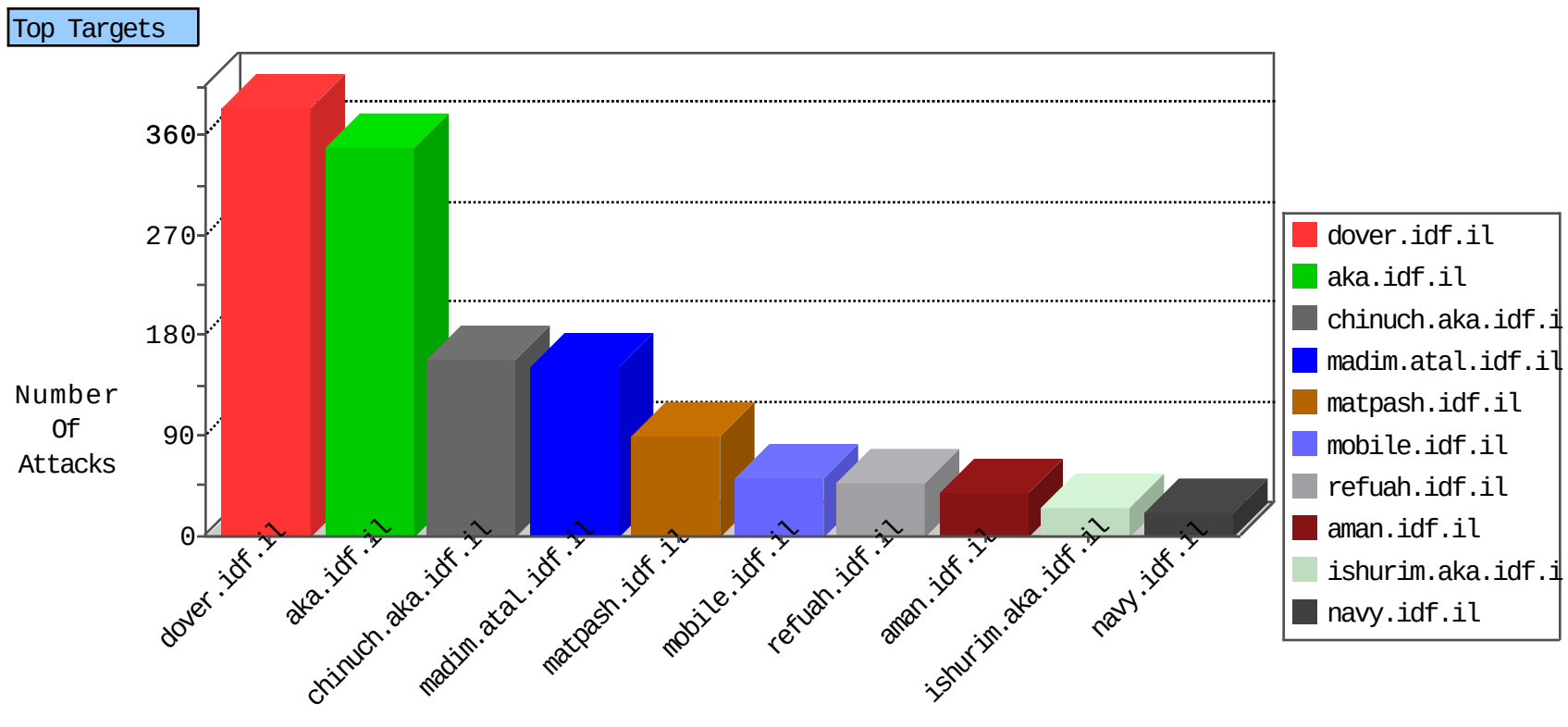
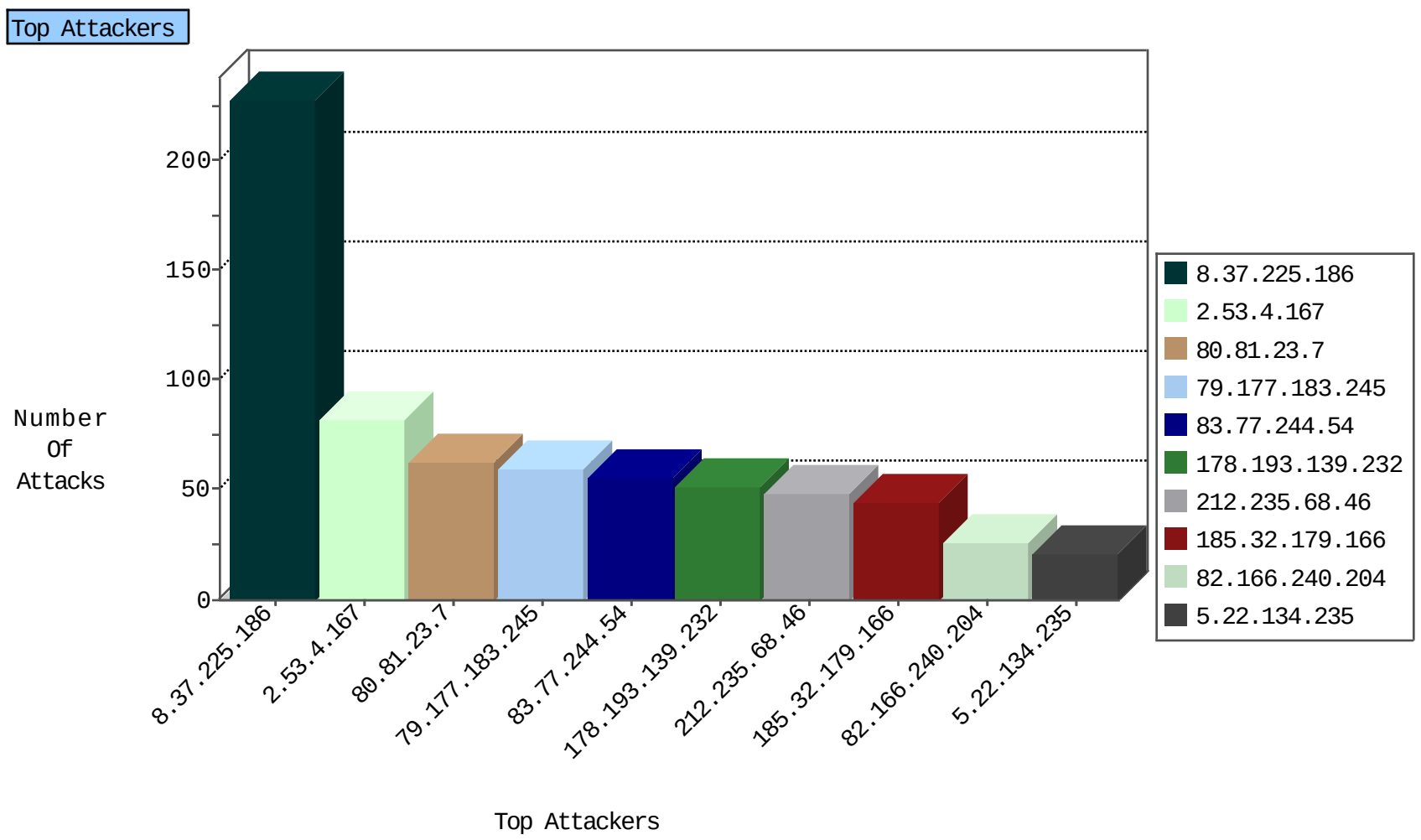
09-27-2016-19:04:01 to 09-27-2016-20:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-19:04:01 to 09-27-2016-20:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.77.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
8.37.225.186	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
109.253.208.90	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
183.60.48.25	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
77.138.33.151	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
71.6.158.166	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
5.28.174.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-27-2016-19:04:01 to 09-27-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.171	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-27-2016-19:04:01 to 09-27-2016-20:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
88.202.218.246	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
202.155.58.28	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.157	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.8.78.63	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -f -sS	1
66.249.93.158	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
202.155.58.28	147.237.0.35	Indonesia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.13	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.76.42	Latvia	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
24.173.213.138	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1

09-27-2016-19:04:01 to 09-27-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
8.37.225.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
80.81.23.7	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	63
8.37.225.186	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
79.177.183.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
79.177.183.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
212.235.68.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
212.235.68.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
5.22.134.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.32.179.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
185.32.179.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
185.32.179.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.86.236	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
213.57.237.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	12
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
2.53.14.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
46.19.86.73	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
2.53.21.91	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.178.148.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
168.103.118.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.177.30.130	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.74	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.177.30.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
213.57.87.62	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.253.135.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.143.41	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.253.196.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
80.246.139.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.168.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.234.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.63.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.148.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.223.189.140	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.157.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.246	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5

09-27-2016-19:04:01 to 09-27-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.4.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
82.166.240.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.13.232.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
77.138.26.59	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	5
2.53.161.69	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
23.109.37.250	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/'	Block	3
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.153.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.90.13.147	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
66.102.9.154	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	2
2.53.42.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.46.37.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.23	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
84.109.71.119	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 84.109.71.119 (Unknown SSL Session)	None	1
66.249.64.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/hebrew/asp/rec.asp	Block	1
77.139.38.191	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
46.19.85.71	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 docid in aka.idf.il/main/haredim/general.aspx	None	1
69.150.27.28	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
66.249.69.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/5.asp	Block	1
157.55.39.70	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage.asp	Block	1
84.109.71.119	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.64.151	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
77.139.199.184	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
76.10.176.221	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.69.18	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
83.220.237.49	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.124.64	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/6/שקופית 13	Block	1
85.65.32.188	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.64.166	Block	1
77.139.242.51	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
77.125.20.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	1
109.253.204.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
84.108.43.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.138.226.229	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.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
176.13.234.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1680	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
79.178.54.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.22.134.235	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

09-27-2016-19:04:01 to 09-27-2016-20:04:01