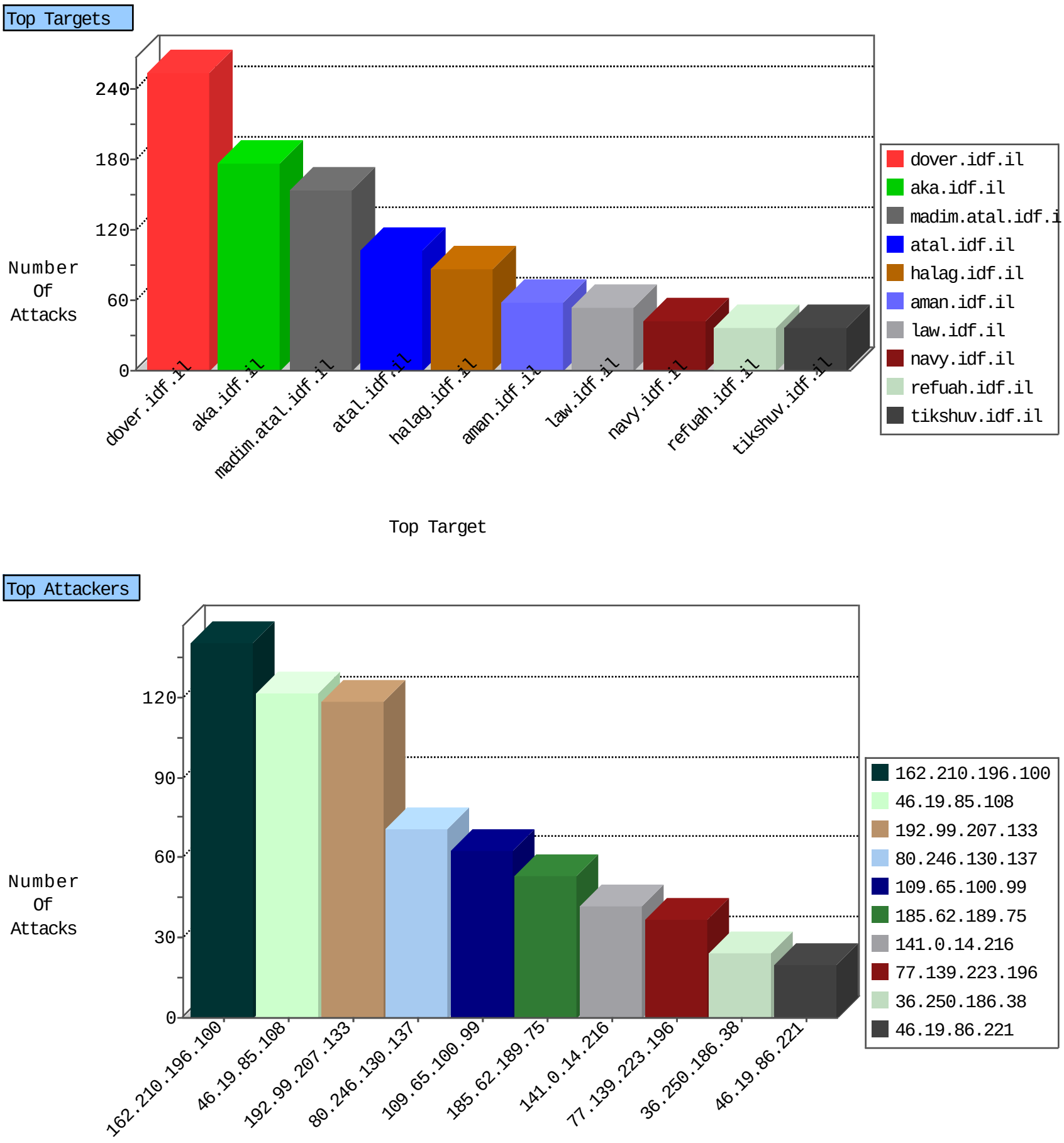
09-06-2016-18:04:04 to 09-06-2016-19:04:04

IDF Under Attack Daily Report



09-06-2016-18:04:04 to 09-06-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.2.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
94.102.49.193	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-06-2016-18:04:04 to 09-06-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	109
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	19
162.210.196.100	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	8
162.210.196.100	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
84.20.63.93	Switzerland	147.237.77.74	law.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
107.175.239.205	United States	147.237.76.86	navy.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
195.154.232.58	France	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

09-06-2016-18:04:04 to 09-06-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	4
91.224.161.69	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
208.67.1.220	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.146.104	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.170.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.94.142	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
85.14.42.2	147.237.76.147	Bulgaria	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
42.121.111.38	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.220	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
194.58.37.41	147.237.77.74	Russian Federation	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
186.115.238.24	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.94.142	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.161.69	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-06-2016-18:04:04 to 09-06-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.137	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
109.65.100.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
141.0.14.216	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
77.139.223.196	France	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
79.180.56.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.15	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
37.76.197.150	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
109.253.246.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.66.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.185	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
77.139.223.196	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.142.107	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.246.137.68	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.235.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.190.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.96.123	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
2.53.164.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.178.235.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
109.65.100.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.55.179.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.235.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.235.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.247.36.95	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.39.148	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.67.174.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.39.148	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.159.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.62.189.75	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.62.189.75	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.149.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
141.226.218.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.62.189.75	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-06-2016-18:04:04 to 09-06-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
36.250.186.38	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 36.250.186.38	Block	17
89.139.200.211	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	17
37.26.149.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
141.226.218.48	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
36.250.186.38	China	147.237.77.74	law.idf.il	PHP Attempt	Block	6
2.53.22.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
85.64.188.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.138.76.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
80.178.89.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.59.50	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.229.21.21	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
192.114.86.6	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.167.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.6.241.239	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.180.56.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
207.232.37.179	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
46.19.85.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.128.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
84.229.15.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
176.13.6.133	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
87.69.247.223	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.19.121.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.15.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
109.253.231.67	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
77.139.214.75	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/giyus/general.aspx	Block	1
188.255.25.100	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
80.246.130.137	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.125.58.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.229.69.124	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.229.69.124 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
36.250.186.38	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.asp	Block	1
77.139.223.196	France	147.237.0.34	tikshuv.idf.il	Unauthorized Method POST for 147.237.0.34/	Block	1
66.249.69.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_	Block	1
37.26.149.178	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
96.241.22.37	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
2.53.55.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.175.64	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.15.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
162.210.196.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
46.117.88.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.229.69.124	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.6.241.239	Greece	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
77.237.146.28	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1

09-06-2016-18:04:04 to 09-06-2016-19:04:04