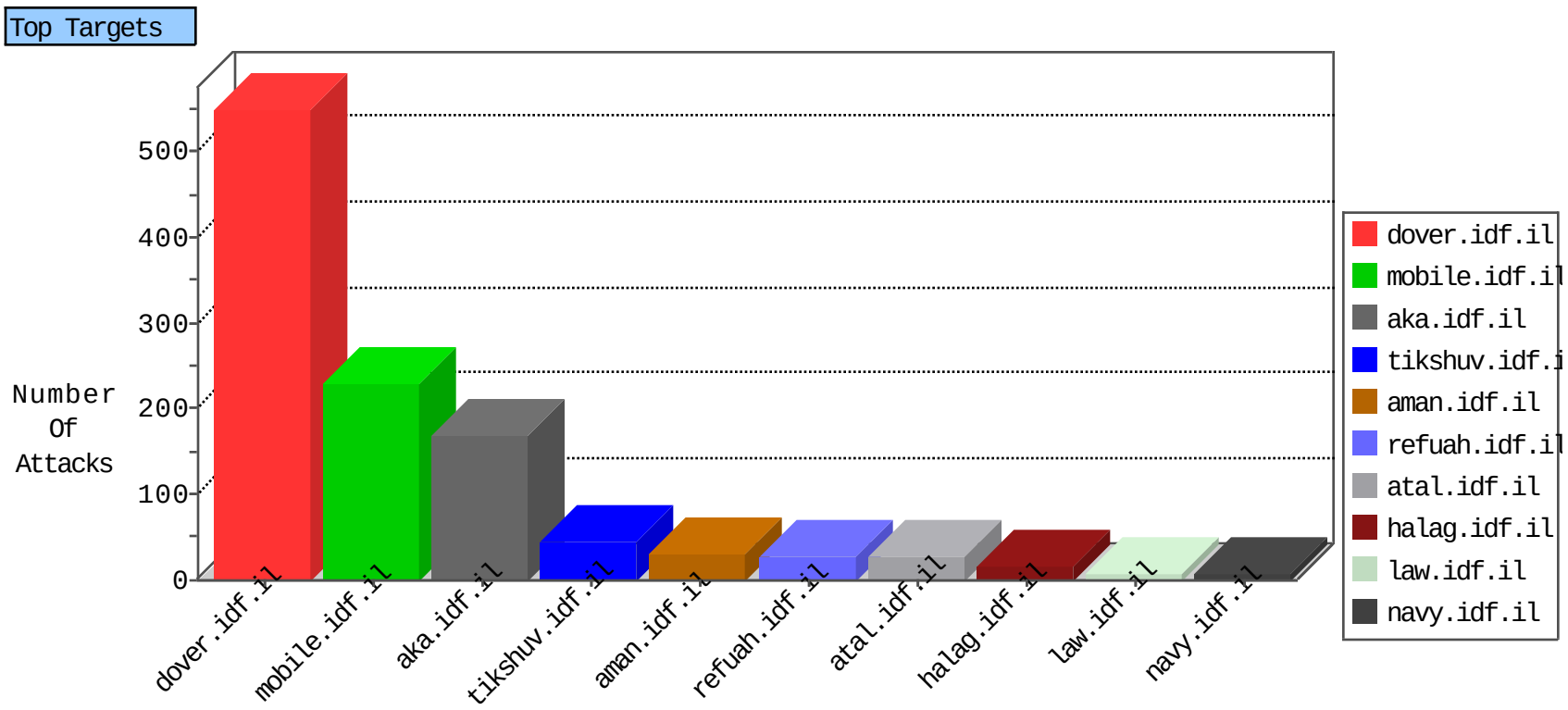
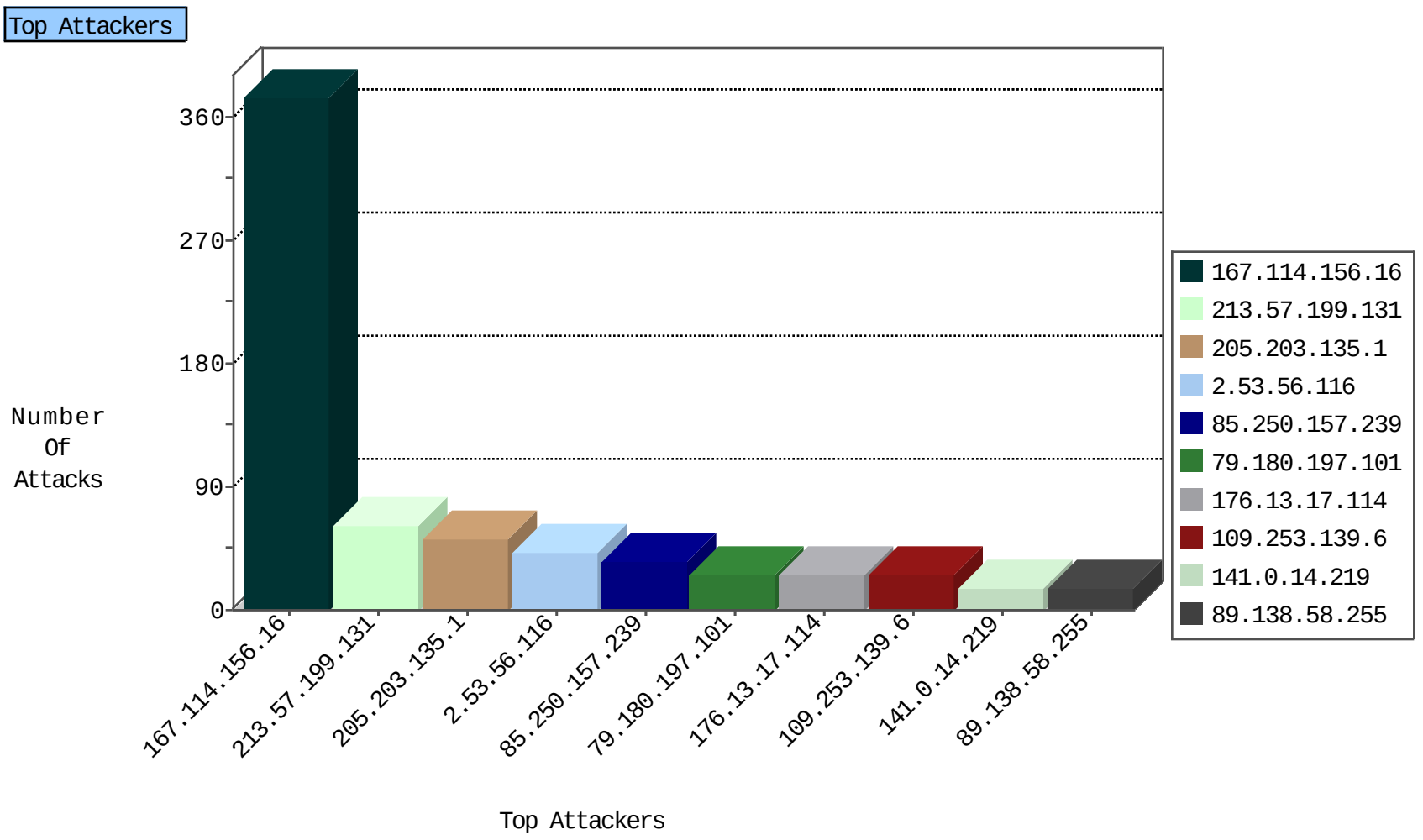
04-29-2016-12:04:01 to 04-29-2016-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-12:04:01 to 04-29-2016-13:04:01

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	16070
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2049
82.145.218.194	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
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
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
46.174.54.63	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
87.70.91.92	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
71.6.146.186	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-12:04:01 to 04-29-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.68.224.173	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

04-29-2016-12:04:01 to 04-29-2016-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
70.68.224.173	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.93.42	147.237.76.31	Europe	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
192.227.172.158	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP admin.php access	1
183.221.192.44	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
179.43.141.214	147.237.8.14	Switzerland	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
213.16.45.243	147.237.0.35	Bulgaria	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
52.16.5.197	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
213.16.45.243	147.237.0.35	Bulgaria	akaws.idf.il	ET SCAN NMAP -f -sS	1
203.86.29.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
183.221.192.44	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.169.100.157	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
213.16.45.243	147.237.0.35	Bulgaria	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
46.151.52.231	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
203.86.29.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
203.81.149.94	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-29-2016-12:04:01 to 04-29-2016-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
2.53.56.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
85.250.157.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
109.253.139.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.180.197.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.17.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.57.199.131	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
213.57.199.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
141.0.14.219	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
213.57.199.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
213.57.199.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.43.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.58.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.250.157.239	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.113.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
87.70.70.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.129.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.18.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.114.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.51.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.0.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.205.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.161.9	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.78.72.170	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.66.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.19.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.193.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.6.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-12:04:01 to 04-29-2016-13:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.176	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.57.161.9	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.32.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-12:04:01 to 04-29-2016-13:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.56.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
79.180.197.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.17.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.139.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
89.138.58.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.227.172.158	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.227.172.158	Block	3
185.32.179.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.99	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
132.66.237.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/default.asp	Block	2
176.13.1.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
87.70.9.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
46.120.66.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.227.172.158	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.120.129.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.64.113.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.43.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.74.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
217.132.131.141	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
46.117.216.81	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
88.198.44.46	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
79.179.145.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.230	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
192.227.172.158	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 192.227.172.158	Block	1
149.78.72.170	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.51.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.250.157.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
176.13.3.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.216.81	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.216.81	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3288.jpg	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspx-title=over	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
85.64.42.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2422.jpg	Block	1
164.132.161.31	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
40.77.167.9	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
88.156.120.11	Poland	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
79.178.18.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.140.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
164.132.161.43	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
88.156.120.11	Poland	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
79.178.153.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/homepage/mobile	Block	1
51.255.65.97	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
192.227.172.158	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1

04-29-2016-12:04:01 to 04-29-2016-13:04:01