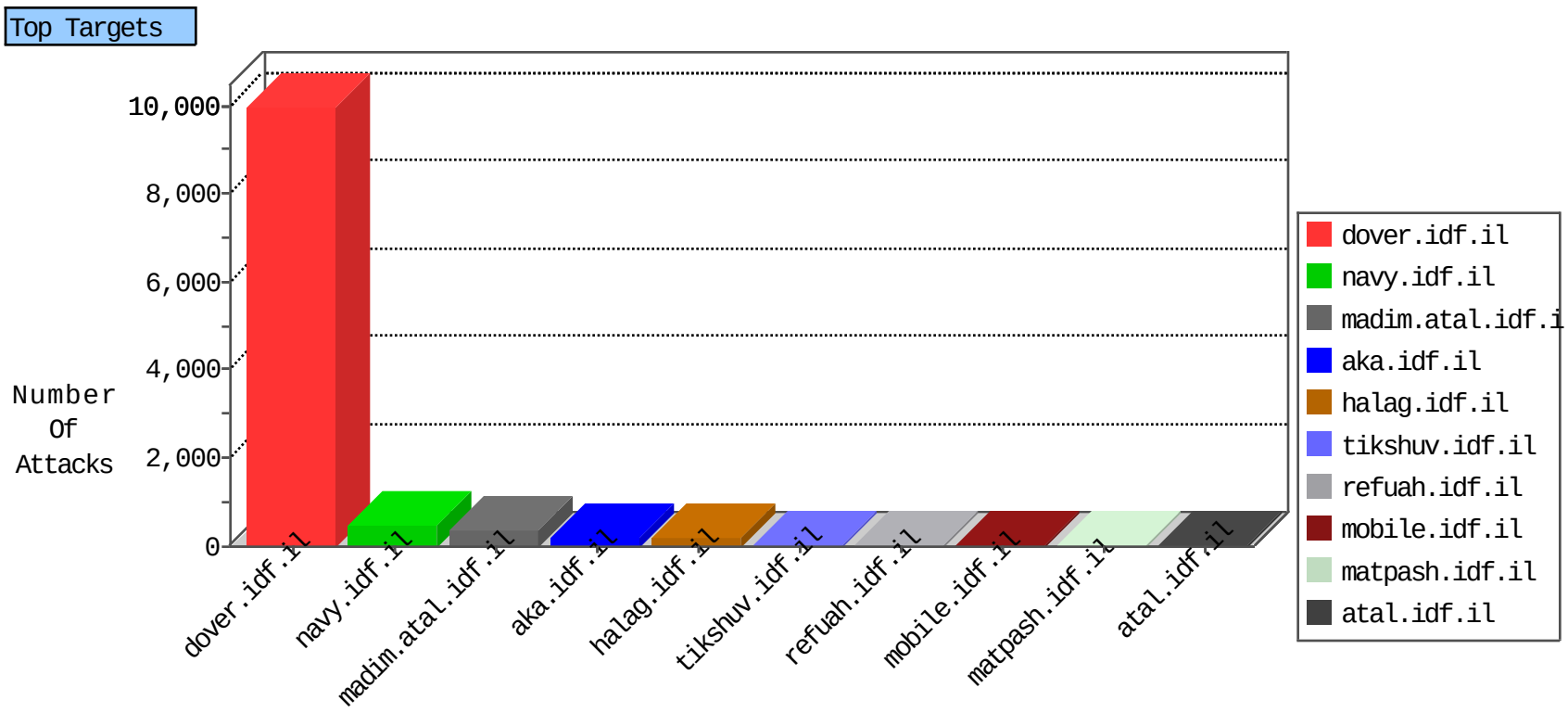
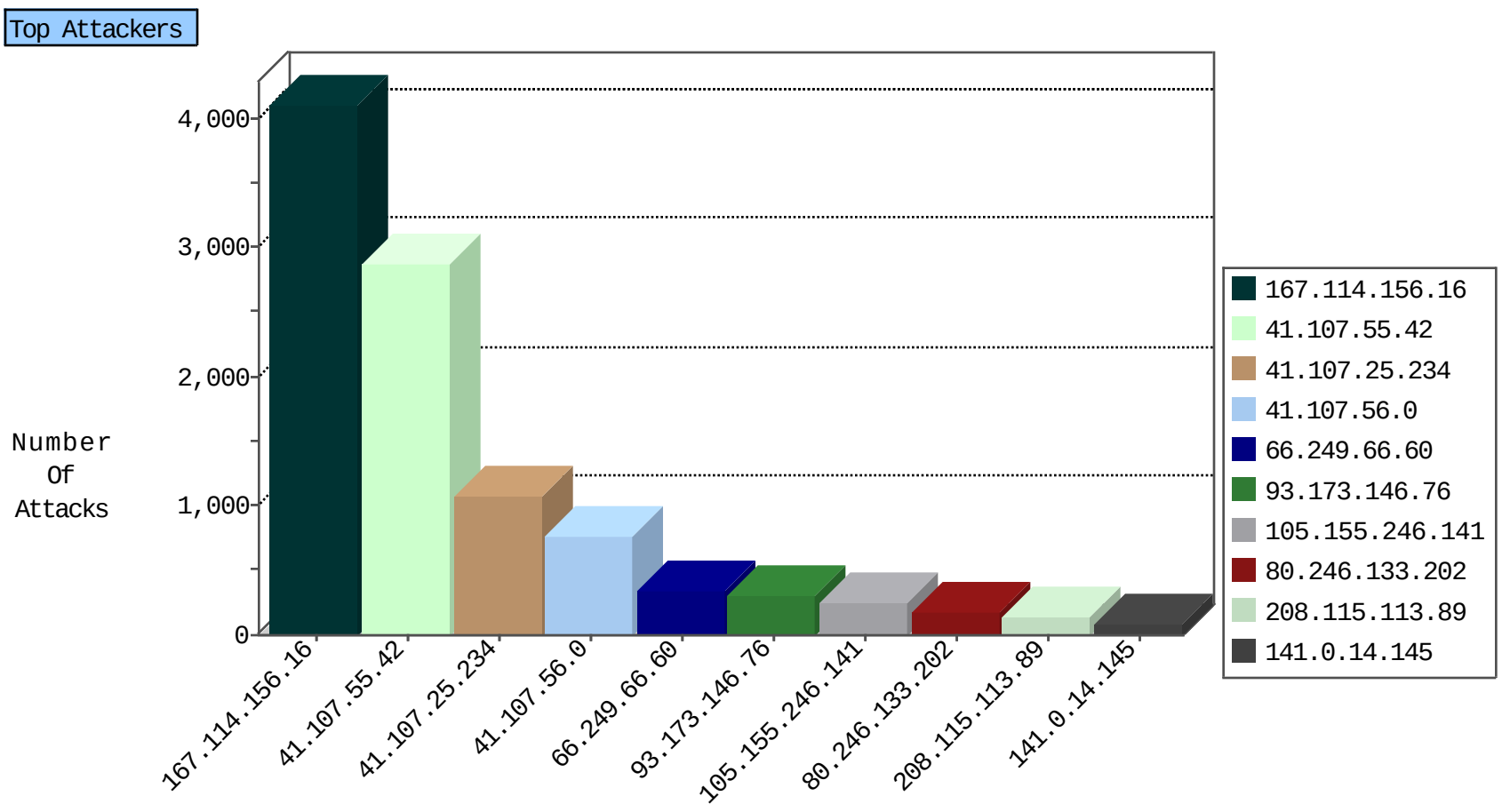
04-16-2016-21:04:04 to 04-16-2016-22:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-16-2016-21:04:04 to 04-16-2016-22:04:04

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	4094
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	614
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	452
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	296
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	62
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	26
41.107.63.148	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	26
14.175.168.54	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	17
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	14
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
37.204.142.237	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
37.204.142.237	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.70.184.164	Netherlands	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
188.214.128.13	Lithuania	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
185.70.184.187	Netherlands	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.187	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
69.64.55.124	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
188.214.128.13	Lithuania	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

04-16-2016-21:04:04 to 04-16-2016-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.122.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
79.179.16.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
5.29.5.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
61.135.189.113	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
46.117.7.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-16-2016-21:04:04 to 04-16-2016-22:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.60	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	343
87.71.107.113	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.133.119	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
108.46.61.58	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
80.246.133.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
89.248.167.131	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
52.25.100.231	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.154	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
52.23.196.75	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
52.23.196.75	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
46.117.182.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.131	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1

04-16-2016-21:04:04 to 04-16-2016-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2100
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	364
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	drop		drop	295
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop		drop	285
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	248
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	199
80.246.133.202	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	165
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	drop		drop	142
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	129
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	50
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
76.102.51.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.117.135.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.243.150.196	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
87.70.121.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.95.15	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.68	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.176.95.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.28.136.175	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.151.61.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.207	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.207	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
217.132.22.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
8.37.228.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.95.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.65.123.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.124.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.79.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
61.90.13.248	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.204.142.237	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.180.204.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.188.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.13.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

04-16-2016-21:04:04 to 04-16-2016-22:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.146.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	302
84.109.69.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
79.182.137.74	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.137.74	Block	7
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 41.107.55.42	Block	6
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 41.107.55.42	Block	6
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed URL from 41.107.55.42	Block	6
185.120.126.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
94.242.225.15	Luxembourg	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
109.253.142.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.213.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.126.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
94.230.92.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
109.253.227.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.182.137.74	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	2
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	2
84.108.68.127	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
149.88.111.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.93	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
2.53.149.149	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.32.179.180	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.120.47.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1603-15075-he/	Block	1
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.65.6.121	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
85.64.113.128	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
117.78.13.51	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Tango in URL down	Block	1
95.83.171.125	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.29.187.130	Israel	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	1
185.120.126.111	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.120.126.111	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/4.asp	Block	1
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Malformed URL down	Block	1
89.139.49.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
207.46.13.178	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.178	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/	Block	1
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
95.83.171.125	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
5.29.187.130	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
80.246.133.202	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
79.179.126.29	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	1
207.46.13.186	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
149.78.222.81	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.87	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/homepage/mobile	Block	1
98.207.46.126	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2367.jpg	Block	1
109.253.227.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-16-2016-21:04:04 to 04-16-2016-22:04:04