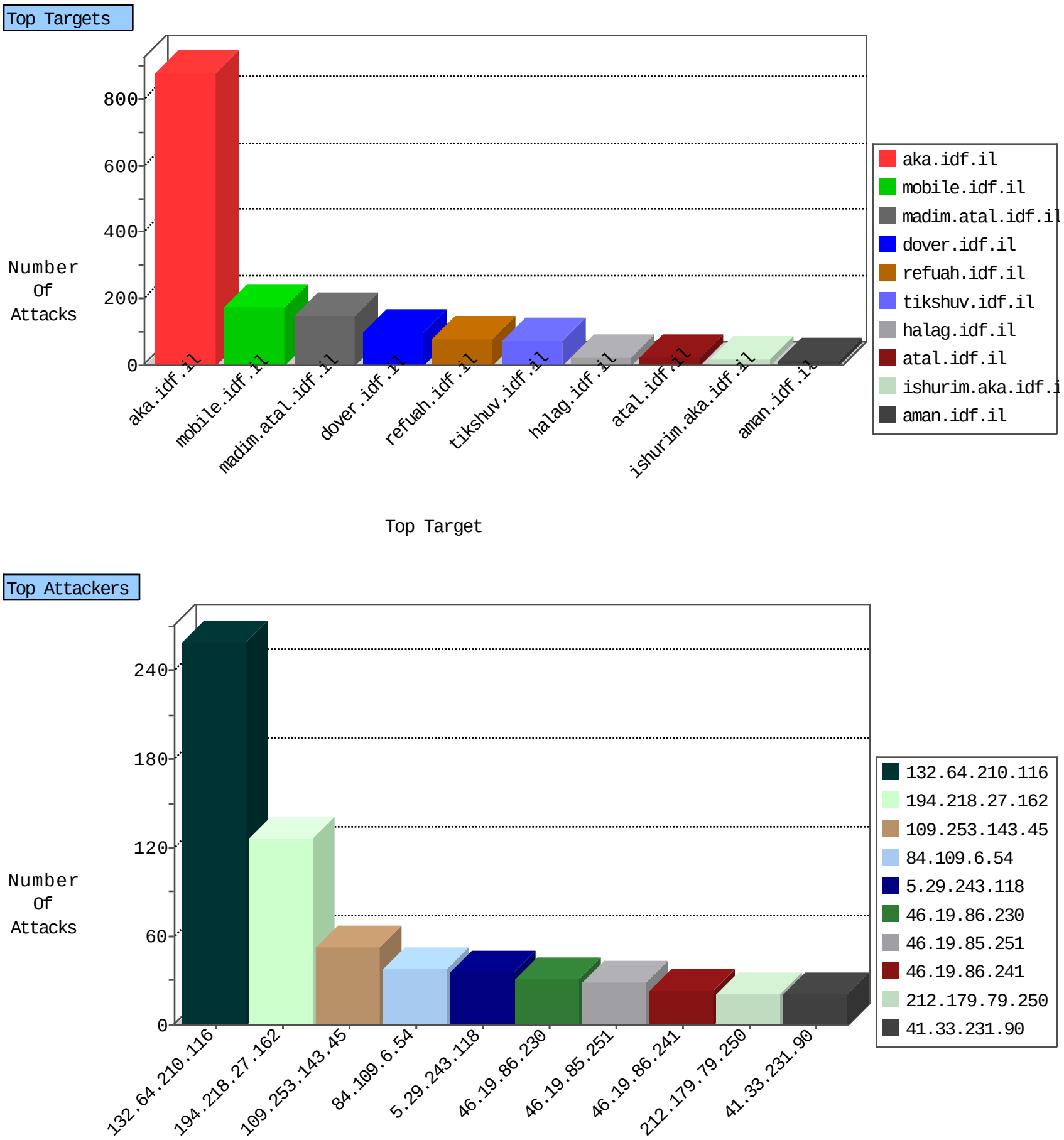
03-01-2016-14:04:04 to 03-01-2016-15:04:04

IDF Under Attack Daily Report



03-01-2016-14:04:04 to 03-01-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
173.234.39.194	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
173.208.176.28	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
185.40.4.45		147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
39.184.139.245	China	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
173.208.176.28	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.40.4.45		147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.37	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
173.208.176.28	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
118.241.52.182	Japan	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1

03-01-2016-14:04:04 to 03-01-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.243.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	32
84.109.18.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
77.125.98.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.250.11.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
37.26.149.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.69.67.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.178.137.60	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.120.134.15	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2

03-01-2016-14:04:04 to 03-01-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.167	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
31.154.29.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.167	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
5.29.243.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.42.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.43.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.87.16.148	147.237.77.121		e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.25.105.125	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
84.228.199.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.164.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.44.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.127.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.38.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.167	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
31.154.16.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
101.187.223.67	147.237.72.156	Australia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.76.202	Romania	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.57.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.91.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.111.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
142.54.171.178	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.246.140.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.135.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.44.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.23.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-14:04:04 to 03-01-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	75
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	55
132.64.210.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	47
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	46
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
84.109.6.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
212.179.79.250	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.86.9	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.5.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.144.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	14
2.52.46.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.124.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.12.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.171.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.125.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.176.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.33.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.210.205.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.3.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.75.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.147.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.144.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.36		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
37.26.147.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.5.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.1.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.150.62.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.181.177.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.90.99.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

03-01-2016-14:04:04 to 03-01-2016-15:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.18.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.203.215.1	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.198.190	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
37.26.147.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
62.90.181.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	7
2.54.20.246	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	7
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	5
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.144.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
212.199.134.136	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.139.52	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
79.177.171.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
212.199.134.138	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.16.224	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.16.224	Block	4
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.54.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.172.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.1.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
109.253.130.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.47.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.199.134.137	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.5.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.0.82.52	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	2
77.125.124.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
213.151.53.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
31.44.133.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/rabanut/general.aspx	None	1
95.86.108.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
54.183.138.211	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
79.177.169.31	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.231		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.148.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.220.145.246	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
54.213.103.226	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
85.65.74.184	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
212.25.105.125	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 212.25.105.125 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
79.182.30.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.12.190	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1