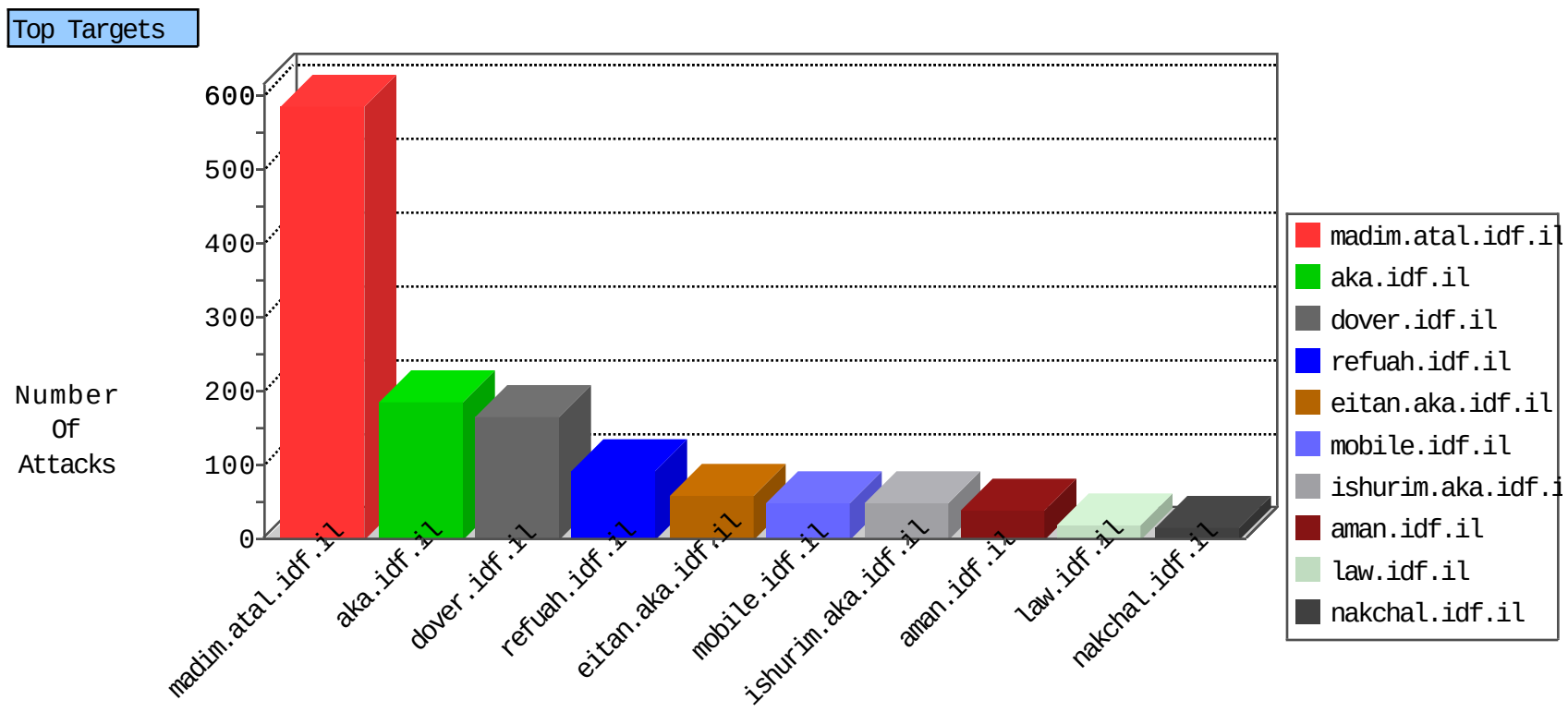
09-15-2016-11:04:03 to 09-15-2016-12:04:03

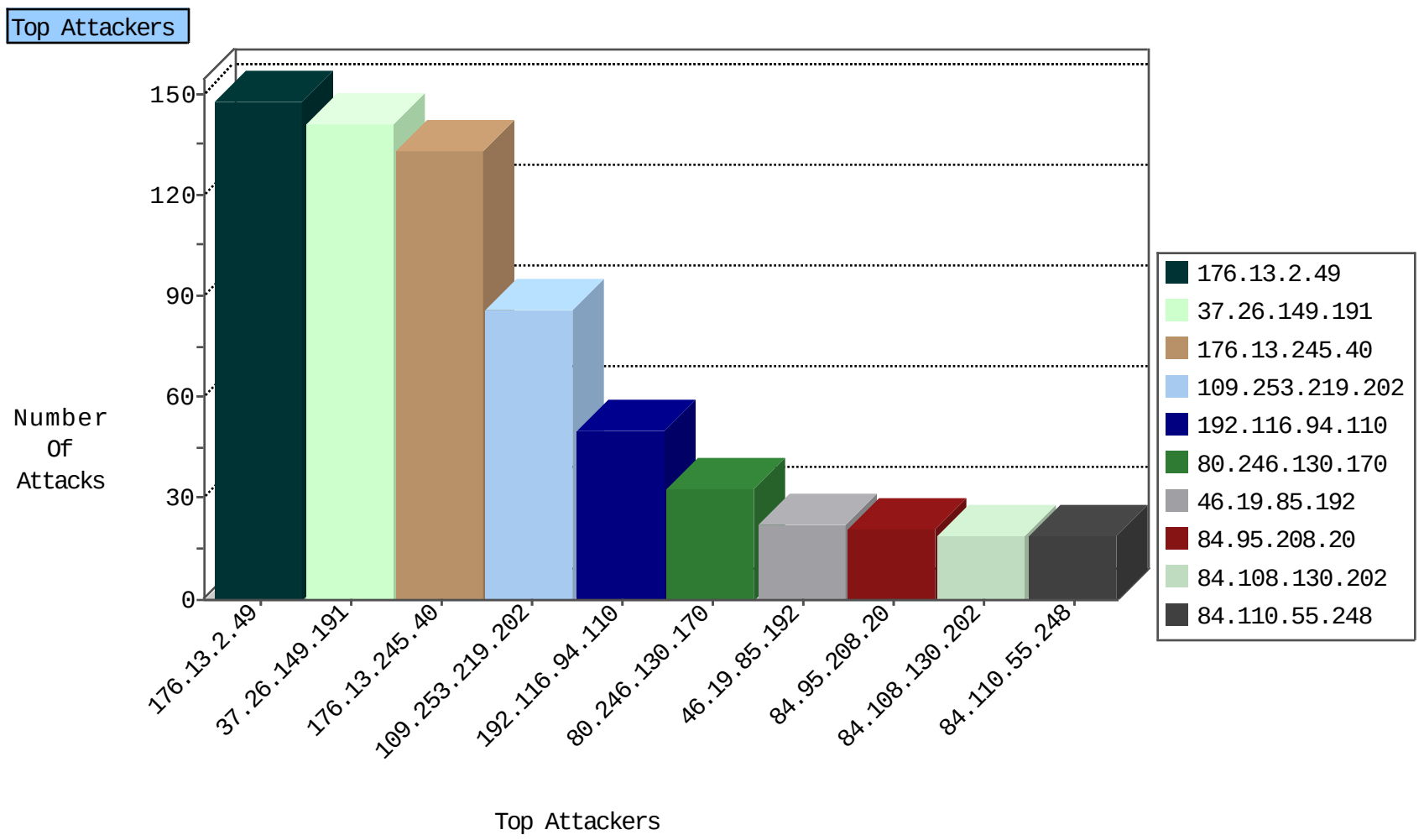
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-15-2016-11:04:03 to 09-15-2016-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	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
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.138	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
129.110.125.52	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.166	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
164.107.127.12	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
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
170.140.119.70	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-11:04:03 to 09-15-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.190	Netherlands	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-15-2016-11:04:03 to 09-15-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
49.14.91.173	147.237.76.31	India	nakchal.idf.il	GPL SCAN nmap TCP	4
46.19.85.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.154.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.162.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.215.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.227.165.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.93.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.74.100.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.139.8.215	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.244.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
109.64.138.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.134.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.234.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.160.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.126.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-15-2016-11:04:03 to 09-15-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.116.94.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
80.246.130.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
84.110.55.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.108.130.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.219.225.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.10.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
62.90.220.150	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
62.0.225.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.127	Israel	147.237.77.74	law.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.177.7.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.252.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.55.48.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.48.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
111.91.6.106	India	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
80.178.150.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
157.55.39.19	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.131.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.109.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.107.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.222.1	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
62.0.222.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.7.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.117.107.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
62.219.225.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
89.139.215.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.39.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.223.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.235.98.139	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
93.173.62.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.235.112.216	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
109.253.137.255	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.169	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
111.91.6.106	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.55.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
111.91.6.106	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.108	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-15-2016-11:04:03 to 09-15-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
176.13.245.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
109.253.219.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.15.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.146.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.108.130.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
82.166.181.20	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
2.55.10.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.242.235	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.242.235	Block	2
2.53.131.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.242.235	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
176.13.18.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
117.200.219.54	India	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
176.13.233.222	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/div.item	Block	1
80.110.26.244	Austria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.202	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
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/default.aspx	Block	1
109.226.14.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
37.26.147.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.24.207.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
2.53.40.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
82.166.181.20	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 82.166.181.20	Block	1
117.200.219.54	India	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method q[[#0]][[#0]][[#0]]&?FŽÄ?UÏwÜðê¯¤#012DßÄjïiu[[#22]]ç25[[#0]]8ruÒ#012ØoHmH_C	Block	1
68.180.229.155	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
217.118.83.158	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
2.55.10.104	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
80.246.130.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
162.247.97.162	Virgin Islands, British	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1

09-15-2016-11:04:03 to 09-15-2016-12:04:03