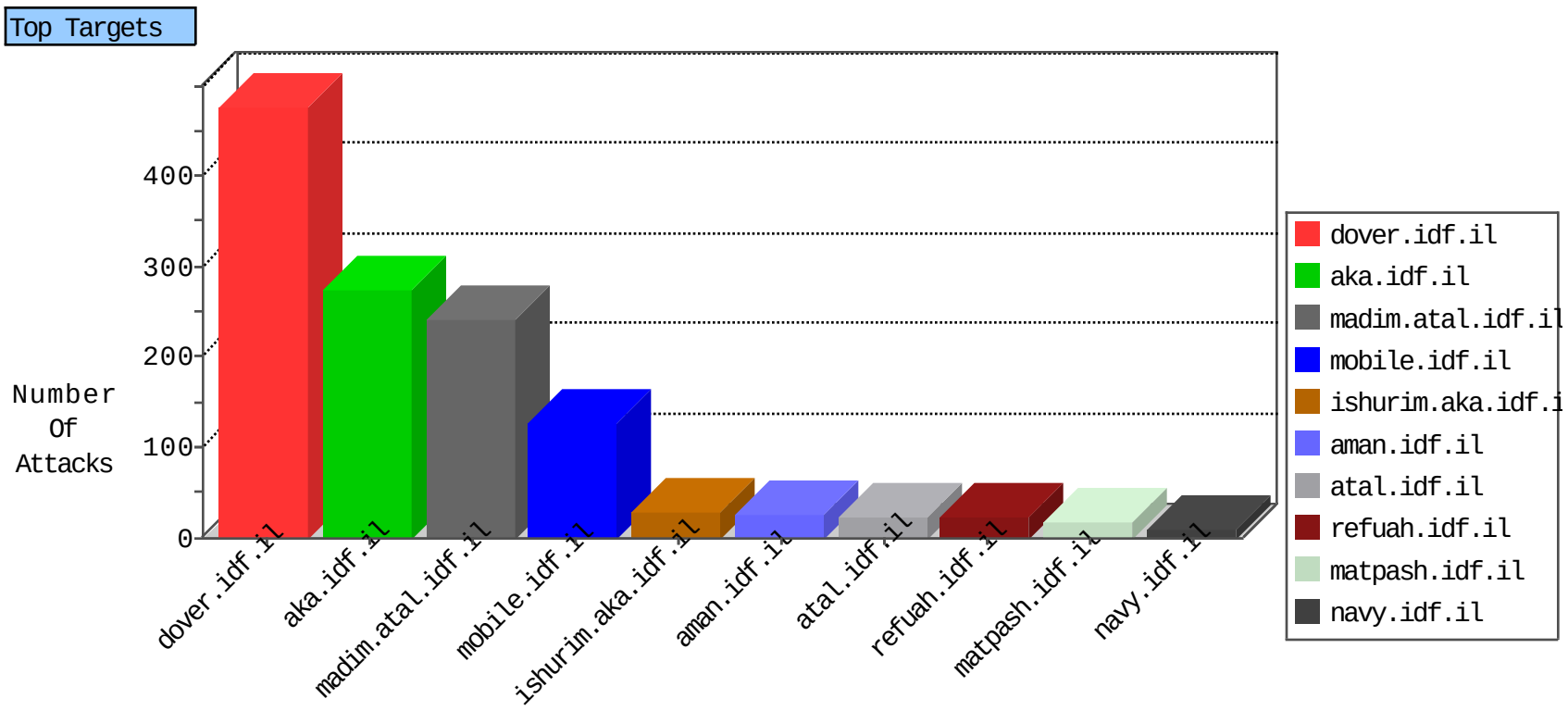
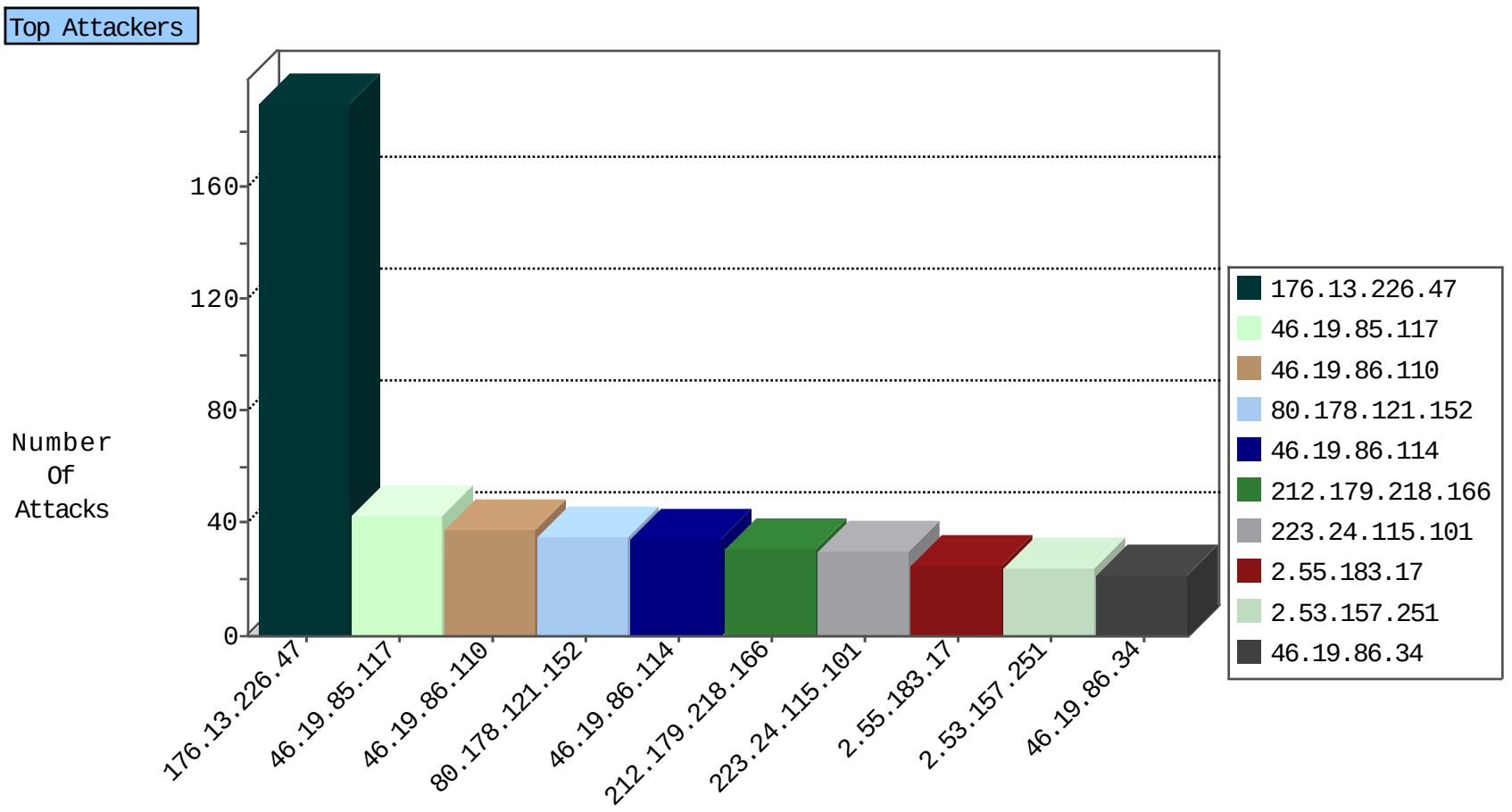
09-29-2016-13:04:02 to 09-29-2016-14:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-13:04:02 to 09-29-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.95.103.71	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	54
132.68.52.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
197.33.83.128	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.7.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
173.208.198.14	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
192.187.118.21	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
69.30.227.218	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
2.53.190.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.102.253.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
155.91.102.182	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
69.30.193.250	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
31.168.133.226	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
213.57.27.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
173.0.52.105	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
198.44.110.12	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
173.208.213.196	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
192.187.118.21	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
173.208.150.116	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
69.30.227.222	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
198.204.255.74	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
142.54.180.68	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
63.141.231.210	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
173.208.150.118	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
31.168.64.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.204.255.76	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
198.44.110.12	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-29-2016-13:04:02 to 09-29-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.186	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-29-2016-13:04:02 to 09-29-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.242.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.239.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.195.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.46.103.70	147.237.76.30	India	himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.55.157.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.142.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.210.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.199.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.218.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.84.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.175.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.129.160.229	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.84.174	147.237.72.167	Israel	ishurim.aka.idf.i	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.165.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.27.116.133	147.237.77.233	China	atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
2.53.45.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.108.95.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.160.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.32.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.175.125.51	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-13:04:02 to 09-29-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
223.24.115.101	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.126.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
82.145.220.255	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.157.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
62.0.214.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.94.193.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
80.178.121.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.178.121.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
37.26.148.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.114	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.114	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.158.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
212.179.218.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.0.214.129	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.223.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.225.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.55.12.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.178.121.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
80.178.121.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.197.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.55.183.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.46.39.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.141.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.47.36	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.226.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.227.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.8.122.115	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
109.253.205.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.63	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.170.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-29-2016-13:04:02 to 09-29-2016-14:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.226.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	188
176.13.225.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.149.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.157.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.213.17.10	Russian Federation	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
95.35.75.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
152.62.109.206	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	5
77.138.67.130	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	4
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
152.62.109.206	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
109.253.193.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.206.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.59.195.197	Denmark	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
176.13.248.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	3
109.253.144.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	2
109.66.176.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.150.25.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishorim	Block	2
80.246.139.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.32.110	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
82.80.170.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.226.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.12.89	France	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.63	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
31.154.81.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage	Block	1
77.139.105.215	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
177.32.124.203	Brazil	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
37.142.233.253	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.118.100.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/113777.pdf	Block	1
85.186.64.60	Romania	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
2.55.141.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.239.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
157.55.39.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
109.64.124.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/0	Block	1
77.139.118.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/	Block	1
180.76.15.24	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9699-he/refuah.aspx	Block	1
176.13.14.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	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
2.55.166.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1

09-29-2016-13:04:02 to 09-29-2016-14:04:02