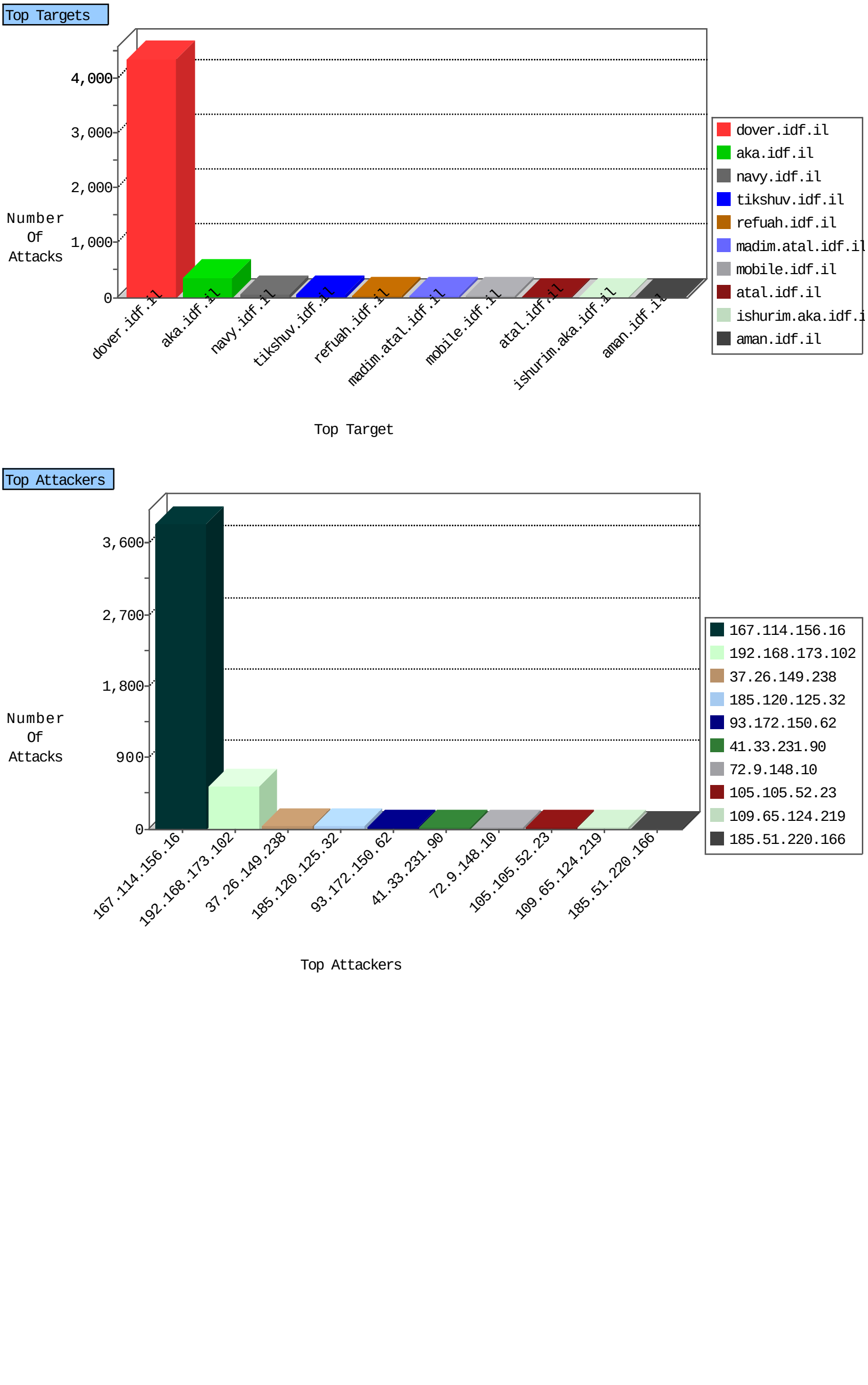
04-08-2016-20:04:04 to 04-08-2016-21:04:04

IDF Under Attack
Daily Report



04-08-2016-20:04:04 to 04-08-2016-21:04:04

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	3841
105.105.52.23	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	13
209.126.127.17	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
209.126.127.17	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
93.215.23.185	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
93.215.23.185	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
93.215.23.185	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.23.185	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
93.215.23.185	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
93.215.23.185	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
217.172.189.11	Germany	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
93.215.23.185	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-20:04:04 to 04-08-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	14
2.53.15.51	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.8.204.34	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
105.105.52.23	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
207.46.13.45	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.136.216	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-20:04:04 to 04-08-2016-21:04:04

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
84.200.15.174	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
67.130.39.67	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
64.13.147.226	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
83.17.11.50	147.237.0.19	Poland	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
67.130.39.67	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1

04-08-2016-20:04:04 to 04-08-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	344
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	205
93.172.150.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.149.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.65.124.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.51.220.166	Iraq	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
147.153.151.30	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
185.32.179.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.240	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
93.172.231.8	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.32.179.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
87.69.165.79	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.193	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.188.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.197.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.4.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
82.166.243.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.3.144.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.12.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
105.105.52.23	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.151.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.88.249.209	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.50.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
78.40.181.34	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.73.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.159.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.36.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.19.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.97.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.70.45.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.170.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-08-2016-20:04:04 to 04-08-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.125.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
197.15.245.65	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.15.245.65	Block	6
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	6
5.102.242.250	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.242.250	Block	3
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
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	2
185.32.179.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.102.242.250	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
74.93.128.228	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#0]]•£ÐFårŠð†[[#0]]t[[#26]]ŸX[[#7]]&~[[#18]]ô[`’¤I in URL ↾<dz‘ ¨[[#0]][[#0]][[#28]]¸/¸+¸0¸,¸[[#19]]¸	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#0]]•£ÐFårŠð†[[#0]]t[[#26]]ŸX[[#7]]&~[[#18]]ô[`’¤I	Block	1
54.153.33.233	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
119.46.1.66	Thailand	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8992-he/0	Block	1
31.223.176.46	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	NULL Character in Header Name at	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.0.187.34	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1398-12396-en/dover.aspx'	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
79.181.36.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch.	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in URL ↾<dz‘ ¨[[#0]][[#0]][[#28]]¸/¸+¸0¸,¸[[#19]	Block	1
197.15.245.65	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/000000000000000	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
134.0.14.205	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
36.248.161.153	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#0]]•£ÐFårŠð†[[#0]]t[[#26]]ŸX[[#7]]&~[[#18]]ô[`’¤I	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers	Block	1
212.34.12.113	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.19.85.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.226	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
79.182.173.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/ctl00_ctl00_cphmain_cphsachar_divpersonalquestionscontent	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Illegal HTTP Version À[[#20]]À	Block	1
197.89.155.34	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.88.66.231	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.8.28.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	NULL Character in URL ↾<dz‘ ¨[[#0]][[#0]][[#28]]¸/¸+¸0¸,¸[[#19]]¸	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
50.62.160.248	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
79.183.184.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Malformed HTTP Header Line 2	Block	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/fatah_activists/index	Block	1
66.249.93.50	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.111	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
50.63.197.202	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
119.46.1.66	Thailand	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 119.46.1.66	Block	1
5.172.237.137	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
74.93.128.228	United States	147.237.77.233	atal.idf.il	Malformed URL ↾<dz‘ ¨[[#0]][[#0]][[#28]]¸/¸+¸0¸,¸[[#19]]¸	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04	Block	1
40.77.167.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

04-08-2016-20:04:04 to 04-08-2016-21:04:04