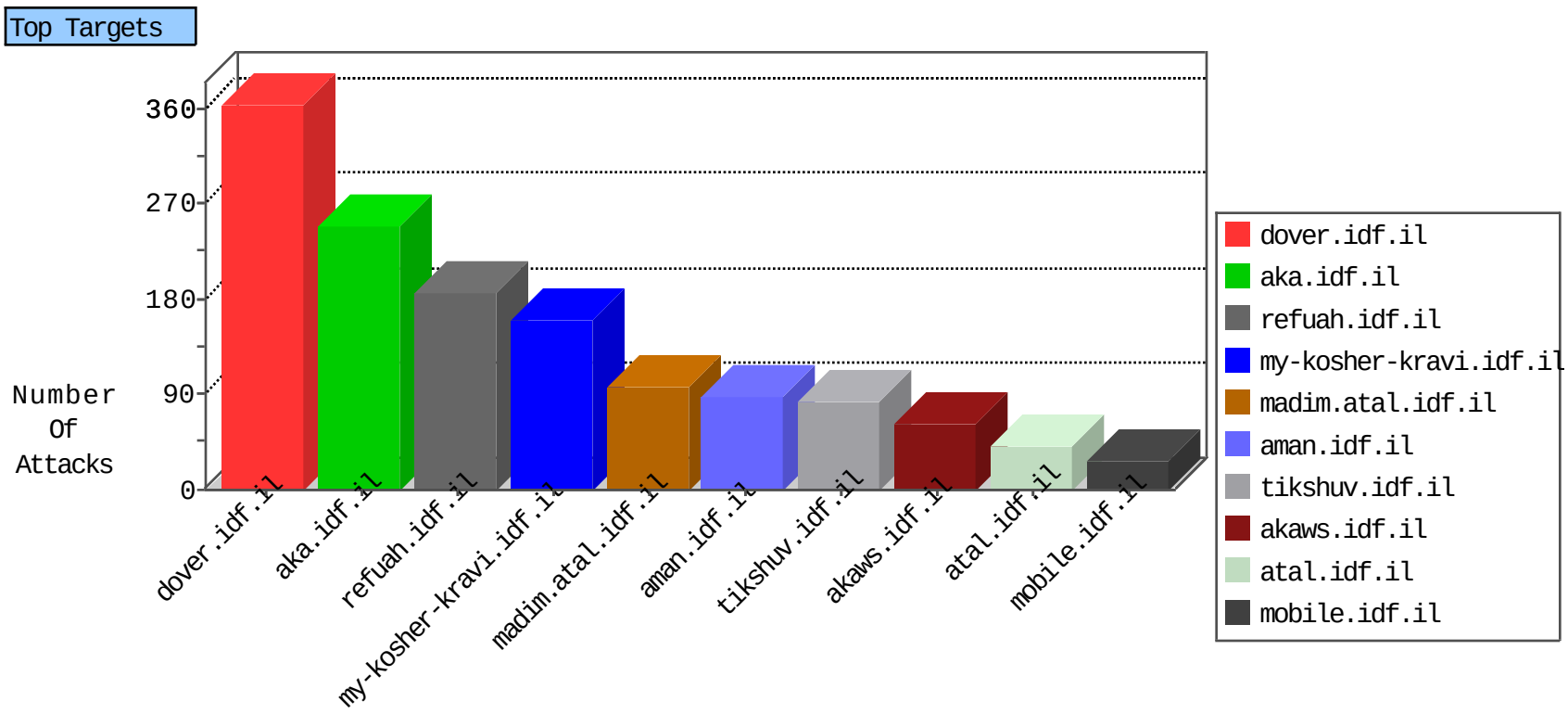
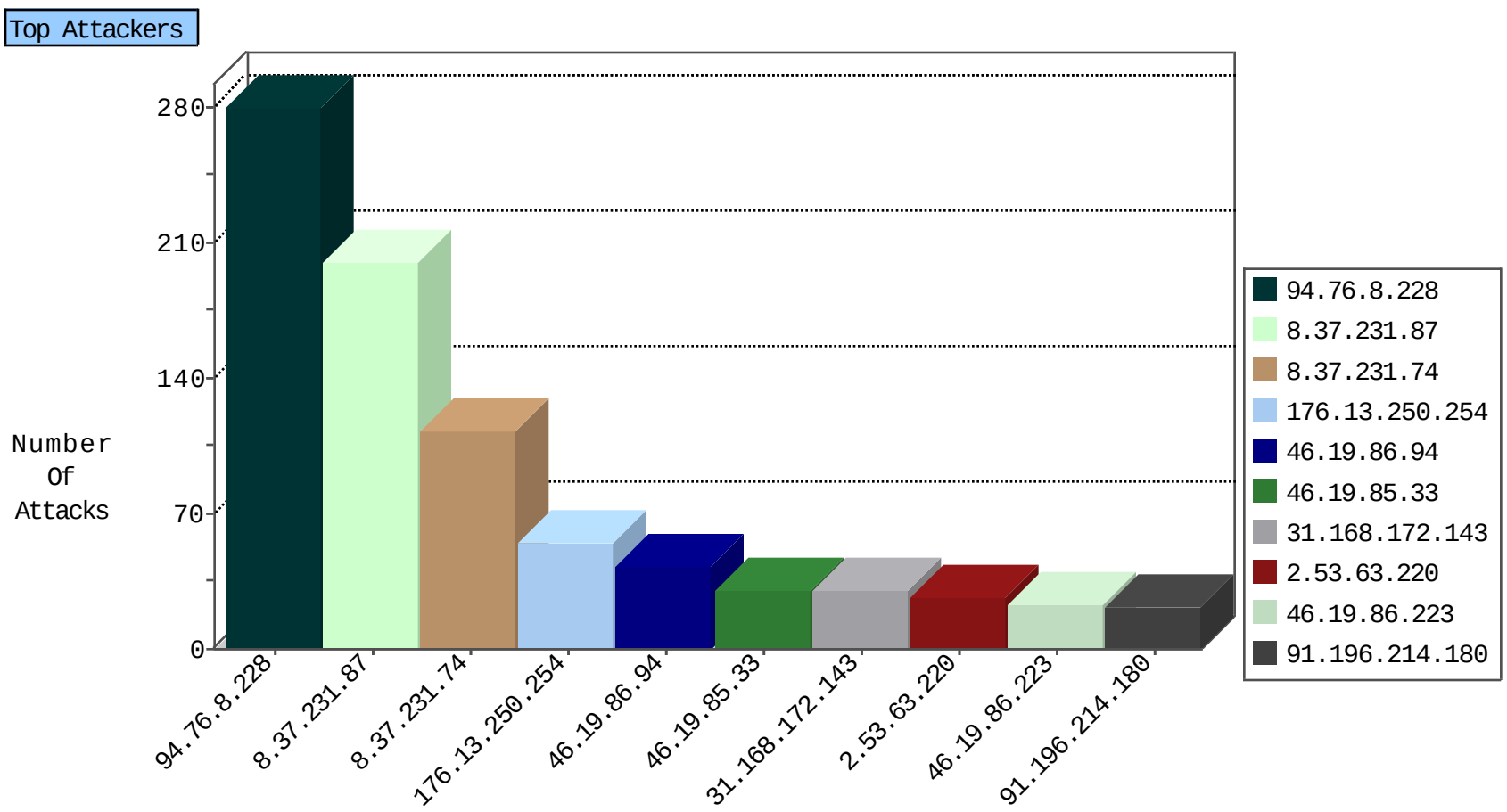
09-14-2016-21:04:09 to 09-14-2016-22:04:09

IDF Under Attack
Daily Report



Top Target



Top Attackers

09-14-2016-21:04:09 to 09-14-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.231.74	United States	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	6
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
2.53.141.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
8.37.231.87	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
46.19.86.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
61.178.42.242	China	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
103.39.16.172	China	147.237.77.212	e.dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-14-2016-21:04:09 to 09-14-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	4
81.163.131.57	Ukraine	147.237.72.166	aka.idf.il	26949: HTTP: Drupal RESTWS Module Page Callback Code Injection Vulnerability	Block	1

09-14-2016-21:04:09 to 09-14-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.172.143	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
31.168.172.143	147.237.76.176	Israel	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
94.76.8.228	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
31.168.172.143	147.237.76.31	Israel	nakchal.idf.il	ET SCAN Potential SSH Scan	2
31.168.172.143	147.237.72.156	Israel	aman.idf.il	ET SCAN Potential SSH Scan	2
31.168.172.143	147.237.76.86	Israel	navy.idf.il	ET SCAN Potential SSH Scan	2
31.168.172.143	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.179	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
198.52.97.84	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
31.168.172.143	147.237.72.14	Israel	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.77.179	Israel	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.172.143	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.77.74	Israel	law.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.0.200	Israel	m4u.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.172.143	147.237.76.201	Israel	e.atal.idf.il	ET SCAN Potential SSH Scan	1
118.103.142.140	147.237.76.177	Bhutan	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.172.143	147.237.76.196	Israel	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.0.15	Israel	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.76.8.228	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.172.143	147.237.76.39	Israel	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.72.166	Ukraine	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.168.172.143	147.237.77.234	Israel	halag.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.73	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.172.143	147.237.8.46	Israel	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.77.170	Israel	maarachot.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.172.143	147.237.77.19	Israel	law-forum.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
31.168.172.143	147.237.76.197	Israel	e.himush.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.143	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.172.143	147.237.76.177	Israel	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.76.8.228	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.201.236.155	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.172.143	147.237.76.38	Israel	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -f -sS	1

09-14-2016-21:04:09 to 09-14-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	198
94.76.8.228	Bahrain	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	156
94.76.8.228	Bahrain	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	61
94.76.8.228	Bahrain	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	59
8.37.231.74	United States	147.237.76.42	refuah.idf.il	SYN Attack		monitor	43
8.37.231.74	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	42
8.37.231.74	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
46.19.85.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
84.111.112.97	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
185.26.180.90	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
79.177.244.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
168.235.196.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
91.196.215.102	Poland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.122	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.3.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
172.58.25.229	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
85.64.130.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
176.13.232.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.60.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
91.196.214.180	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
91.196.214.180	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.116.66.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.206.30	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.3.147.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
88.202.218.236	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.223	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.81.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
194.242.174.63	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.74	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
176.13.232.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
199.30.24.4	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.196.214.180	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.116	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.223	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.157.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.218.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

09-14-2016-21:04:09 to 09-14-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.250.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.53.63.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
77.139.24.167	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.24.167	Block	4
185.27.106.89	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
185.32.179.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.221.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
46.19.86.122	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	2
77.139.39.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
217.132.36.134	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
85.65.151.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.81.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.79.180.74	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
77.127.48.242	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.8	Block	1
87.70.10.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
2.53.167.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
46.117.128.85	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
94.98.254.125	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.109.203.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	1
42.96.177.34	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.138.163.106	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
124.73.11.123	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-he/idfg.aspx/trackback/	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
46.19.86.217	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
87.71.40.126	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
5.29.71.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.57.31	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.64.137	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
192.198.151.36	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.198.151.36	Block	1
109.15.143.6	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
46.120.164.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.112.97	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
42.96.177.34	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
2.53.36.231	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.163.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	1
176.13.232.79	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21969-he/idfgdover.aspx	Block	1
46.19.86.217	Israel	147.237.77.233	atal.idf.il	Malformed URL	Block	1
88.202.218.236	United Kingdom	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.212.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.125.64.137	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.125.64.137	Block	1
192.198.151.36	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
109.65.76.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.6.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
85.64.129.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

09-14-2016-21:04:09 to 09-14-2016-22:04:09