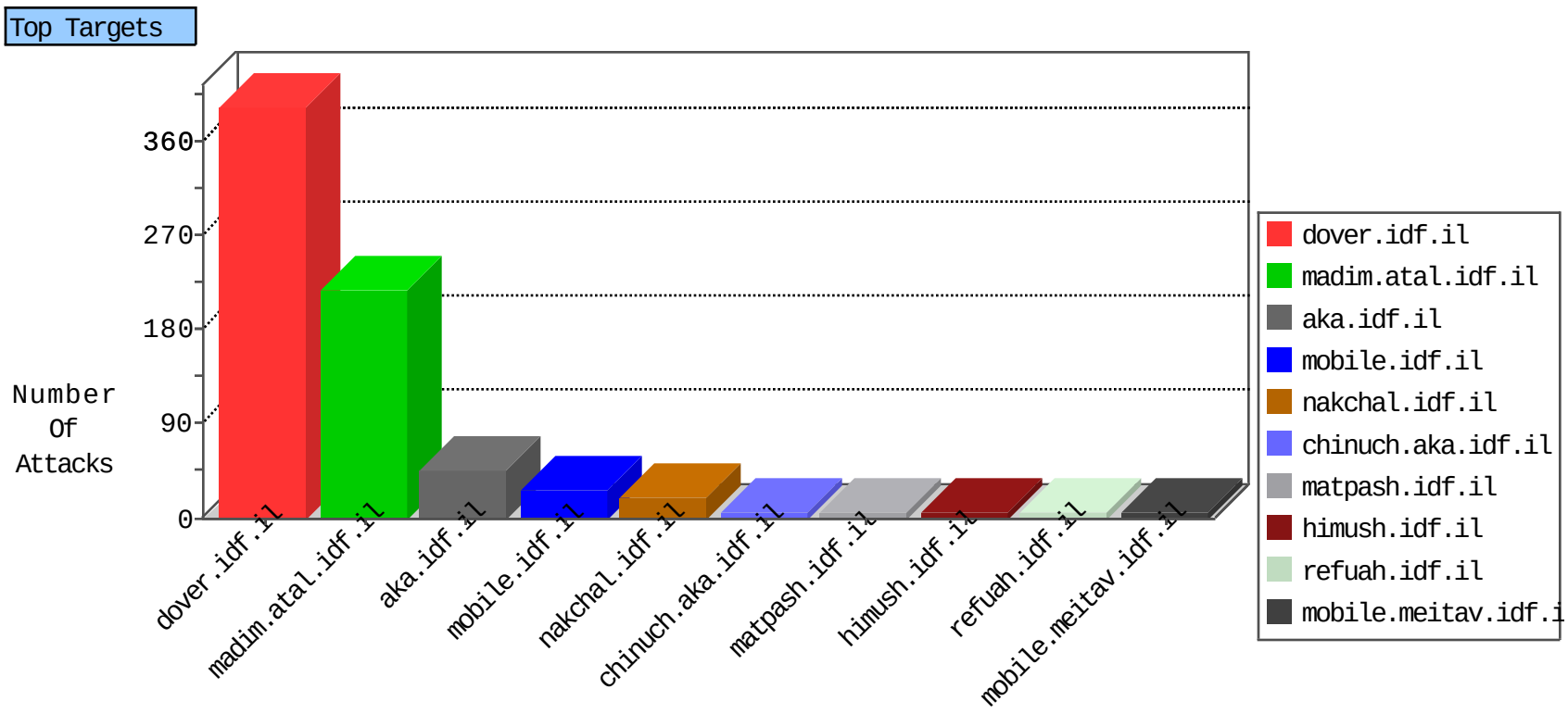
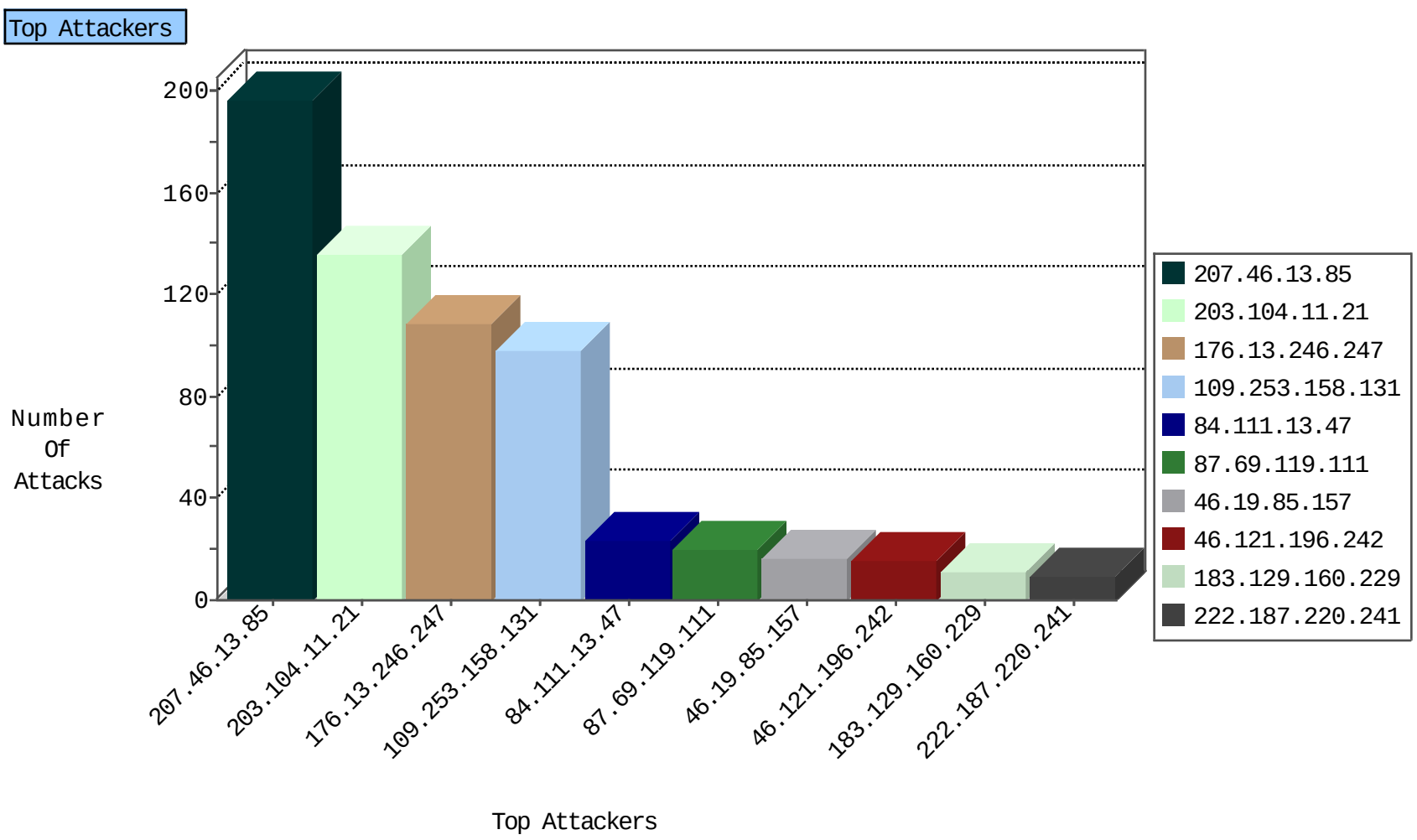
10-05-2016-06:04:09 to 10-05-2016-07:04:09

IDF Under Attack Daily Report





10-05-2016-06:04:09 to 10-05-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.193.252	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
142.54.174.83	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.193.250	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
183.60.48.25	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
198.204.255.78	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
192.187.101.234	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
93.174.94.235	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
211.155.16.154	China	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
173.208.198.10	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
192.187.118.21	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
93.174.94.235	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
63.141.231.198	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.198.10	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
192.187.118.67	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
142.54.174.82	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
63.141.231.211	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

10-05-2016-06:04:09 to 10-05-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
179.158.81.117	Brazil	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-05-2016-06:04:09 to 10-05-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
115.208.41.75	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
122.225.95.78	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
109.236.86.32	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.187.220.241	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.187.220.241	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
222.187.220.241	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
54.91.134.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.187.220.241	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
45.55.3.37	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
204.42.253.136	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.55.3.37	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.187.220.241	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.187.220.241	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.187.220.241	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
54.147.7.228	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.187.220.241	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
45.55.3.37	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
222.187.220.241	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.55.3.37	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Potential SSH Scan	1
39.167.57.151	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.185.179.222	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-05-2016-06:04:09 to 10-05-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	197
203.104.11.21	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
87.69.119.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
84.111.13.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.121.196.242	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
223.182.188.176	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.82.56.247	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
109.253.159.240	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.111.13.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.242.91.219	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.228.167	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
192.0.117.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.111.13.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
51.255.162.163	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
176.13.228.167	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.111.13.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.64.61.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.146.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.125.50	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.26.148.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.244	United States	147.237.0.33	idf.il	drop		drop	1
104.237.146.151	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.20	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
182.68.99.226	India	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.20	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.226.217.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.0.113.241	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.248.234.22	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.214	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
183.129.160.229	China	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.252	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.237.146.151	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.82	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.126.8.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
182.68.99.226	India	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.247.82.206	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
23.248.237.25	United States	147.237.0.200	m4u.idf.il	drop		drop	1
118.97.145.213	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-05-2016-06:04:09 to 10-05-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.246.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
109.253.158.131	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	98
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
77.138.8.147	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/faq.aspx	Block	4
46.19.85.0	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 183.129.160.229 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	1
46.121.196.242	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
66.249.64.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/theproj/heproj.asp	Block	1
183.129.160.229	China	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 183.129.160.229 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.82.56.247	United States	147.237.76.147	chinuch.aka.idf.i	Malformed URL 54.90.189.128:80	Block	1
84.161.102.130	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/asp	Block	1
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
183.129.160.229	China	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.229.178	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/↑	Block	1
54.82.56.247	United States	147.237.76.147	chinuch.aka.idf.i	NULL Character in Method	Block	1
2.53.2.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.108	Block	1
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
183.129.160.229	China	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 183.129.160.229 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.229.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9687-he/refuah.aspx	Block	1
31.168.104.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.109	Block	1
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 57f475958fc8e401000 in URL	Block	1
74.101.116.50	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.64.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8754-he/refuah.aspx	Block	1

10-05-2016-06:04:09 to 10-05-2016-07:04:09