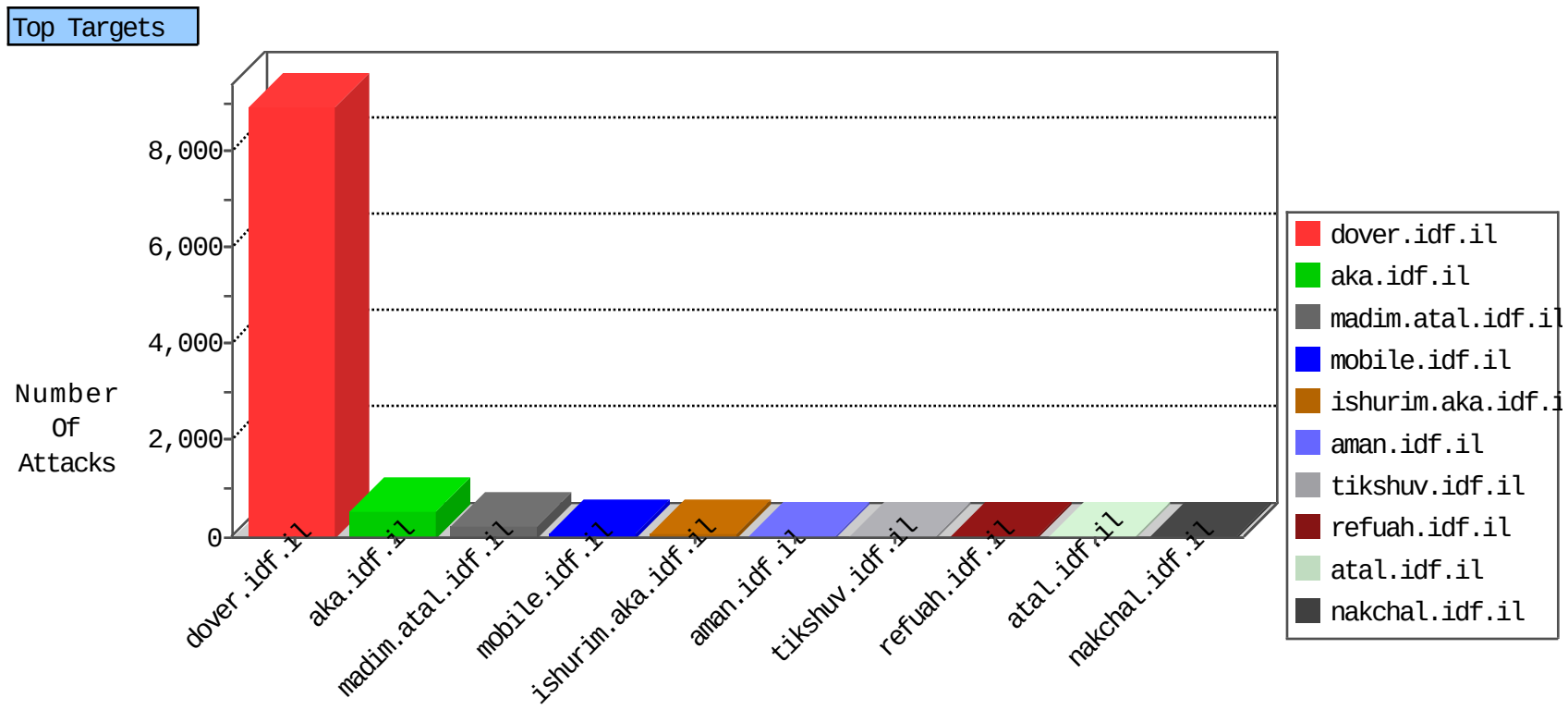
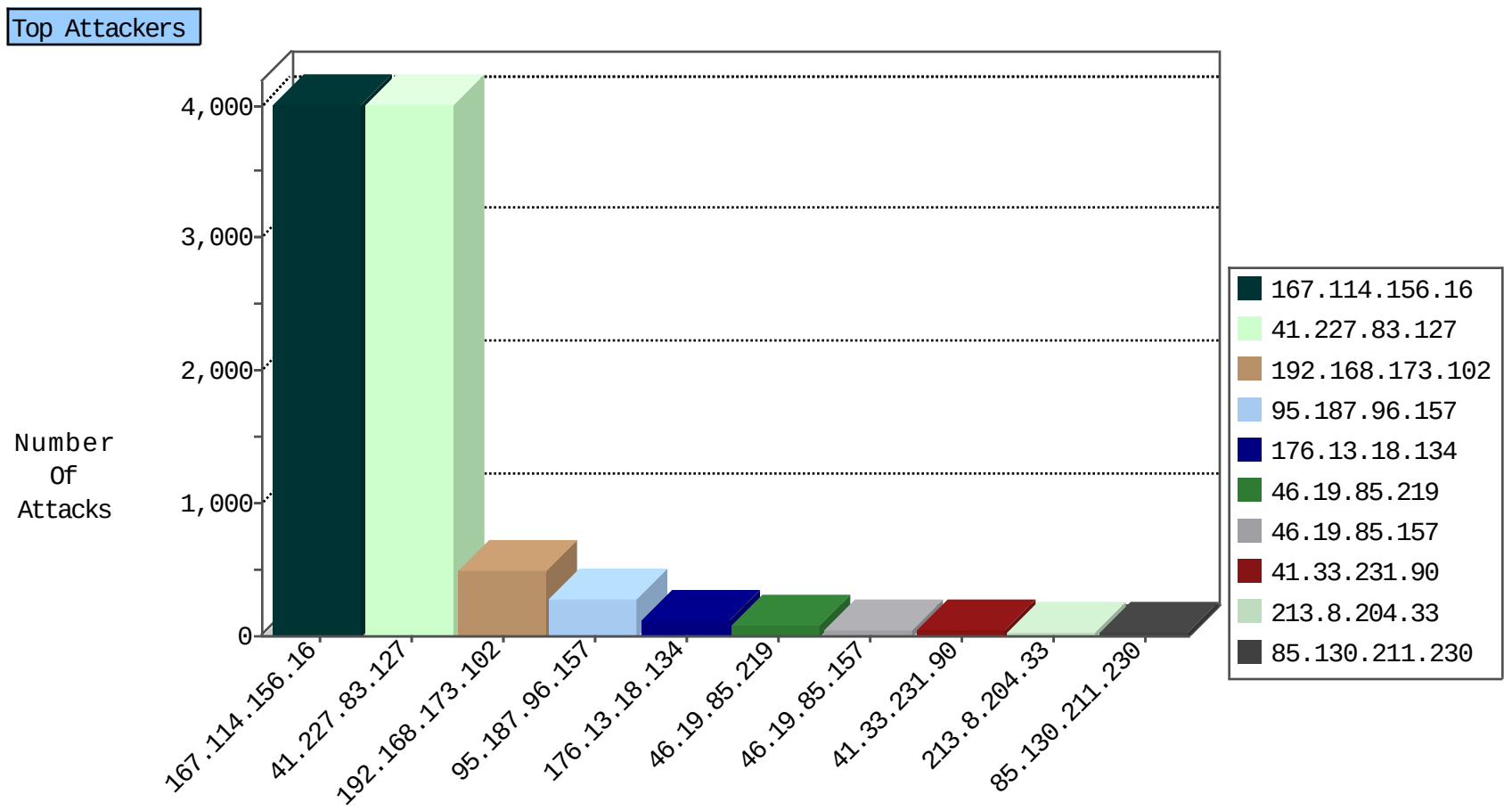
04-10-2016-17:04:05 to 04-10-2016-18:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-17:04:05 to 04-10-2016-18:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4015
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	604
185.120.125.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	82
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
82.145.217.212	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.211.192	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
82.145.221.234	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
87.248.214.97	Italy	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
78.46.133.14	Germany	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1
78.46.133.14	Germany	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
108.166.11.20	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
23.222.28.185	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
84.94.207.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.138.2.83	Germany	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
109.67.32.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-10-2016-17:04:05 to 04-10-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.150.5.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	10
91.230.243.165	United Kingdom	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.164.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.253.141.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
109.64.215.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.117.56.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
87.71.66.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-10-2016-17:04:05 to 04-10-2016-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.109.73.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.21.15.100	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.178.98.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
212.150.5.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
46.121.80.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.159.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.187.96.157	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
27.109.89.211	147.237.77.216	Philippines	dover.idf.il	portscan: TCP Distributed Portscan	1
88.248.21.75	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.108.110.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
212.143.154.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
149.88.169.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.78.73.30	147.237.76.201	Somalia	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 4096	1
31.135.91.107	147.237.0.33	Russian Federation	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
90.127.61.170	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

04-10-2016-17:04:05 to 04-10-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2920
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop		drop	980
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	336
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	166
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	71
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.193	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	26
100.15.163.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
213.8.204.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.130.211.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.245	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
37.19.120.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.67.62.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
78.72.167.240	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.166.221.34	Israel	147.237.77.234	halag.idf.il	drop	SAM rule	drop	13
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	13
46.19.85.245	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	12
85.130.211.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.88	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	12
46.19.86.170	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
79.178.39.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
181.136.54.96	Colombia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.164.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.166.221.34	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.109.45.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.183.3.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.22.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.182.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.8.204.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.160.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.37.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.22.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.121.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.221.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
141.0.13.174	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.151.35.221	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	5

04-10-2016-17:04:05 to 04-10-2016-18:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 95.187.96.157	Block	79
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 95.187.96.157	Block	79
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 95.187.96.157	Block	79
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.18.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.33	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	3
2.53.27.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.100.127	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	2
79.178.151.56	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	2
37.19.120.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.19.120.30	Block	2
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.207.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.24.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.182.173.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
176.13.15.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.134	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.134.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.25.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.130.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/1268-he/refuah	Block	1
2.54.160.89	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
40.77.167.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
82.205.23.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_medium in www.aka.idf.il/main/rabanut/general.aspx	None	1
132.76.10.42	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.231	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method 36 in URL	Block	1
85.250.215.238	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
176.13.22.215	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.121.232.54	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
40.77.167.86	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/qsystemform/	Block	1
84.108.195.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.225.211	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.129	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
95.86.123.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.19.120.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
176.31.115.148	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
65.55.210.231	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.15.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

04-10-2016-17:04:05 to 04-10-2016-18:04:05