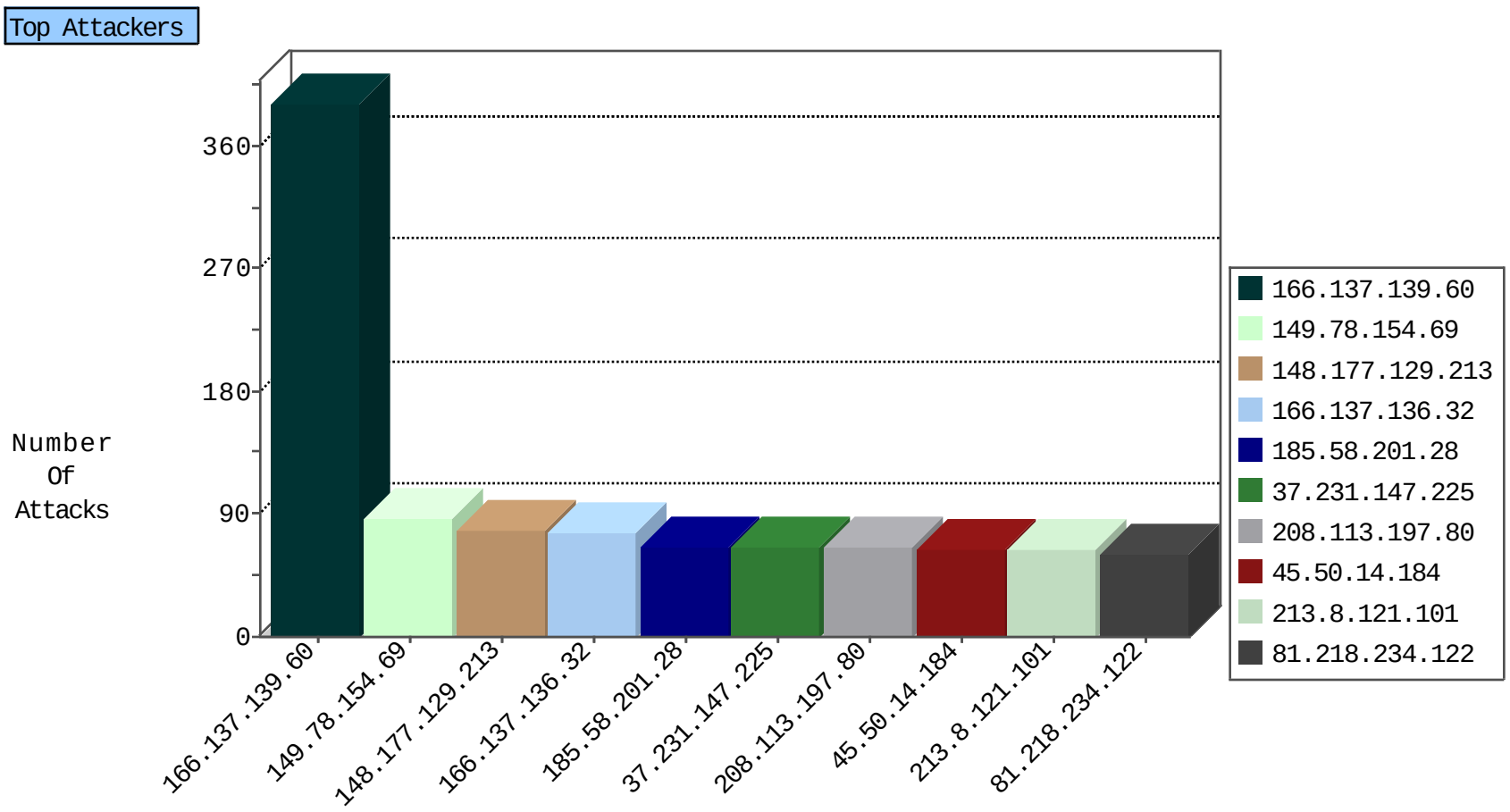
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-19-2015-07:04:09 to 10-19-2015-08:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
213.8.121.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
213.8.121.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
109.67.142.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.143.112.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
80.179.184.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.52.155.32	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
58.84.176.119	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.67.142.79	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.199.244.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.69.121.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
2.54.31.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

10-19-2015-07:04:09 to 10-19-2015-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.212.168.178	Belarus	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
213.8.52.148	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-19-2015-07:04:09 to 10-19-2015-08:04:09

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	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.173	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
77.108.69.253	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
117.69.174.208	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.108.69.253	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.108.69.253	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
77.108.69.253	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.28	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
77.108.69.253	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
37.143.121.235	147.237.72.14	Spain	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.108.69.253	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
77.108.69.253	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1

10-19-2015-07:04:09 to 10-19-2015-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
166.137.139.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	392
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
148.177.129.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
166.137.136.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
45.50.14.184		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
81.218.234.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
64.30.110.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
83.56.31.155	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
5.29.34.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
69.164.141.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.85.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
91.228.127.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.231.147.225	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	45
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
213.8.121.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.86.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.183.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.37.179.139	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
70.209.49.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.52.180.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
41.47.58.191	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
84.108.169.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
212.143.112.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
197.41.234.129	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
216.67.32.145	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
212.143.159.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.231.147.225	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
176.12.140.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.181.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
168.253.181.207		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.52.177.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
149.78.160.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.52.145.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
197.41.213.252	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
80.179.13.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.168.99.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
131.253.35.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
82.102.169.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

10-19-2015-07:04:09 to 10-19-2015-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.113.197.80	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.197.80	Block	65
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
46.121.252.184	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	39
194.90.239.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	39
176.13.12.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
185.32.179.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
185.32.179.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	26
79.197.218.144	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	13
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/17360.jpg	Block	13
91.231.193.150	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;rnd in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	13
69.109.8.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/wwwwwww=f69b07b3wwwwwww_f69b07b3	Block	13
193.106.206.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	13
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	13
81.176.228.59	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/backup/	Block	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17365.jpg	Block	13
91.231.193.150	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/scriptresource.axd	None	13
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	13
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	13
157.55.39.13	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
81.218.48.37	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/12607.jpg	Block	13
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
185.32.179.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
2.54.182.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	13
91.231.193.150	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/webresource.axd	None	13
208.115.113.89	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	13
74.76.168.112	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	13
195.159.233.44	Norway	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	13
176.13.8.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	13
83.223.122.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx):	Block	13
199.188.204.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	13
92.225.32.247	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	13
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	13
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
195.159.233.44	Norway	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	13
176.13.8.98	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	13
91.231.193.150	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	13
207.46.13.88	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/×ž×™×œ×•×?×™×?/contact/	Block	13
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
188.165.15.89	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/hebrew/html	Block	13
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
93.196.123.111	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13

10-19-2015-07:04:09 to 10-19-2015-08:04:09