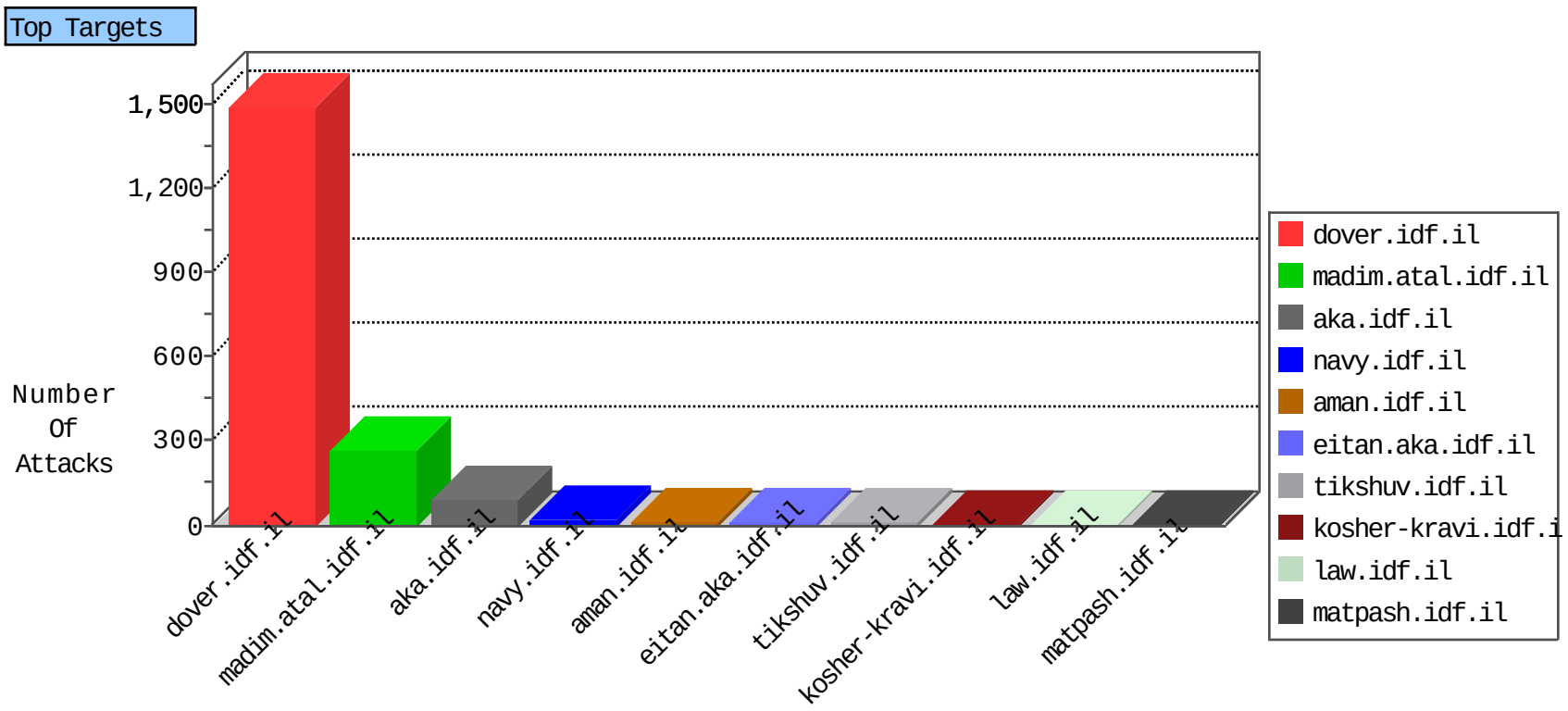
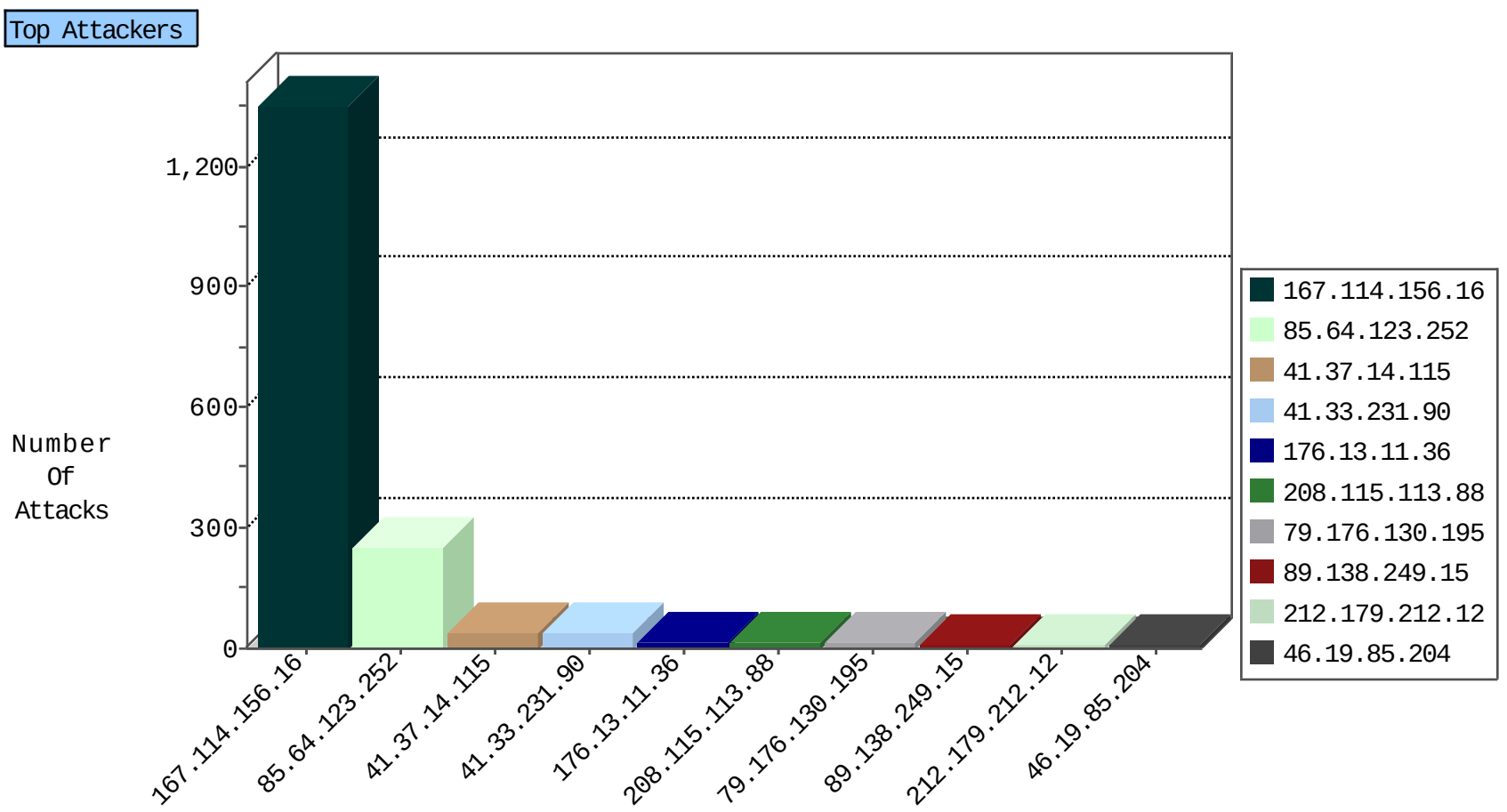
04-15-2016-07:04:09 to 04-15-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-15-2016-07:04:09 to 04-15-2016-08:04:09

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	1345
101.201.147.32	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.112	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-07:04:09 to 04-15-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
69.197.177.50	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-07:04:09 to 04-15-2016-08:04:09

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
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
104.171.126.27	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.126.27	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -f -sS	1
97.74.4.26	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
97.74.4.26	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
173.65.154.27	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
165.138.213.4	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
23.102.168.255	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
107.158.255.194	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
14.172.3.137	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.100.128	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
106.184.2.29	147.237.8.14	Japan	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.171.126.27	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 2048	1
97.74.4.26	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
97.74.4.26	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.76.202	Lithuania	e.halag.idf.il	ET SCAN Potential SSH Scan	1
97.74.4.26	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.65.154.27	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
165.138.213.4	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
23.102.168.255	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.100.128	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1

04-15-2016-07:04:09 to 04-15-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
41.37.14.115	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
41.37.14.115	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.138.249.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
41.37.14.115	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.123.252	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.148.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.78	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.130.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.130.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.51.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.212.12	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
179.211.231.7	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
172.56.4.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.8.163.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.102.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.165.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.120.126.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.212.12	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.40.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.145.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
144.76.30.236	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
37.142.64.120	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.142.64.120	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
162.208.92.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.144.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.52	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
185.3.144.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.209	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.187.114.171	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.201.147.32	China	147.237.0.15	kosher-kravi.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
5.102.195.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.70.198	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.210	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.134.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.84	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.21.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.147.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

04-15-2016-07:04:09 to 04-15-2016-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.123.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	242
176.13.11.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	12
85.64.123.252	Israel	147.237.0.19	madim.atal.idf.il	Automated Vulnerability Scanning V1	Block	6
198.50.189.250	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.50.189.250	Block	5
66.220.145.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.181.102.110	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.102.110	Block	2
66.249.66.1	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.78	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/asp/home.asp/info.asp	Block	1
141.8.132.2	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-6584-en/patzar.aspx,	Block	1
79.181.102.110	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.33.212.11	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
198.50.189.250	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
46.0.52.15	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	1
157.55.39.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/ã—â¦ã—â€•	Block	1
79.182.110.251	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.202.150.86	Brazil	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
97.74.215.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
72.29.127.17	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
46.0.52.15	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
157.55.39.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/news/	None	1
79.182.110.251	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	1
186.202.153.123	Brazil	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
37.187.114.171	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /irj/portal	Block	1
104.131.30.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
72.167.232.30	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/mesiratmeida/	Block	1
50.62.161.39	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
167.114.211.10	Canada	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
79.183.118.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/error/styles/error.css	Block	1
192.249.109.14	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
37.187.114.171	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /irj/portal	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
211.35.53.5	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
50.62.161.175	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
176.9.61.55	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1

04-15-2016-07:04:09 to 04-15-2016-08:04:09