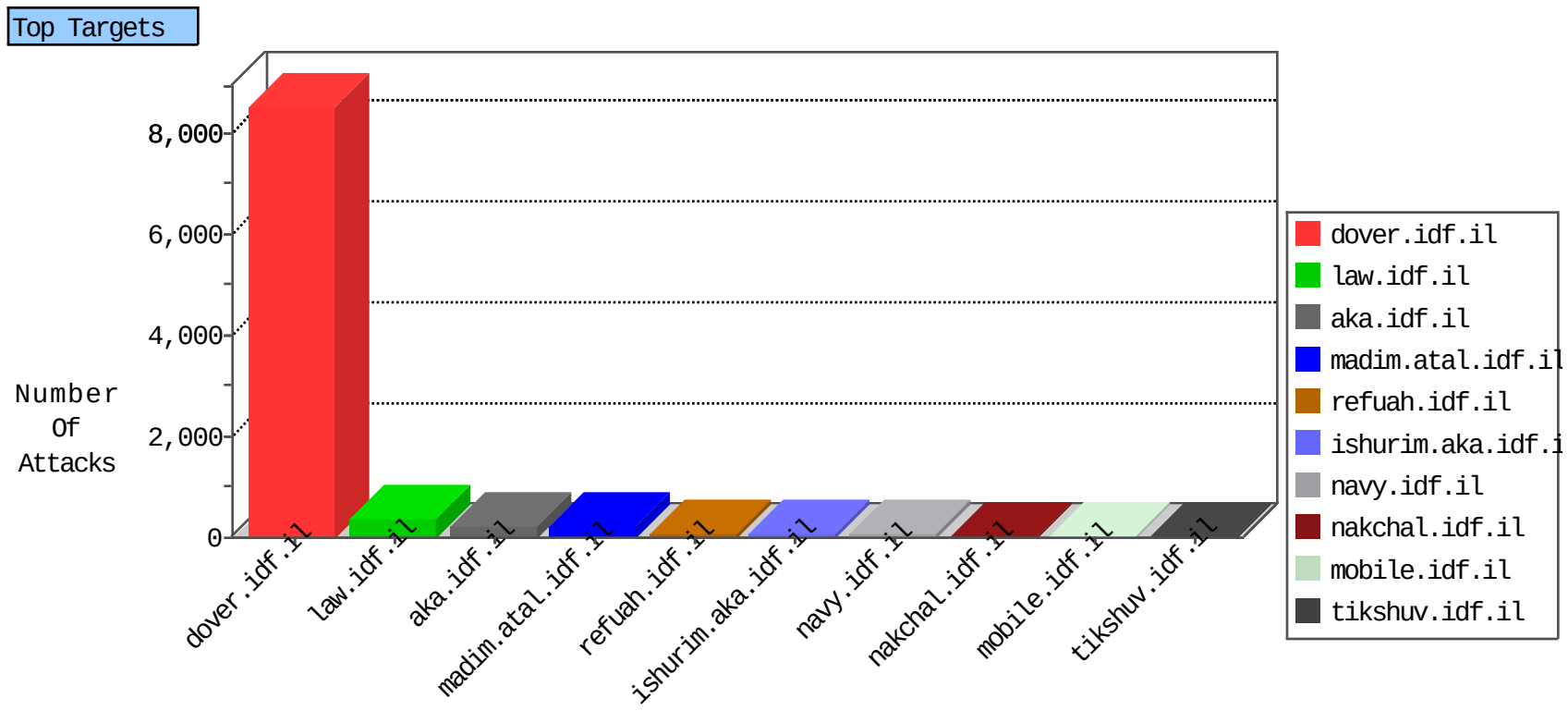
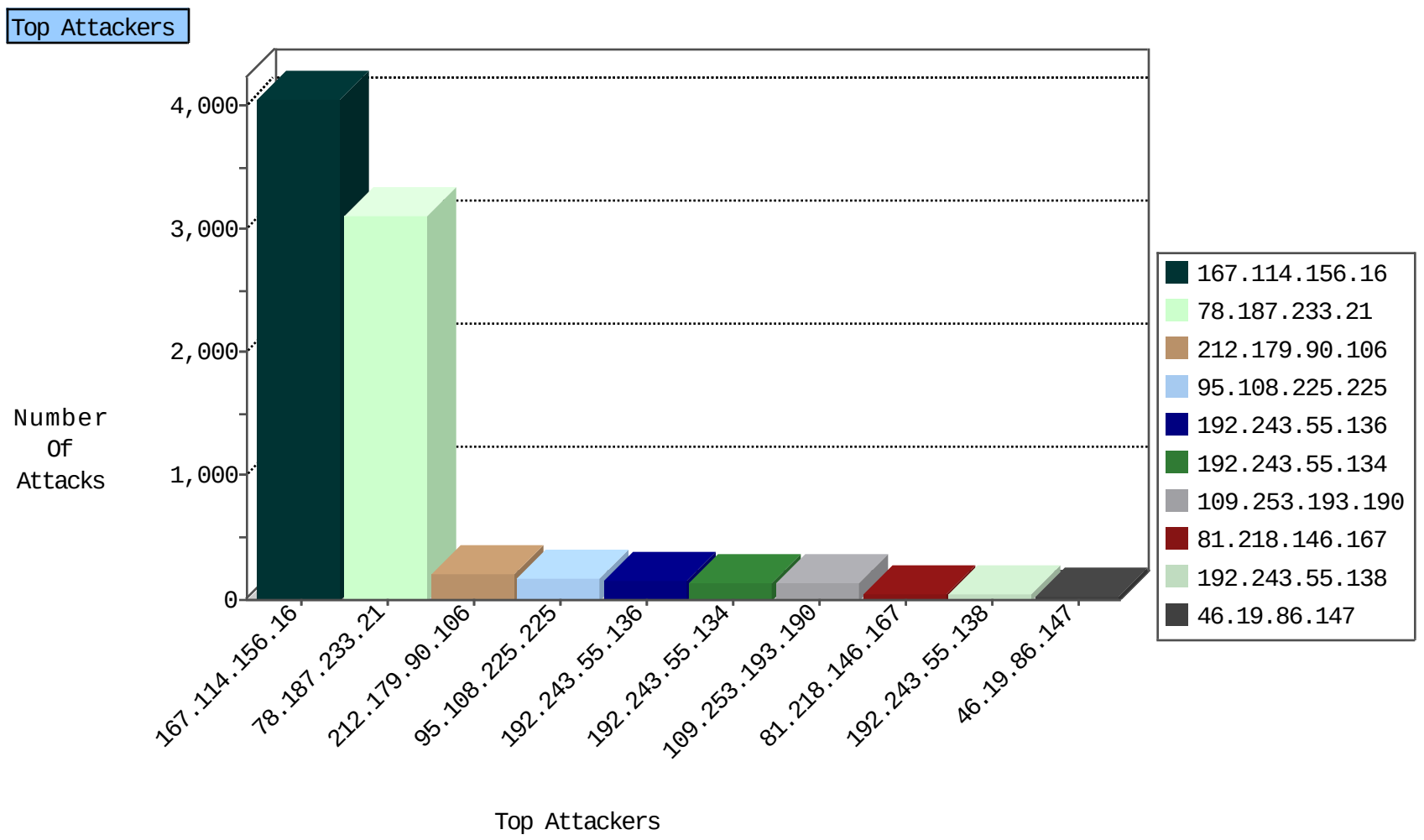
04-13-2016-11:04:03 to 04-13-2016-12:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-13-2016-11:04:03 to 04-13-2016-12:04:03

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	Block_Ip_Web_In	drop	4050
46.117.157.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	170
46.19.85.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	118
95.86.120.77	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	63
78.187.233.21	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	61
79.178.29.28	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35
212.150.66.161	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
45.55.189.162	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
85.64.129.138	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
212.199.15.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
217.132.21.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
78.187.233.21	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
95.108.225.225	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
62.219.86.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
194.54.168.65	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
183.136.196.157	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.90.99.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.74	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.235	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
46.121.93.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.94	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
94.230.86.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.93.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.182.123.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.102	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
2.53.190.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.102	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
95.108.133.222	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-13-2016-11:04:03 to 04-13-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.187.233.21	Turkey	147.237.77.216	dover.idf.il	C1000096: HTTP: BanglaDos	Block	26
81.218.146.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.67.18.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.172	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

04-13-2016-11:04:03 to 04-13-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
78.187.233.21	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	5
82.102.244.234	147.237.77.176	Palestinian Territory, Occupied	matpash.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
89.138.253.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
122.52.104.84	147.237.76.42	Philippines	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.111.188.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.201.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.60.46.124	147.237.77.216	Israel	dover.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

04-13-2016-11:04:03 to 04-13-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
78.187.233.21	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2987
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	207
95.108.225.225	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
93.173.128.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
81.218.146.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
109.253.202.78	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
91.240.80.16	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	21
37.26.148.204	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
125.215.235.181	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
89.241.24.212	United Kingdom	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	19
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
165.225.72.64	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.8	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
80.246.137.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.146.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
188.120.148.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.67.50.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
212.25.86.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
192.116.94.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.222.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.33.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
46.19.85.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.168.144.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.111.188.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.69.113.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.54.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
93.173.254.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.165.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.33.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8

04-13-2016-11:04:03 to 04-13-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.193.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.53.148.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	9
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.220.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
91.240.80.16	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.61	Israel	147.237.76.42	refuah.idf.il	Multiple Abnormally Long Request from 46.19.85.61	Block	2
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	2
46.19.85.61	Israel	147.237.76.42	refuah.idf.il	Multiple Illegal HTTP Version from 46.19.85.61	Block	2
109.67.18.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.85.61	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.61	Block	2
46.19.85.61	Israel	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.61	Block	2
84.111.188.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
79.177.246.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
219.74.239.90	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.10.182	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple _vti_ from 81.218.53.114	Block	1
38.107.67.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/69054.pdf	Block	1
46.19.86.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.88.229.201	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
82.81.90.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/images/1.he/error.png	Block	1
79.180.33.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
176.13.10.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
94.76.121.14	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
40.77.167.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/_vti_bin/owssvr.dll	Block	1
69.89.21.76	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/wp-admin/	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.61	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
82.81.90.82	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.81.90.82	Block	1
79.181.119.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyu	Block	1
37.26.148.204	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.204 (Open Mode)	None	1
192.243.55.136	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
66.249.66.128	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
81.218.146.167	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
72.47.224.30	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
62.219.54.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
162.217.144.45	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
82.166.102.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

04-13-2016-11:04:03 to 04-13-2016-12:04:03