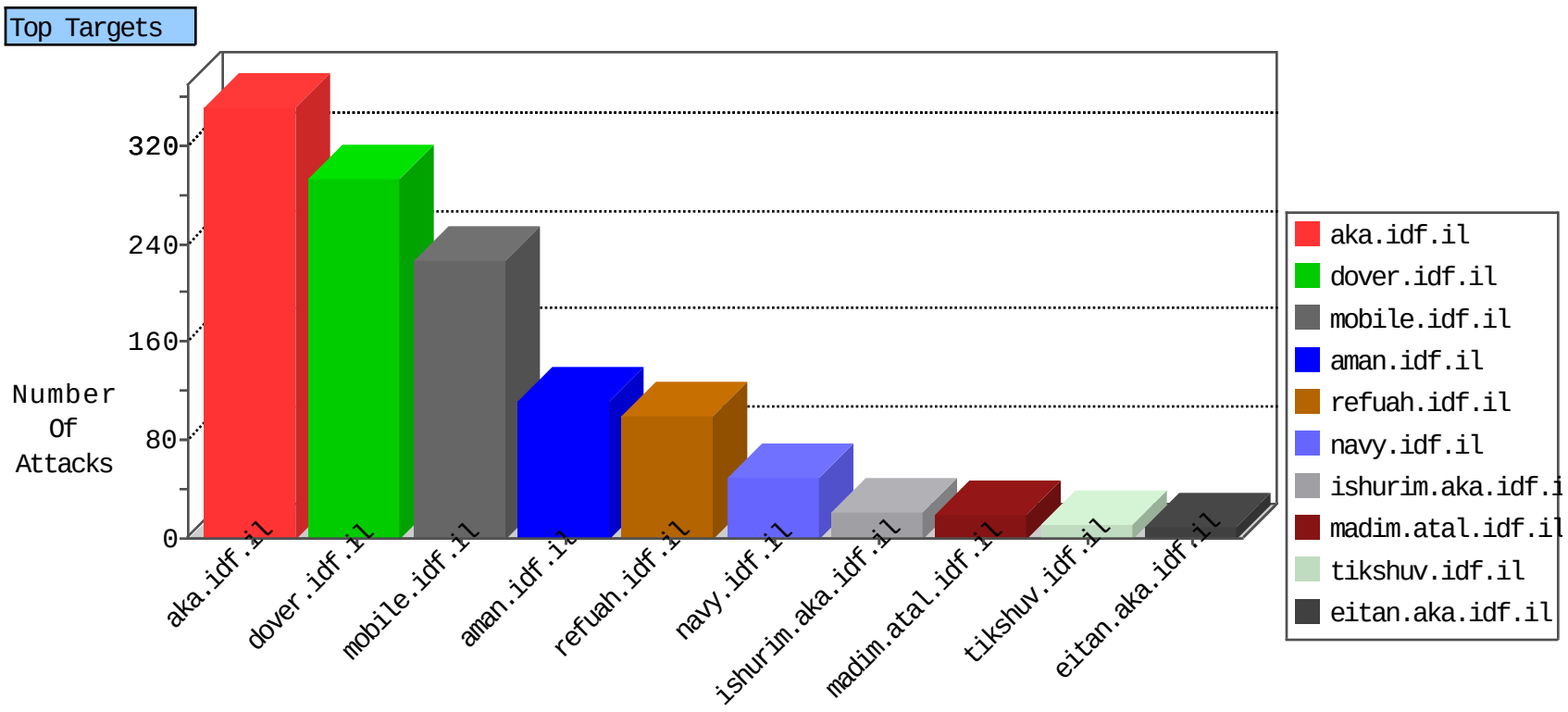
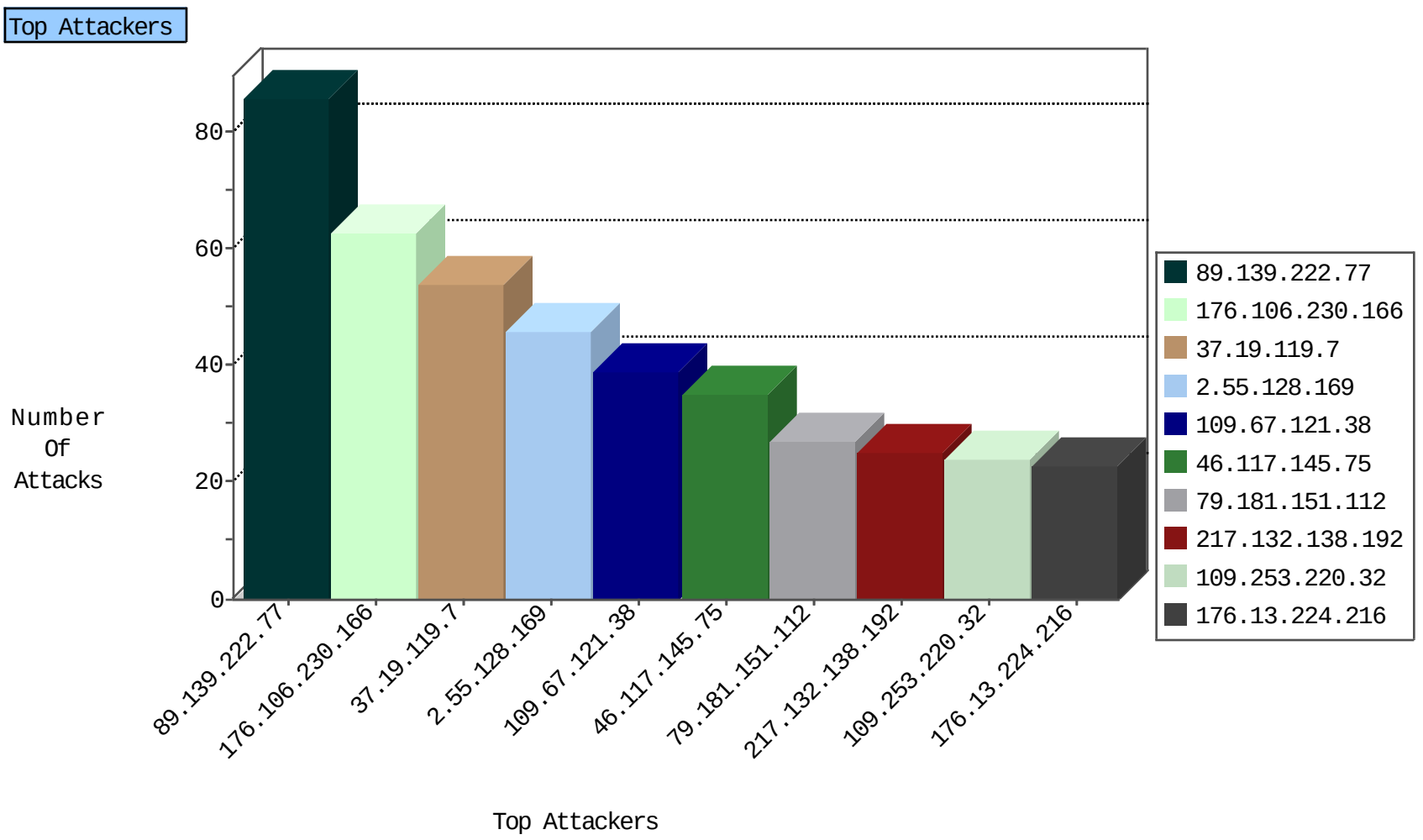
09-29-2016-19:04:03 to 09-29-2016-20:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-19:04:03 to 09-29-2016-20:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.168.2.30		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	3
2.53.134.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
192.187.118.20	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
192.187.101.234	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
173.208.150.117	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
192.187.109.62	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.227.220	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
63.141.250.156	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
85.65.247.48	Israel	147.237.72.166	aka.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	1
63.141.250.157	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
204.12.217.3	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
63.141.231.195	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
192.187.101.235	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
69.30.227.219	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
204.12.217.5	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
173.208.198.12	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
63.141.231.213	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1

09-29-2016-19:04:03 to 09-29-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-29-2016-19:04:03 to 09-29-2016-20:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.71.5.8	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
2.53.166.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
202.67.237.220	147.237.0.33	Hong Kong	idf.il	ET SCAN Potential SSH Scan	1
85.25.236.59	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.25.236.59	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.127.53.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.161.40.17	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
13.79.155.79	147.237.77.176	Ireland	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.37	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.25.236.59	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.138.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.81.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.161.40.17	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-29-2016-19:04:03 to 09-29-2016-20:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.106.230.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
37.19.119.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
109.67.121.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.117.145.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.181.151.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	23
89.139.222.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
89.139.222.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
176.13.224.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.229.11.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
147.235.8.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.220.32	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.55.128.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
80.246.136.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
100.92.235.225		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.55.128.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
89.139.222.77	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
2.55.128.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.55.128.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.220.32	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
217.132.138.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
176.13.235.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.253.212.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.172.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
195.60.235.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.210.185.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.67	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
84.94.59.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
147.235.8.67	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.239.10	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.161.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.52.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.195.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.145.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.189.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.56.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.108.152.81	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

09-29-2016-19:04:03 to 09-29-2016-20:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
80.179.202.129	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
176.13.224.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
89.237.76.125	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/faq.aspx	Block	5
46.117.145.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
37.19.119.7	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
176.13.231.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.57.161.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.23.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	2
213.151.36.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	2
89.139.172.244	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.212.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.56.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.9.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.145.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/67537.pdf	Block	1
46.19.85.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.134.2	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.80.216	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.121.253.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
89.139.122.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.52.6	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/klali.aspx	Block	1
77.126.7.18	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.151	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/y1cebowm67a	Block	1
109.253.195.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.107.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.53.180.117	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
77.138.80.216	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/klali.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/60900.pdf	Block	1
46.210.185.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.90.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.47.68	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
2.53.52.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.205.242.250	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
46.19.86.170	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
84.94.56.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.189.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.122.172	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/71511.pdf	Block	1
185.120.125.131	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
54.70.57.110	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/web-console/serverinfo.jsp	Block	1
89.139.222.26	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.178.179.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
37.142.8.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.57.157.177	Block	1

09-29-2016-19:04:03 to 09-29-2016-20:04:03