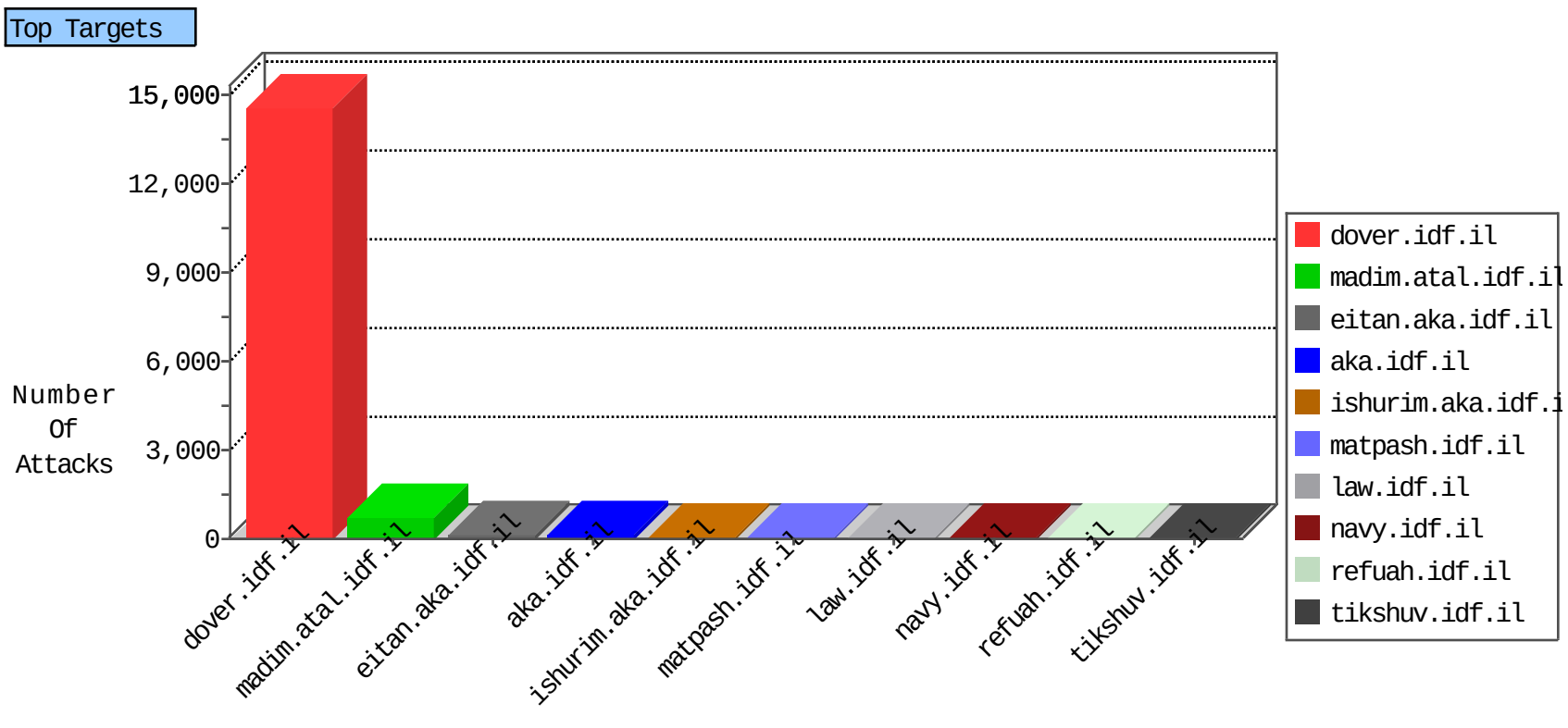
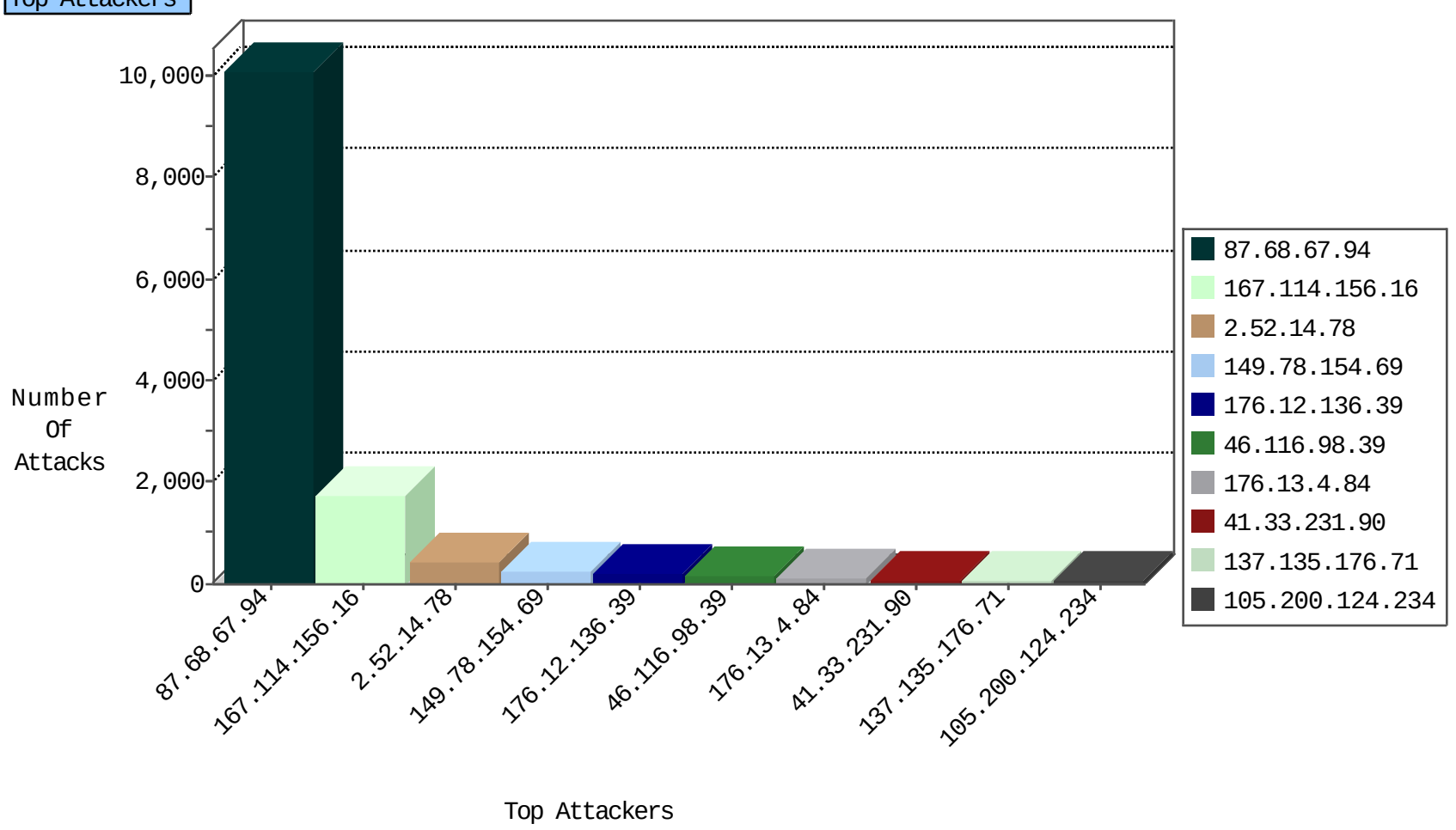
11-07-2015-09:04:01 to 11-07-2015-10:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-07-2015-09:04:01 to 11-07-2015-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2892
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	385
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	49
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
71.238.10.216	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.178.52.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.235.68.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.180.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
197.155.133.113	Mali	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.114.127.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
115.29.173.108	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
115.29.173.108	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
115.29.173.108	China	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
115.29.173.108	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
79.165.196.39	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
5.8.66.78	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
115.29.173.108	China	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

11-07-2015-09:04:01 to 11-07-2015-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-07-2015-09:04:01 to 11-07-2015-10:04:01

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	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
74.117.133.194	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
78.142.19.47	147.237.76.30	Bulgaria	himush.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.133.194	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
74.117.133.194	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
78.142.19.47	147.237.8.28	Bulgaria	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

11-07-2015-09:04:01 to 11-07-2015-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.67.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10067
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	254
176.13.4.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
137.135.176.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
105.200.124.234	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
82.190.98.42	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
197.155.133.113	Mali	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.52.180.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
87.68.67.94	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
71.238.10.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.237.161.2	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
89.139.59.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
46.116.98.39	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
157.55.39.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
81.218.234.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
187.180.14.37	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.187.55.213	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	16
40.77.167.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
168.253.241.174		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.106.40.243	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.14.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.14.78	Block	224
2.52.14.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	197
46.116.98.39	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.98.39	Block	136
176.12.136.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
176.12.136.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
207.232.37.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
80.246.139.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
185.32.179.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
2.52.14.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.14.78	Block	4
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	2
87.68.59.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
185.32.179.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.56.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/9/279.pdf	Block	1
133.130.63.178	Japan	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.154.179.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 31.154.179.86	None	1
79.183.215.105	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/pirsumeymofet.aspx	Block	1
207.46.13.116	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/70239.pdf	Block	1
66.249.64.31	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2954.pdf	Block	1
85.65.106.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.14.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
188.138.1.218	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.1	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2963.pdf	Block	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
188.138.1.218	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.7	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/recruitinformation	Block	1
46.117.89.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.166.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
66.249.67.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg	Block	1
184.105.139.67	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
91.196.50.33	Poland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
79.177.227.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.81.88	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
157.55.39.51	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
81.218.166.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2956.pdf	Block	1
109.66.182.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
31.154.179.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding N]];qB*KSvKg} in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
79.180.57.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1