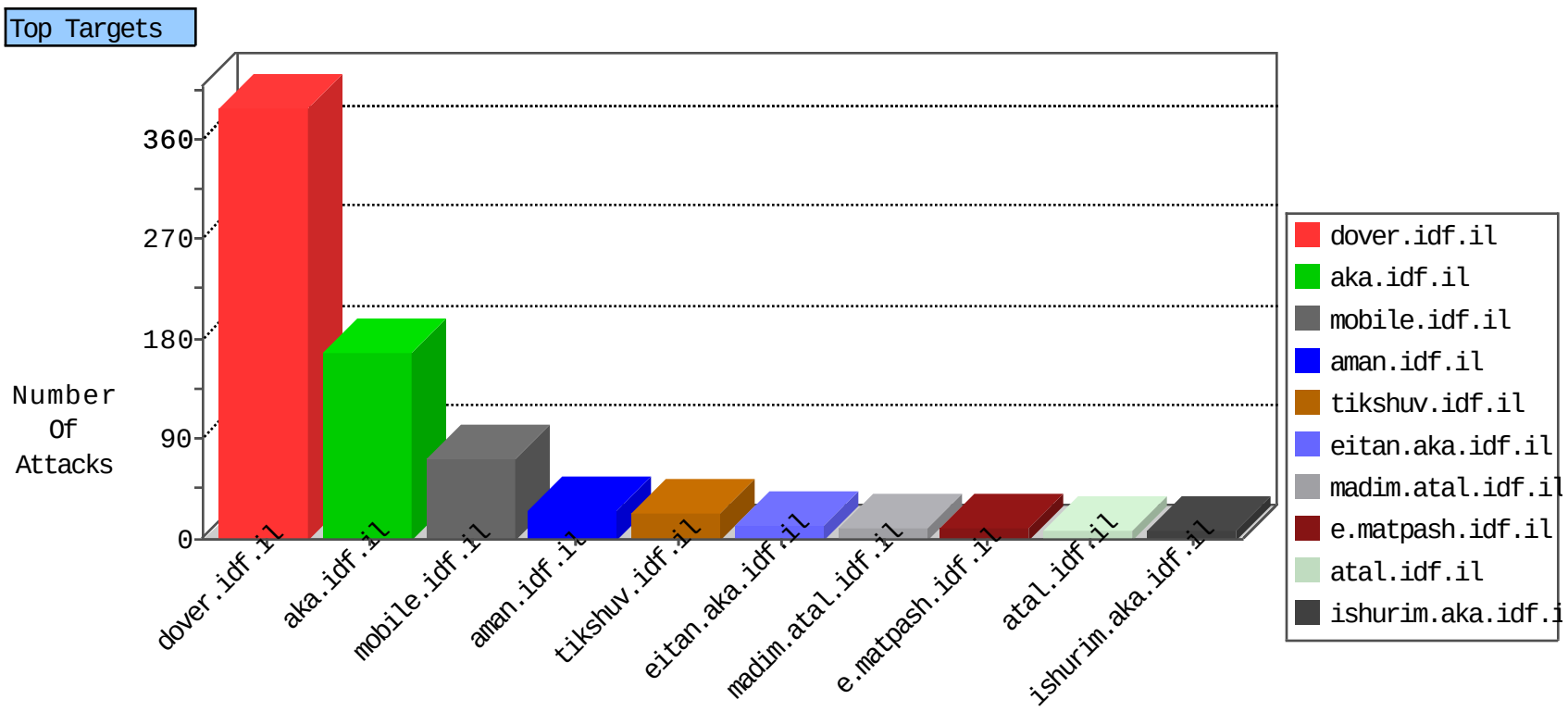
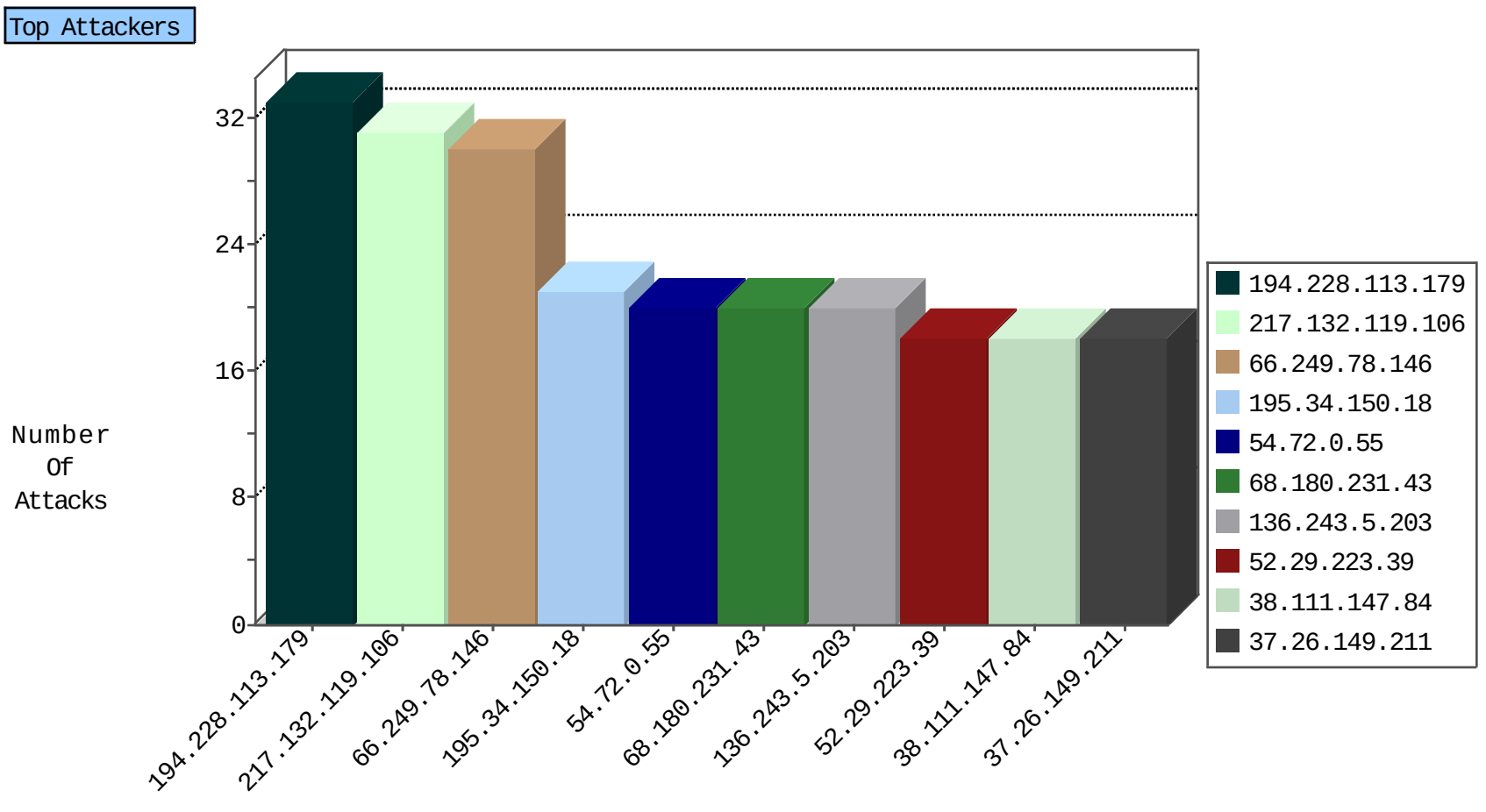
04-29-2016-11:04:00 to 04-29-2016-12:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-11:04:00 to 04-29-2016-12:04:00

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	DOS-Tool-SwitchbladG	dest-reset	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
219.255.42.89	Korea, Republic of	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
139.196.8.79	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.84	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.85	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

04-29-2016-11:04:00 to 04-29-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-11:04:00 to 04-29-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
1.187.26.174	147.237.77.19	India	law-forum.idf.il	GPL SCAN nmap TCP	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sA (2)	2
91.216.3.130	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.17.100.16	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.240.139	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.219.125.17	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.170	Nicaragua	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
161.202.120.149	147.237.77.234	Japan	halag.idf.il	ET SCAN Potential SSH Scan	1
110.138.129.109	147.237.0.33	Indonesia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.17.100.16	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.170	Nicaragua	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
185.103.252.11	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
122.3.133.57	147.237.76.42	Philippines	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-29-2016-11:04:00 to 04-29-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.228.113.179	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
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
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
62.202.183.233	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.132.119.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
217.132.39.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.28.23	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
70.198.203.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
97.74.24.187	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.213	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.41.122	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.227.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.105.76.180	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.37.194.144	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.41.122	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.128.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.101	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
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.21.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.172.254.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.186.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-11:04:00 to 04-29-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.119.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	19
109.67.219.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
149.78.7.185	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.154.162.140	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
195.154.59.69	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
5.28.167.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
195.154.162.140	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.154.162.140	Block	2
149.88.213.236	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.88.213.236	Block	2
176.106.40.252	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.106.40.252	Block	2
37.26.149.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.132.39.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.15.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms/aspx	Block	1
51.255.65.2	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
164.132.161.41	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/links.asp	Block	1
93.172.132.132	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx.	Block	1
79.182.80.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
54.189.220.2	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter ForumId	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
149.88.213.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
80.246.139.200	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
54.203.211.102	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
176.106.40.252	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
77.126.24.177	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
195.154.162.140	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
151.80.31.179	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/↑	Block	1
84.94.61.61	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.28.167.247	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.28.167.247	Block	1
141.212.122.161	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
46.120.135.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
157.55.2.174	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.93.99	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sachar/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/63017.doc	Block	1
195.154.162.140	France	147.237.77.216	dover.idf.il	Admin Blocking	Block	1

04-29-2016-11:04:00 to 04-29-2016-12:04:00