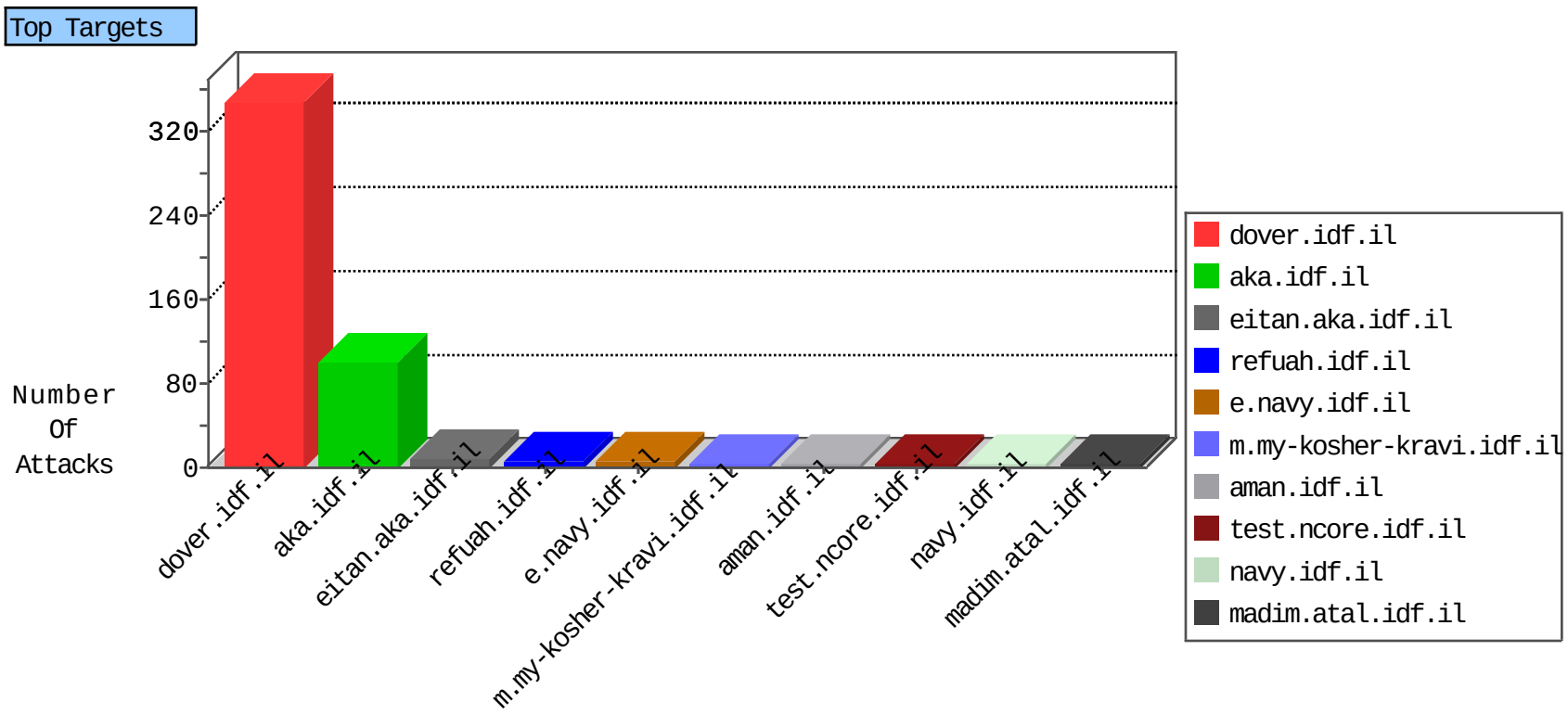
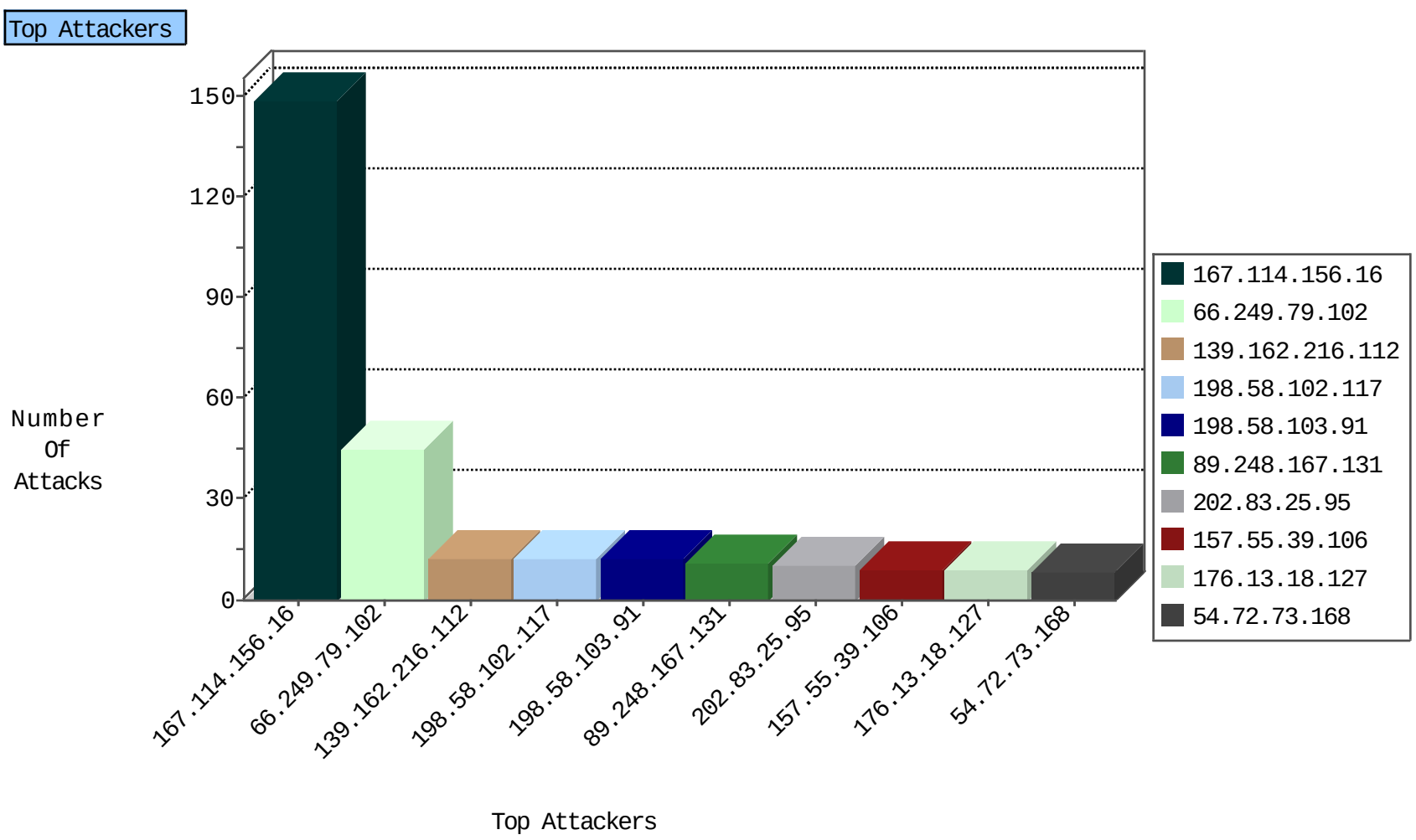
04-30-2016-07:04:08 to 04-30-2016-08:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-30-2016-07:04:08 to 04-30-2016-08:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	5804
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1811
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
67.210.40.189	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
163.172.153.224	United Kingdom	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
198.20.69.74	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
78.31.67.9	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
163.172.153.224	United Kingdom	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
5.206.231.84	Portugal	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
209.126.136.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
163.172.153.224	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
78.31.67.9	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-30-2016-07:04:08 to 04-30-2016-08:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-07:04:08 to 04-30-2016-08:04:08

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
66.249.81.212	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.248.167.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.84.22	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
187.160.167.110	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.84.22	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.84.22	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
125.26.17.247	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.82.25.17	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.167.131	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1

04-30-2016-07:04:08 to 04-30-2016-08:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.18.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.101.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.62.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.197.176.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.55.210.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.67.36.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.197.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.144.63.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.143.180.166	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
66.249.64.186	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.142.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
63.249.66.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.2.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.65.24.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.83.25.95	India	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
2.53.8.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.215	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.24.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
202.83.25.95	India	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.10	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.120.238.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

04-30-2016-07:04:08 to 04-30-2016-08:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.187.64.91	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 200.187.64.91	Block	5
62.210.97.48	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.97.48	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
62.210.97.48	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman-->אימות	Block	1
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	1
109.200.5.149	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
54.67.36.215	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
202.83.25.95	India	147.237.76.86	navy.idf.il	Unauthorized Method HEAD for /	Block	1
81.169.144.135	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.64.181	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in eitan.aka.idf.il/938-en/eitan.aspx	None	1
157.55.39.76	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	1
54.184.43.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/homepage.aspx	Block	1
202.83.25.95	India	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
84.108.126.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.214.67.94	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1380-he/dover.aspx parameter PageNum	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
94.190.62.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.79.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
202.83.25.95	India	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
107.178.109.112	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.79.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
49.177.22.136	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
202.83.25.95	India	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1

04-30-2016-07:04:08 to 04-30-2016-08:04:08