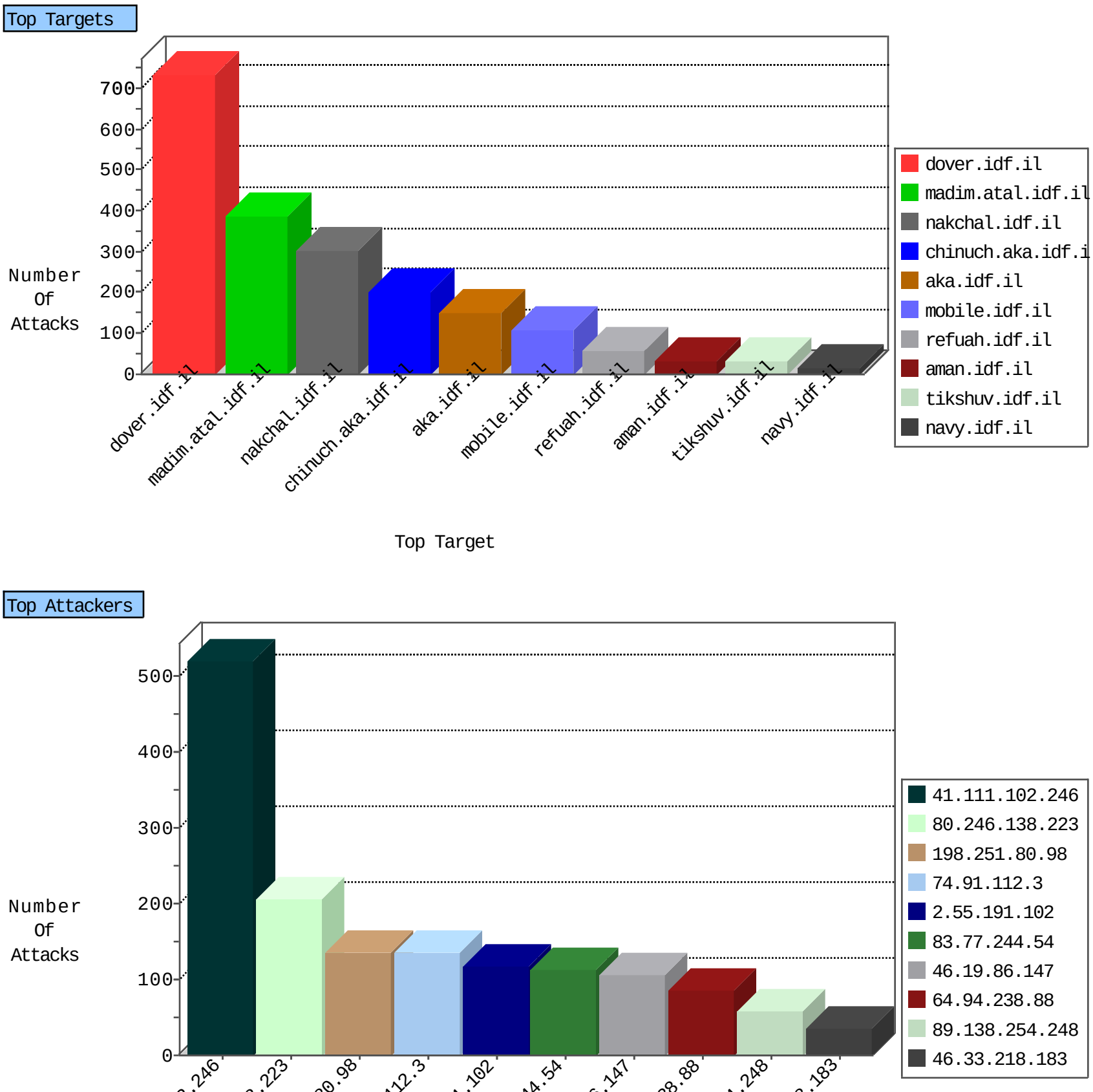
09-27-2016-23:04:05 to 09-28-2016-00:04:05

IDF Under Attack Daily Report



09-27-2016-23:04:05 to 09-28-2016-00:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.125.58.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.249.69.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

09-27-2016-23:04:05 to 09-28-2016-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
5.9.89.170	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-27-2016-23:04:05 to 09-28-2016-00:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
124.197.95.73	147.237.76.86	Singapore	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
66.249.76.10	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
27.54.62.253	147.237.0.16	Singapore	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
211.141.78.56	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
1.54.210.7	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.61	Cote D'Ivoire	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
139.59.28.44	147.237.77.179	Singapore	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.138.223	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
1.54.210.7	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
202.155.58.28	147.237.77.179	Indonesia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.61	Cote D'Ivoire	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
149.255.108.192	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1

09-27-2016-23:04:05 to 09-28-2016-00:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	242
64.94.238.88	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	51
109.253.222.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
46.19.86.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
84.226.41.158	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
46.19.86.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
74.91.23.166	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
84.180.120.54	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
77.139.143.150	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.86.147	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.33.218.183		147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
109.253.222.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.28.154.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
176.13.237.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.196.5	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.33.218.183		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
85.130.196.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.67.143.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
77.139.143.150	France	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
109.67.143.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.206.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

09-27-2016-23:04:05 to 09-28-2016-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.111.102.246	Block	225
80.246.138.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
2.55.191.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
89.138.254.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
98.245.86.75	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	4
77.139.131.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	4
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 41.111.102.246	Block	3
79.178.150.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 41.111.102.246	Block	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed URL from 41.111.102.246	Block	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 41.111.102.246	Block	3
2.55.45.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 41.111.102.246	Block	3
79.181.32.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 41.111.102.246	Block	3
109.253.206.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.138.81.74	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
5.28.154.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.222.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
166.137.139.15	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
176.13.237.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
180.76.15.143	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
66.102.9.5	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	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Data in URL	Block	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 1	Block	1
77.138.162.143	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
207.46.13.176	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
103.27.126.210	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.142.3.37	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
79.180.96.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.32	Block	1
157.55.39.28	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
84.109.118.53	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Malformed URL -	Block	1
77.138.162.143	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	1
2.53.191.86	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
103.27.126.210	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
79.180.103.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.125.56.161	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.117.30.93	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.111.227.174	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
217.33.23.241	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
66.249.69.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
109.253.197.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

09-27-2016-23:04:05 to 09-28-2016-00:04:05