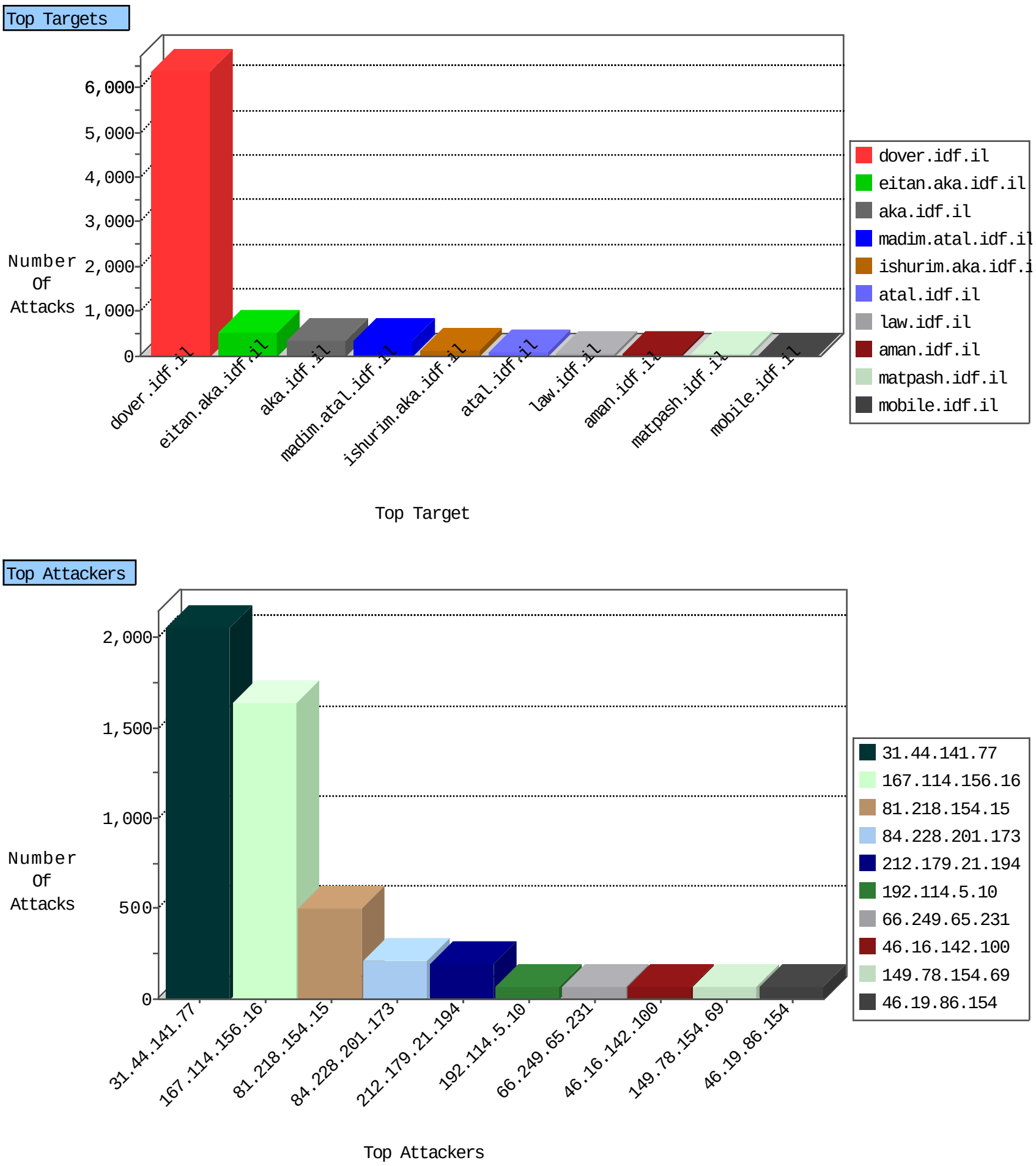
11-08-2015-13:04:05 to 11-08-2015-14:04:05

IDF Under Attack
Daily Report



11-08-2015-13:04:05 to 11-08-2015-14:04:05

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	2654
192.118.30.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	70
37.26.147.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	67
109.65.36.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
80.246.137.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
176.13.10.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
192.118.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.143.186.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
85.64.250.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
95.35.216.145	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
95.35.216.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
37.26.149.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.235.69.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.143.186.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.1.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.64.28.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.155.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
91.228.248.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.127.163.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.148.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.139.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
113.108.21.16	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
95.35.216.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
81.218.17.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
80.74.123.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
183.79.221.142	Japan	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.246.137.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
62.90.45.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
118.3.83.108	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-08-2015-13:04:05 to 11-08-2015-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.242	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	8
81.218.245.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.68.157.177	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-08-2015-13:04:05 to 11-08-2015-14:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
128.234.92.44	147.237.77.216	Romania	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
213.57.146.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
5.8.66.101	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
176.12.141.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.101	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
101.1.17.53	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -sS window 2048	1
87.68.71.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.159.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.101	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
192.115.90.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.101	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.34.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
101.1.17.53	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -f -sS	1
85.65.81.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.130.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-08-2015-13:04:05 to 11-08-2015-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.44.141.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2060
81.218.154.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	456
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	195
192.114.5.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	63
149.78.49.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.65.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
132.71.16.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
31.168.87.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.93.220	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	33
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
217.132.83.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
157.55.39.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.65.91		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	27
212.150.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
89.163.222.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
115.84.95.161	Lao People's Democratic Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.93.216	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	24
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.116.160.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.65.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.93.224	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
5.22.129.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
149.88.231.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.247.161.206	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
91.228.248.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
62.219.239.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
107.184.248.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
65.49.68.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.12.145.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.201.171.211	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.121.75.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.154	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.201.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	140
84.228.201.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.201.173	Block	75
81.218.154.15	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.154.15	Block	47
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
37.142.132.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.210.143.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.12.151.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
162.144.48.198	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 162.144.48.198	Block	4
194.90.66.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
80.246.137.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.140.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 213.139.52.84	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	2
176.13.9.236	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
109.67.17.110	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.12.146.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	2
82.81.42.185	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	2
93.172.159.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/112192.pdf	Block	1
2.54.31.164	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
176.13.2.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.96.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/valtam/main/home.asp	Block	1
157.55.39.141	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
62.210.88.201	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Malformed HTTP Header Line 1	Block	1
109.65.113.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
176.12.145.20	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
138.134.102.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed HTTP Header Line from 213.139.52.84	Block	1
84.228.201.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
2.54.163.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.187.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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/4/2944.pdf	Block	1
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Malformed URL http/1.1	Block	1
81.218.154.15	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
195.212.29.174	Europe	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.93.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	Block	1
46.117.221.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Redundant HTTP Headers Referer	Block	1
2.54.179.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.139.52.84	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request request version	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1