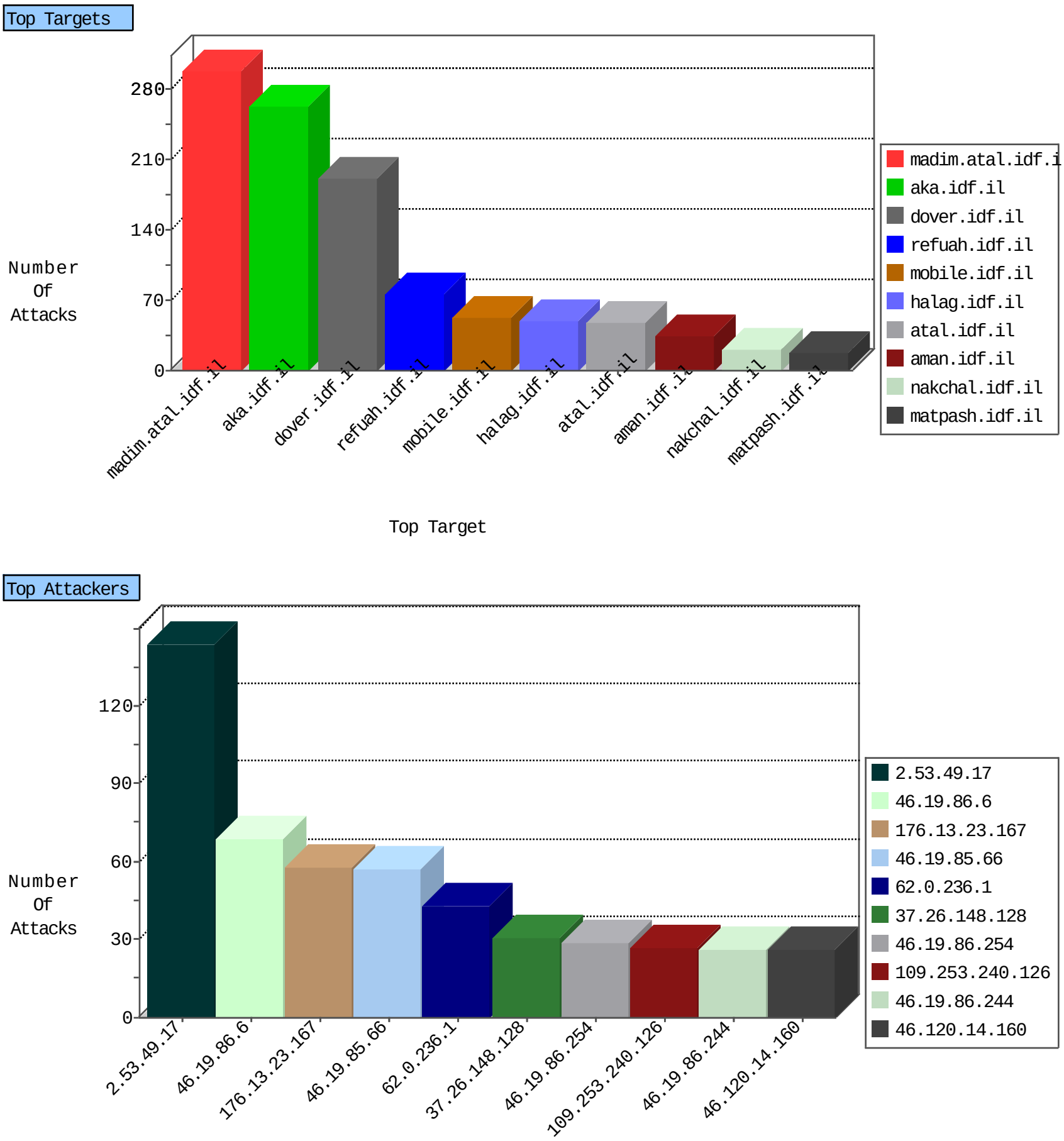
09-15-2016-09:04:00 to 09-15-2016-10:04:00

IDF Under Attack Daily Report



09-15-2016-09:04:00 to 09-15-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
87.68.42.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
153.90.1.34	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	6
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
2.55.7.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
211.1.156.90	Japan	147.237.72.167	ishurim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
211.1.156.90	Japan	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Http	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.67	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-09:04:00 to 09-15-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-15-2016-09:04:00 to 09-15-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.81.76.144	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1
200.98.129.125	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	1
79.177.53.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.98.129.125	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
200.98.129.125	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.73.66.166	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
2.53.2.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.115.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.46.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.251.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.159.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.183.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.40.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.98.129.125	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
62.219.136.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.98.129.125	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.160.222.18	147.237.0.200	South Africa	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.106.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.73.66.166	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.230.86.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.131.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.105.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.32.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-15-2016-09:04:00 to 09-15-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
46.19.86.6	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
46.19.85.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.120.14.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.55.13.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.6	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.53.15.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.237.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
81.218.66.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.120.14.160	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
176.13.251.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.53.0.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
62.0.202.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.238.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.48.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.101	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.53.0.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.19.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.64	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.99	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.251.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.145.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.88	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.183.28	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.127	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.188	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.127	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.90	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.99	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
81.218.118.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.32.179.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.5.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
95.35.71.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.13.194.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-15-2016-09:04:00 to 09-15-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.49.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
176.13.23.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
37.26.148.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.240.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.146.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
82.81.160.227	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
109.253.205.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.178.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.180.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.1.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.15.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.160.227	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/areceber	Block	2
77.138.186.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
213.151.43.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	2
109.226.21.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.19.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.150	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.186.151	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
46.19.86.33	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
81.218.37.2	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.218.37.2	Block	1
2.53.29.175	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
46.19.85.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.138.76.208	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.55.24.24	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
194.90.247.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
66.102.9.5	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
84.95.251.242	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
37.26.149.243	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
81.218.251.252	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
2.53.37.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
213.151.43.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.43.1	Block	1
46.19.86.254	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	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.22	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
104.128.144.131	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/redirect.php	Block	1
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.88	Block	1
37.142.11.45	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.142.11.45 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
81.218.251.252	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
176.13.23.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1

09-15-2016-09:04:00 to 09-15-2016-10:04:00