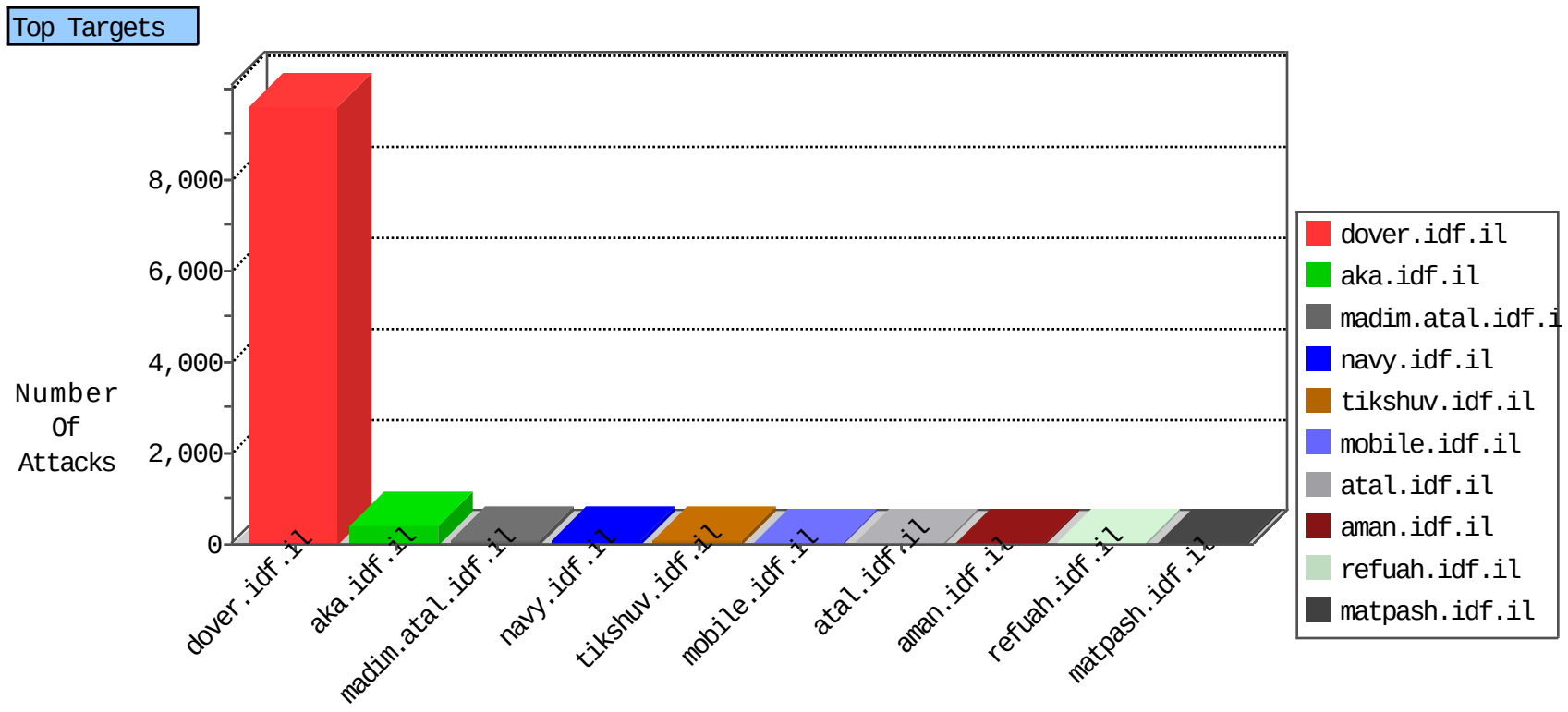
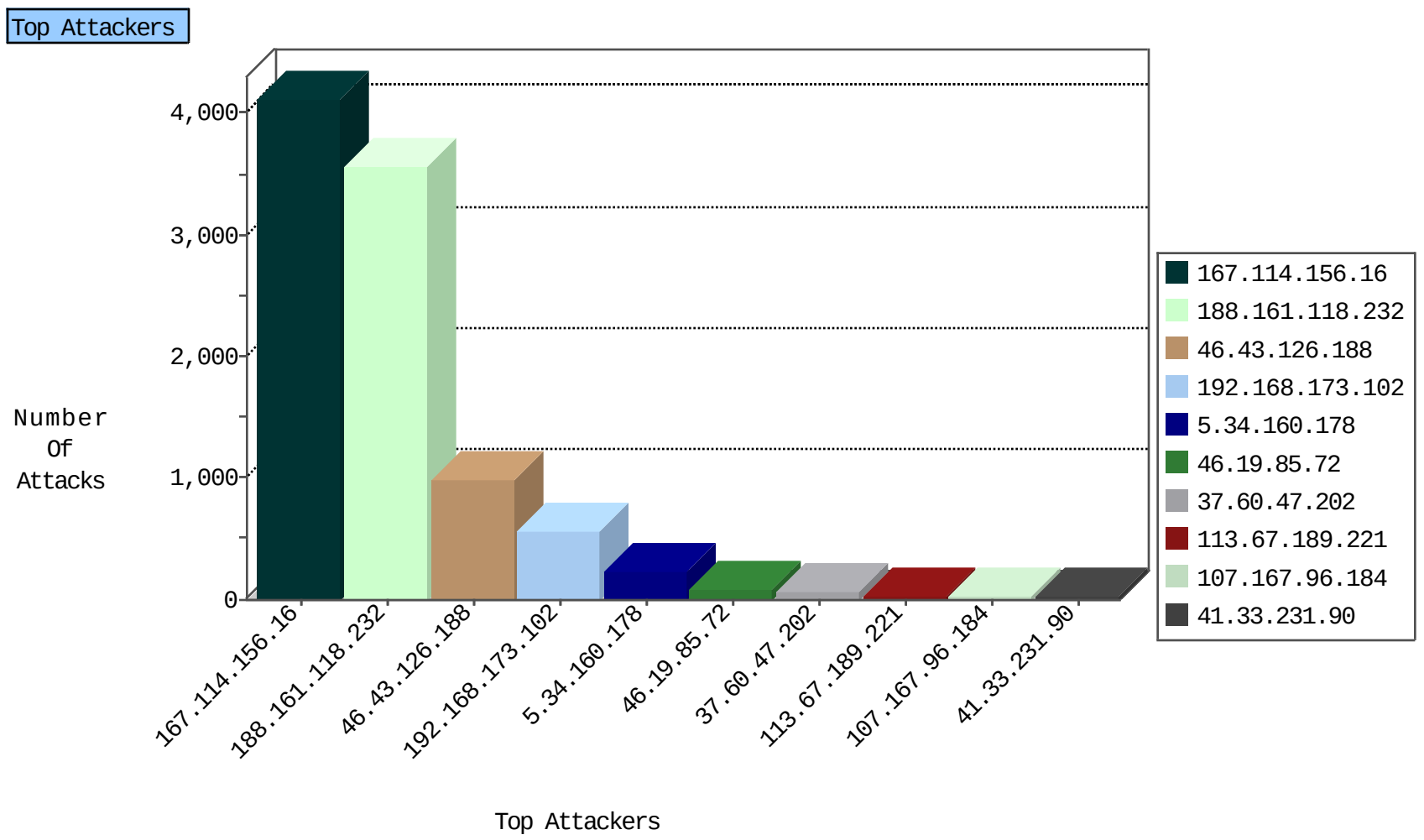
04-08-2016-16:04:03 to 04-08-2016-17:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-08-2016-16:04:03 to 04-08-2016-17:04:03

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	4096
46.43.126.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	1101
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	502
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	10
209.126.127.17	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
82.145.220.179	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
209.126.110.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
209.126.110.228	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
209.126.110.228	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
210.140.82.35	Japan	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1

04-08-2016-16:04:03 to 04-08-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.187.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.228.248.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.105.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.50.122.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
132.66.237.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.214.249.152	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
105.110.23.24	Algeria	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
105.110.23.24	Algeria	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-16:04:03 to 04-08-2016-17:04:03

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
66.249.79.109	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.240.213.93	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.73	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
218.108.132.58	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
216.227.58.7	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
216.198.187.120	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.6.7.73	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
105.110.23.24	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1
63.221.141.195	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
45.63.16.73	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
216.227.58.7	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
216.227.58.7	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
201.172.194.198	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.218.22.12	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.172.34.79	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2016-16:04:03 to 04-08-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2775
46.43.126.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	686
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	360
46.43.126.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	239
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	222
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	203
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop		drop	199
37.60.47.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
107.167.96.184	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.228.248.18	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.52.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
31.210.186.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
94.230.86.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
90.230.58.172	Sweden	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	11
197.27.82.194	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
94.230.86.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.101.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.27.82.194	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
31.44.143.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
94.230.86.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.86	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.86	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.199.57.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.144	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.139.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
105.110.23.24	Algeria	147.237.77.216	dover.idf.il	SQL Injection	SQL injection detected in request: 'concat'	monitor	5
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop		drop	5
5.102.242.160	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.217.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.167.112.106	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.28.134.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.120.154.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
88.80.184.136	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.139.183.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
176.13.0.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

04-08-2016-16:04:03 to 04-08-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
113.67.189.221	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.67.189.221	Block	27
149.50.82.87	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.50.82.87	Block	17
37.46.38.22	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
105.110.23.24	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
93.173.223.98	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.173.223.98	Block	6
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
37.26.149.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.177.197.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.173.223.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1601	Block	3
176.228.50.195	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	3
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Multiple Illegal HTTP Version from 46.19.85.185	Block	2
93.173.223.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Multiple Malformed URL from 46.19.85.185	Block	2
107.72.162.15	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/cgi-bin/ipdiags.ha	Block	2
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.185	Block	2
113.67.189.221	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 46.19.85.185	Block	2
87.70.125.233	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.43.126.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.140	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
105.131.16.221	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
177.54.224.214	Brazil	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
52.169.157.143	United States	147.237.76.42	refuah.idf.il	Parameter Type Violation &l in www.refua.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
207.46.13.144	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
151.237.179.41	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.asp	Block	1
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
105.158.116.215	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.182.52.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
177.54.224.214	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/images/xxu.php	Block	1
113.67.189.221	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
52.169.157.143	United States	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx	Block	1
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
80.246.136.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.161.118.232	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
141.212.122.209	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
176.13.0.153	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Malformed URL __atssc=facebook;2	Block	1
2.52.144.209	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method 5707b41aebb8c825000; in URL __atssc=facebook	Block	1
207.46.13.15	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	1
46.18.17.136	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
113.67.189.221	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 113.67.189.221	Block	1

04-08-2016-16:04:03 to 04-08-2016-17:04:03