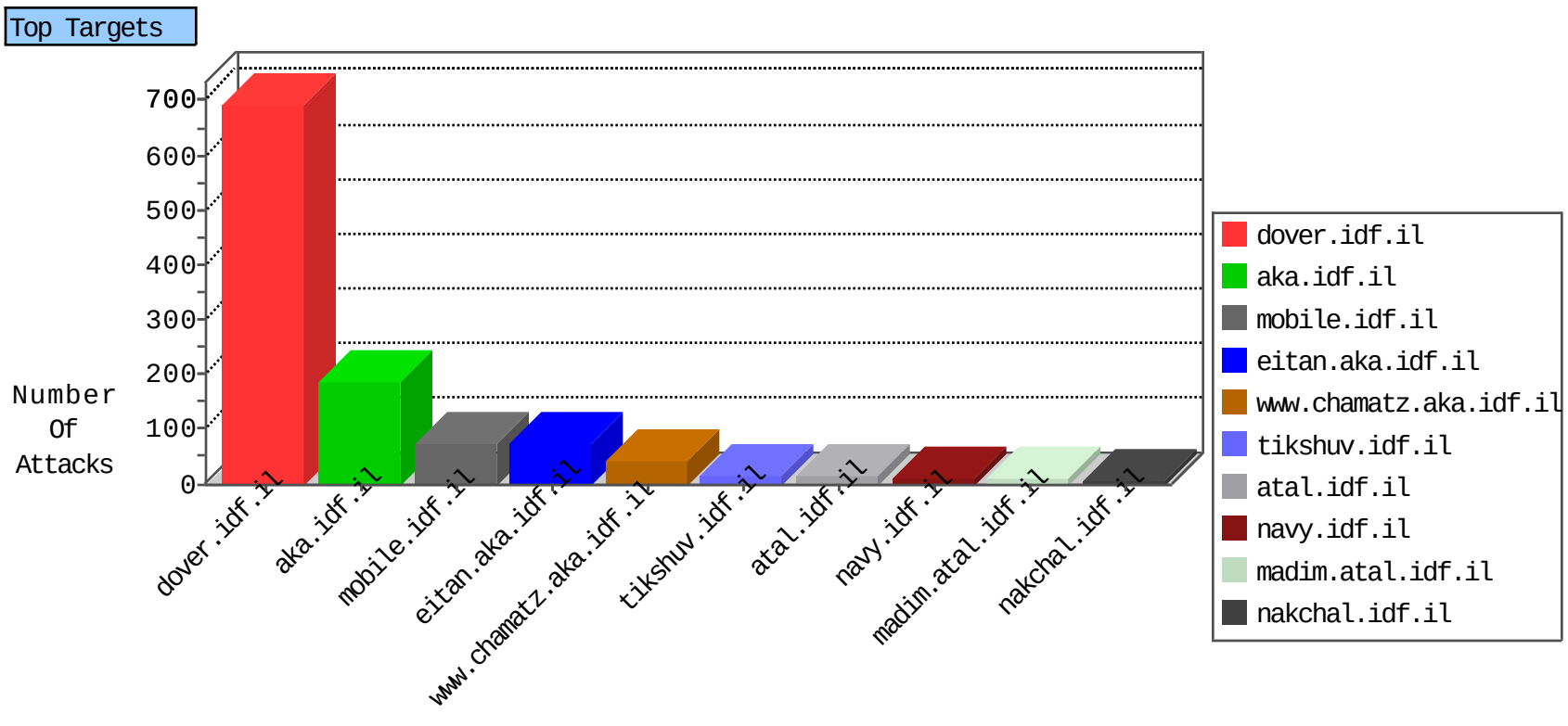
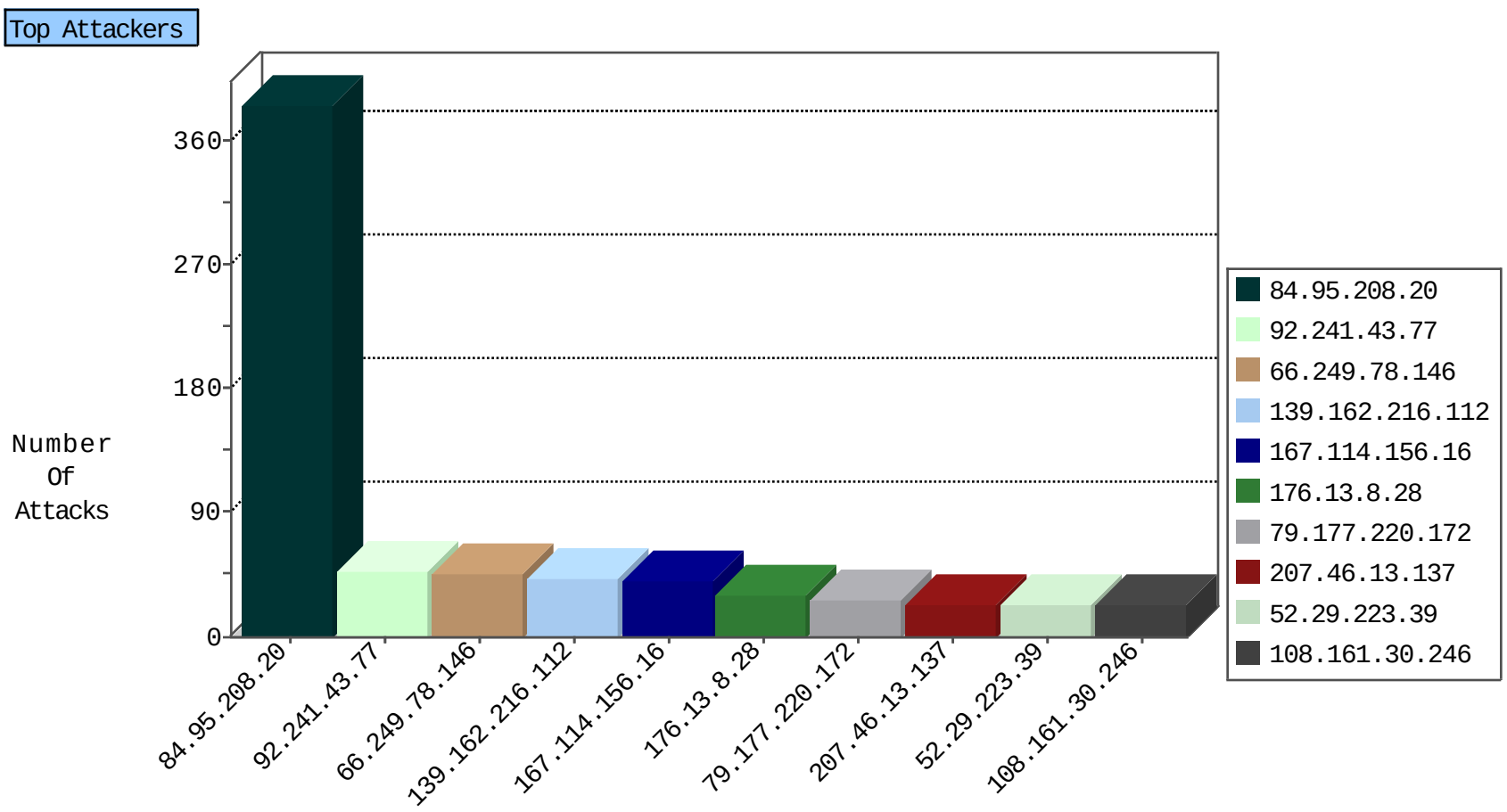
04-29-2016-02:04:03 to 04-29-2016-03:04:03

IDF Under Attack
Daily Report





04-29-2016-02:04:03 to 04-29-2016-03:04:03

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	TCP handshake violation, first packet not syn	drop	18234
8.29.198.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4007
207.46.13.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2291
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	8
84.111.83.57	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
188.138.1.218	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-02:04:03 to 04-29-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-02:04:03 to 04-29-2016-03:04:03

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
89.248.167.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
161.202.120.148	147.237.77.19	Japan	law-forum.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.97.45	147.237.76.86	Spain	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.232.98.3	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
78.56.201.63	147.237.72.166	Lithuania	aka.idf.il	Xenu Link Sleuth User Agent	1
104.232.98.3	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
183.2.242.64	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.148	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.148	147.237.77.121	Japan	e.navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.147	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.3	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
71.6.216.47	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
208.67.1.222	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
23.96.109.87	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
183.2.242.64	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
183.2.242.64	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.148	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-29-2016-02:04:03 to 04-29-2016-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
92.241.43.77	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
176.13.8.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
108.161.30.246	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.177.220.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
45.55.62.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
69.78.1.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
95.130.89.4	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.184.225.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.184.242.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.37	Israel	147.237.76.31	nakchal.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	6
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.51.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.116.116.111	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.200.182.174	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.148.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.142.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.21.66.6	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.224.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
8.29.198.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
162.203.2.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-29-2016-02:04:03 to 04-29-2016-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	117
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	73
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	26
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
176.13.8.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
79.177.220.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
131.253.25.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
37.26.149.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.150.244.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.150.244.228	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
43.240.13.215	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
5.29.51.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.65.143.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
43.240.13.215	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
65.55.210.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/apple-app-site-association	Block	1
212.150.244.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.79.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.37	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
79.178.57.161	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
198.58.103.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
65.55.210.236	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.79.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
79.178.57.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	1
199.30.24.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
212.150.244.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/mobile	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.137	Block	1

04-29-2016-02:04:03 to 04-29-2016-03:04:03