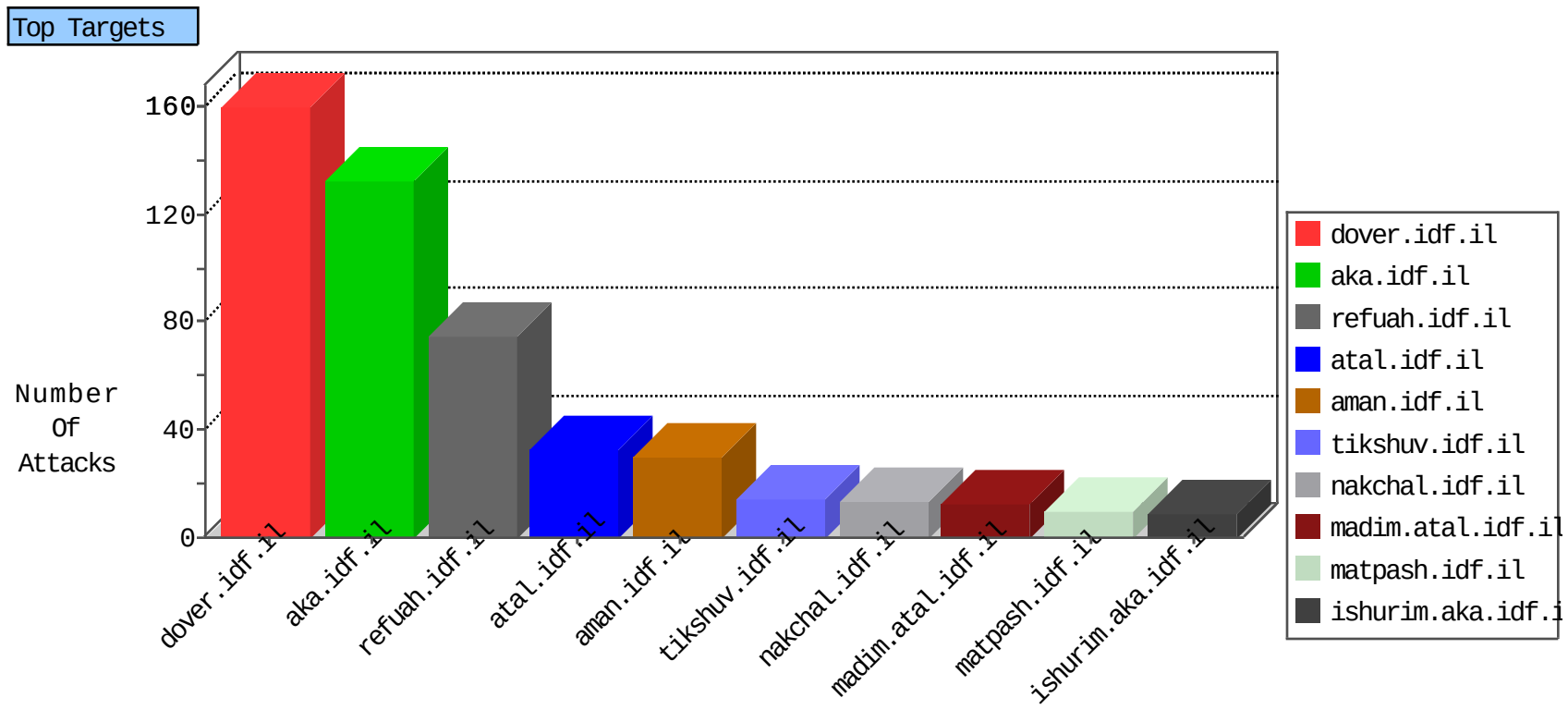
09-14-2016-00:04:06 to 09-14-2016-01:04:06

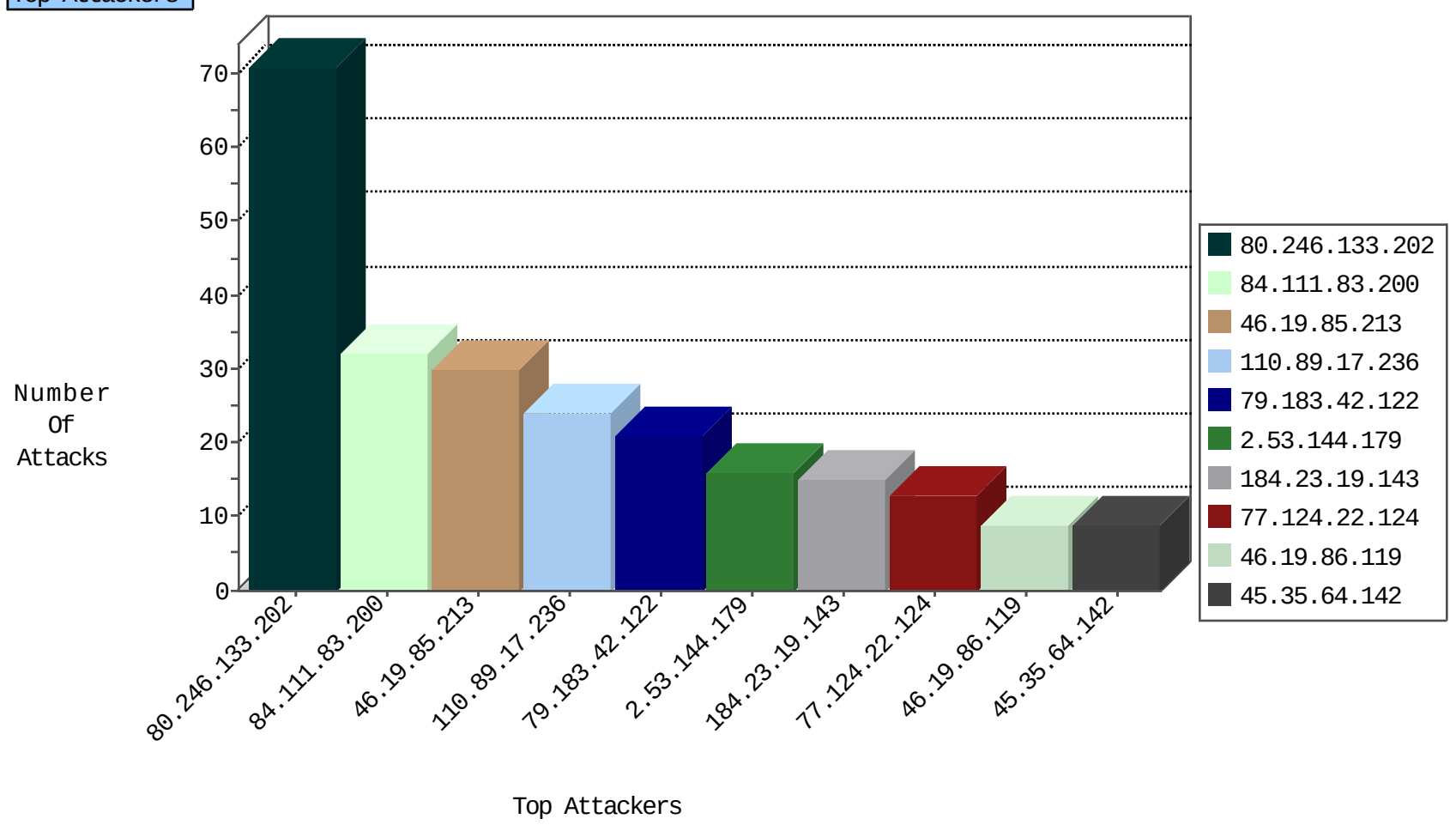
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-14-2016-00:04:06 to 09-14-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	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	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	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
200.19.159.35	Brazil	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
211.1.156.90	Japan	147.237.72.156	aman.idf.il	JLM_Purple_Con_Limit_Http	drop	1
195.209.126.50	Russian Federation	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
130.206.158.138	Spain	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
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
219.138.216.129	China	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
195.209.126.50	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
193.1.13.14	Ireland	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
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-00:04:06 to 09-14-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.200	eitan.aka.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1

09-14-2016-00:04:06 to 09-14-2016-01:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.0.253	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
52.166.249.197	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
190.253.144.9	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.161.173.106	147.237.72.217	Mexico	e.idf.il	ET SCAN NMAP -sS window 3072	1
177.200.192.51	147.237.77.178	Brazil	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.129.15	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.161.173.106	147.237.72.217	Mexico	e.idf.il	ET SCAN NMAP -sS window 4096	1
188.0.236.165	147.237.77.179	Moldova, Republic of	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
177.200.192.51	147.237.77.178	Brazil	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1

09-14-2016-00:04:06 to 09-14-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
84.111.83.200	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.213	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.16.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
1.144.96.162	Australia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.144.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
184.23.19.143	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
79.183.42.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.144.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.42.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.183.42.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.42.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.183.42.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.67.42.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.171.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
109.253.132.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.244.72.69	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.244.72.69	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.17.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.120.122.219	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	4
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.213	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.144.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.147.177	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
186.129.187.118	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
176.13.4.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.23.19.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.194.67.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.3.147.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
178.134.63.55	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
77.127.41.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
87.69.79.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
184.23.19.143	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.244.86.122	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
87.69.79.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

09-14-2016-00:04:06 to 09-14-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.89.17.236	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 110.89.17.236	Block	17
77.124.22.124	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	13
109.253.193.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
110.89.17.236	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
80.246.136.106	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
176.13.227.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.254	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.4.254	Block	2
176.13.4.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1709	Block	2
109.67.204.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
114.97.198.63	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.97.198.63	Block	2
66.147.244.101	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
106.184.21.179	Japan	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
5.102.206.92	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.76.15.141	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
110.89.17.236	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
220.181.51.105	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
46.116.199.195	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
185.27.106.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/1528.png	Block	1
83.219.136.156	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
79.176.49.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/fgiyus/kiosk/kiosk.aspx	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
114.97.198.63	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/cogat.aspx/trackback/	Block	1
84.111.83.200	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	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
176.14.130.138	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
80.246.133.164	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 198.161.119.4 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
84.111.164.30	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.251	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
5.102.206.92	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.102.206.92 (Open Mode)	None	1
178.134.63.55	Georgia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/login/	Block	1
80.246.133.202	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
204.79.180.62	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method 488 in URL	Block	1

09-14-2016-00:04:06 to 09-14-2016-01:04:06