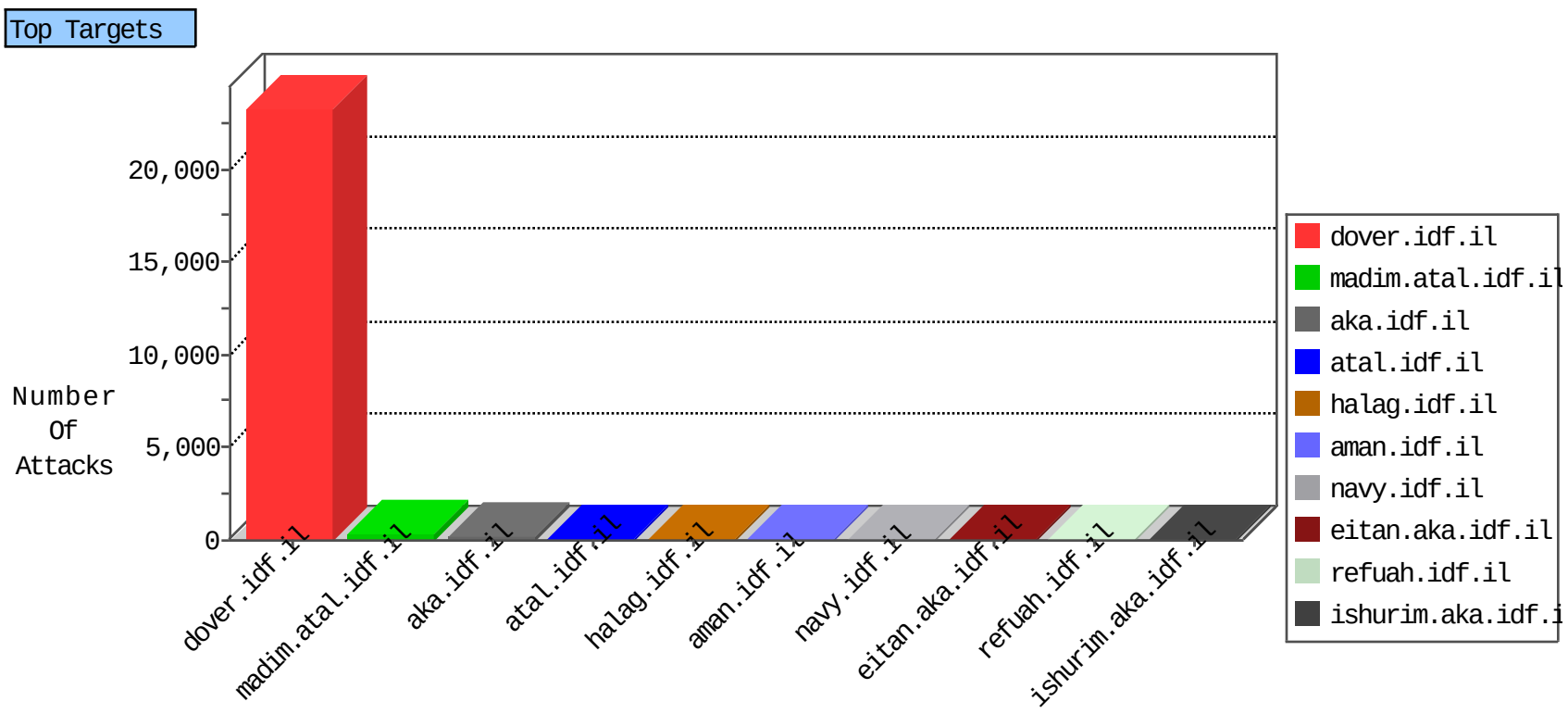
09-12-2016-21:04:04 to 09-12-2016-22:04:04

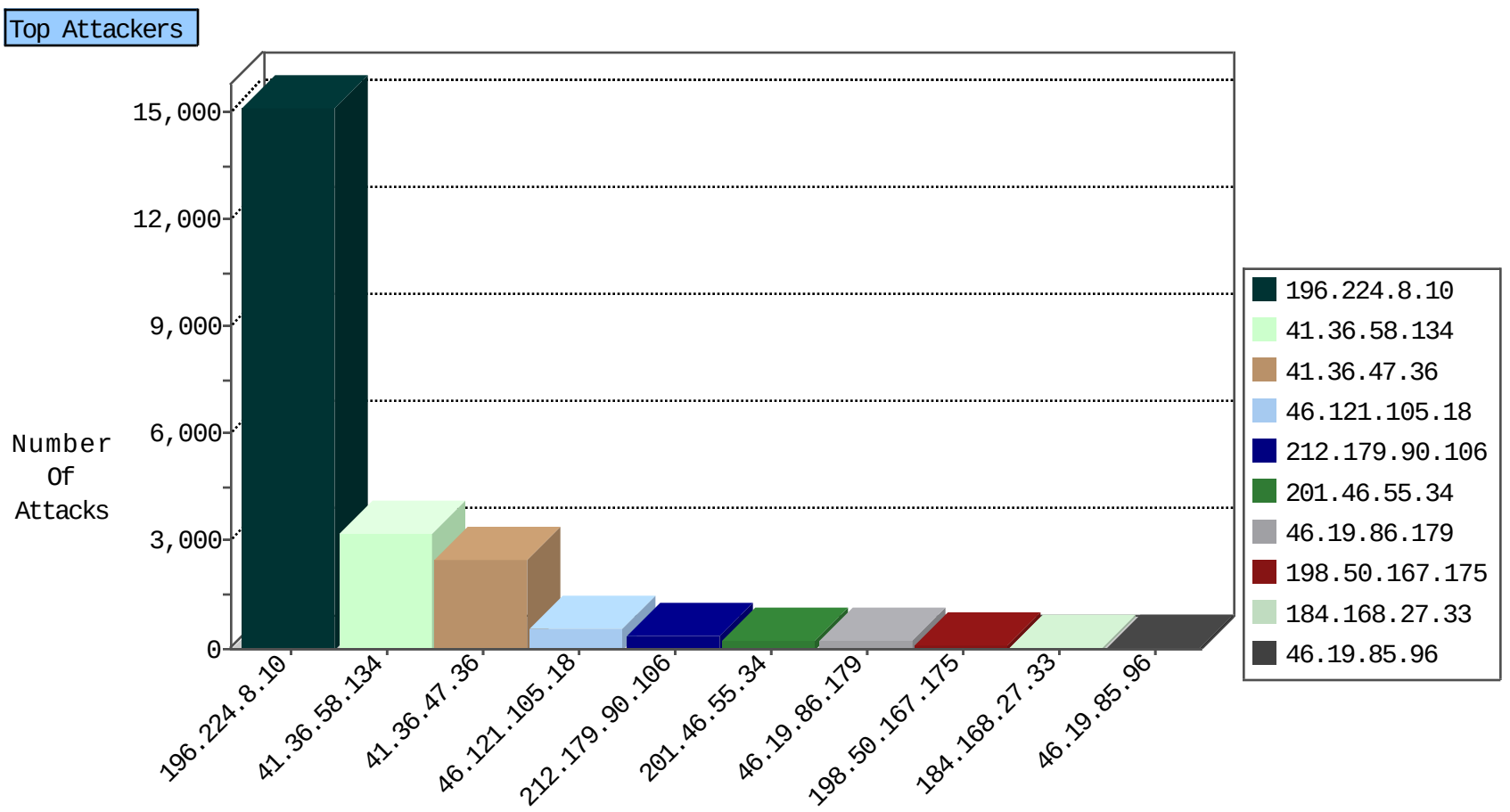
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-12-2016-21:04:04 to 09-12-2016-22:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
196.224.8.10	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.208.4.99	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.41	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
217.132.2.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.83	Czech Republic	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-21:04:04 to 09-12-2016-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.27.33	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
77.67.47.7	France	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
198.50.200.198	Canada	147.237.72.166	aka.idf.il	C1000026: HTTP: Access to - index.php?option=com_jce	Permit	8
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.33	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
77.67.47.7	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-12-2016-21:04:04 to 09-12-2016-22:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.27.33	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	26
77.67.47.7	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	20
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
194.15.116.205	147.237.77.216	Russian Federation	dover.idf.il	Xenu Link Sleuth User Agent	2
45.79.103.178	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
71.6.165.200	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
46.254.9.91	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
41.36.47.36	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
183.239.198.105	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
103.207.36.84	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
71.6.165.200	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
46.254.9.91	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
202.103.177.162	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.254.9.91	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.239.198.105	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
183.239.198.105	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
93.174.91.29	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

09-12-2016-21:04:04 to 09-12-2016-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
196.224.8.10	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15114
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2794
41.36.47.36	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2348
46.121.105.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	563
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	380
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	359
41.36.47.36	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	107
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	36
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.149.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
156.204.212.202	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.253.193.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
194.90.247.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.186.81.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
37.142.99.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
89.237.110.147	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.253.145.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.178.132.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.180.22.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.182.32.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.76.111.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	14
2.53.160.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.96	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
196.224.8.10	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.96	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.253.192.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
31.154.25.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.142.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
196.224.8.10	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
68.180.229.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
5.22.134.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.182.57.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
201.46.55.34	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
176.13.10.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.132.66.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

09-12-2016-21:04:04 to 09-12-2016-22:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	210
89.138.185.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	17
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
192.114.91.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
5.29.118.55	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.147.172	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 37.26.147.172	Block	4
77.127.78.97	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation searchText in www.tikshuv.idf.il/905-he/tikshuv.aspx	Block	2
176.13.5.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.235.66.84	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
77.126.40.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/default.aspx	None	1
161.209.206.201	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
79.179.125.59	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
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/sachar/	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
79.179.125.59	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.179.125.59	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
212.179.220.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.237.74.146	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
77.138.15.199	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
185.120.125.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.137.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.124.20.14	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Value at 101 for www.aman.idf.il/modiin/questionnaires.aspx	Block	1
46.19.86.37	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.142.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.70.210	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/kamlar/home/default.asp	Block	1
5.29.118.55	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
81.218.136.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
77.126.40.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspxcatId=58609&docId=72568	Block	1
77.138.193.58	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
47.54.146.126	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
32.60.95.34	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
87.68.38.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

09-12-2016-21:04:04 to 09-12-2016-22:04:04