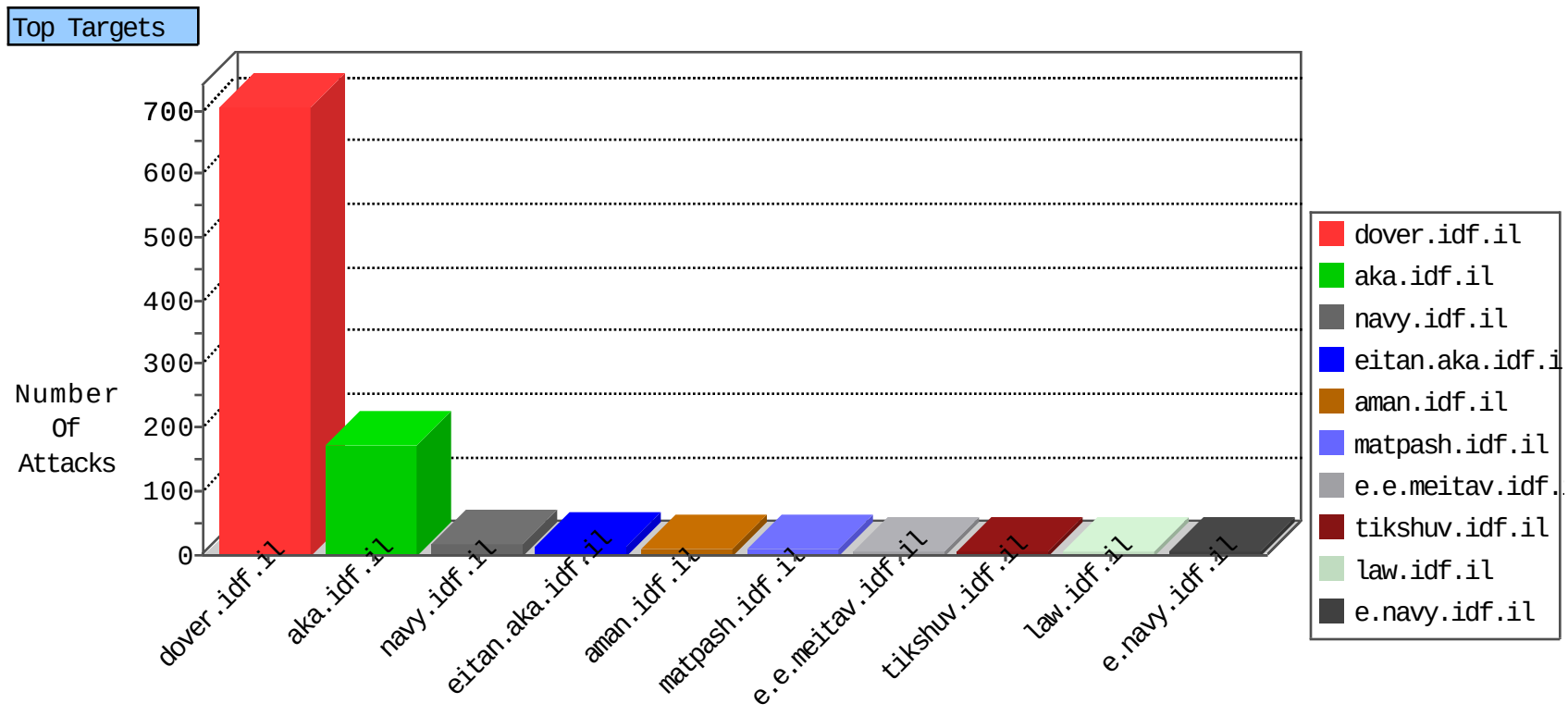
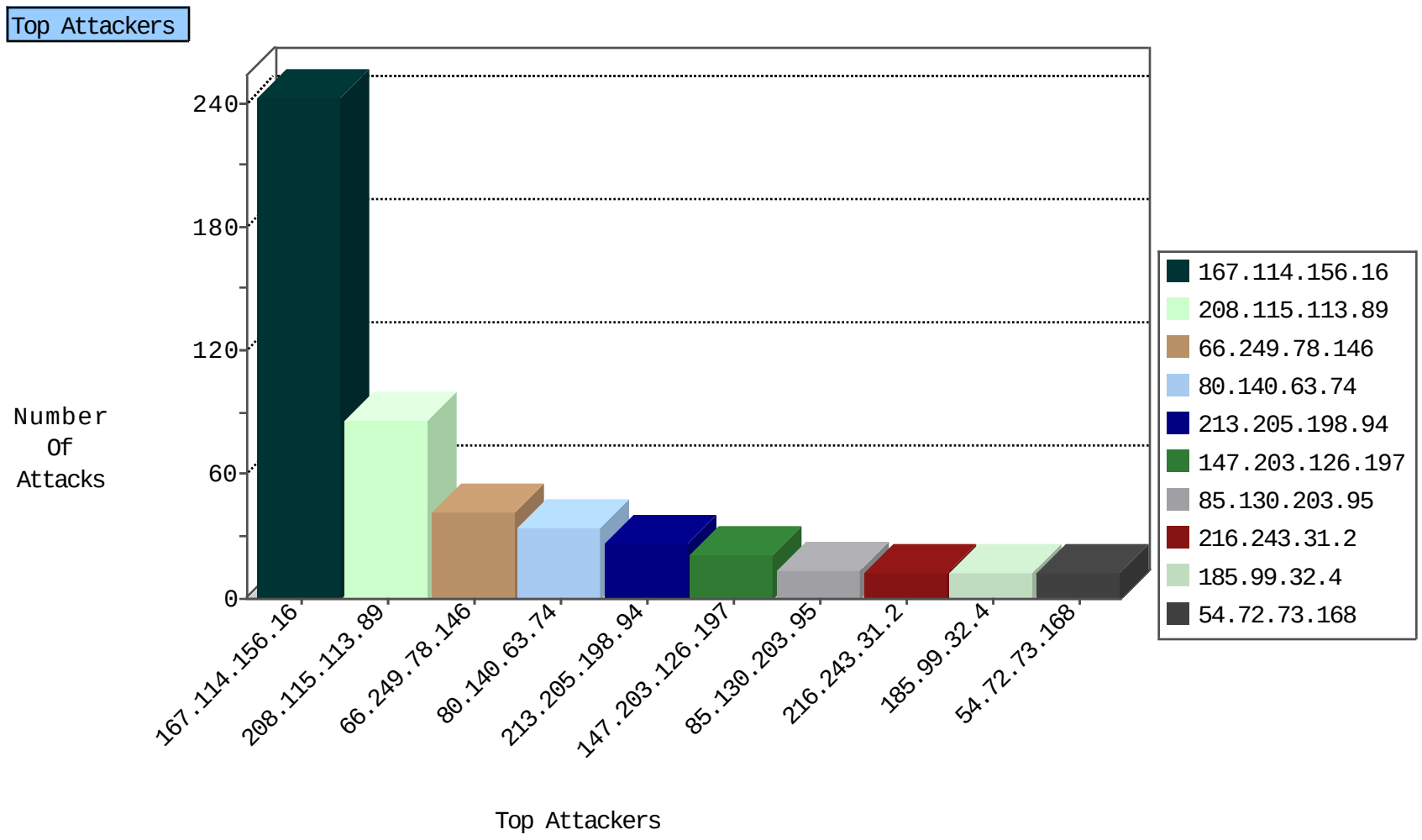
04-26-2016-23:04:08 to 04-27-2016-00:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-23:04:08 to 04-27-2016-00:04:08

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	9859
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2808
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	12
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.48	Lithuania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.48	Lithuania	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
207.244.166.154	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
185.130.5.48	Lithuania	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
5.102.197.45	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
185.130.5.48	Lithuania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.48	Lithuania	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

04-26-2016-23:04:08 to 04-27-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-23:04:08 to 04-27-2016-00:04:08

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
96.237.50.37	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.13.60	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.240.213.93	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
187.160.94.228	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.245.177	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -f -sS	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
117.20.41.62	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
96.237.50.37	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
96.237.50.37	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.13.60	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.245.177	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1
183.60.252.84	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
177.231.203.88	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
104.219.238.10	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-23:04:08 to 04-27-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
80.140.63.74	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
213.205.198.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
147.203.126.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.99.32.4	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.33.122.121	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.95.205.13	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.166.162.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.86.83.56	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.129.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
198.58.102.95	United States	147.237.77.216	dover.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	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
67.68.181.12	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.203.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.160.168.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.179.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
69.120.110.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
88.224.108.13	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
157.55.12.79	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
201.212.5.12	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.8.127.42	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
86.211.183.128	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
201.212.5.12	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.130.203.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.145.218.186	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.183.62.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
201.212.5.12	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
200.4.25.109	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.205.198.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.117.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.120.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.221.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.205.10.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
82.166.247.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/faq/mobile	Block	4
79.178.175.106	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.178.175.106	Block	3
2.53.156.78	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
217.132.49.109	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/lobby/lobby.aspx	Block	3
104.155.92.247	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
104.155.92.247	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	2
95.86.80.233	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2414.jpg	Block	1
136.243.48.84	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
89.139.10.158	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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
37.26.147.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
213.151.38.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/319,	Block	1
104.155.92.247	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
79.178.175.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
2.53.8.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/general/mobile	Block	1
141.161.13.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
89.139.10.158	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 89.139.10.158	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	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
217.132.49.109	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.law.idf.il/421-he/patzar.aspx	Block	1
104.155.92.247	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
79.179.213.180	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.75.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.27	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
94.199.151.22	United Kingdom	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 94.199.151.22	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/about_israel.asp	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
204.79.180.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.199.151.22	United Kingdom	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
71.244.112.136	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.64.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId\u003d58624 in www.aka.idf.il/main/giyus/general.aspx	None	1
31.168.16.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-26-2016-23:04:08 to 04-27-2016-00:04:08