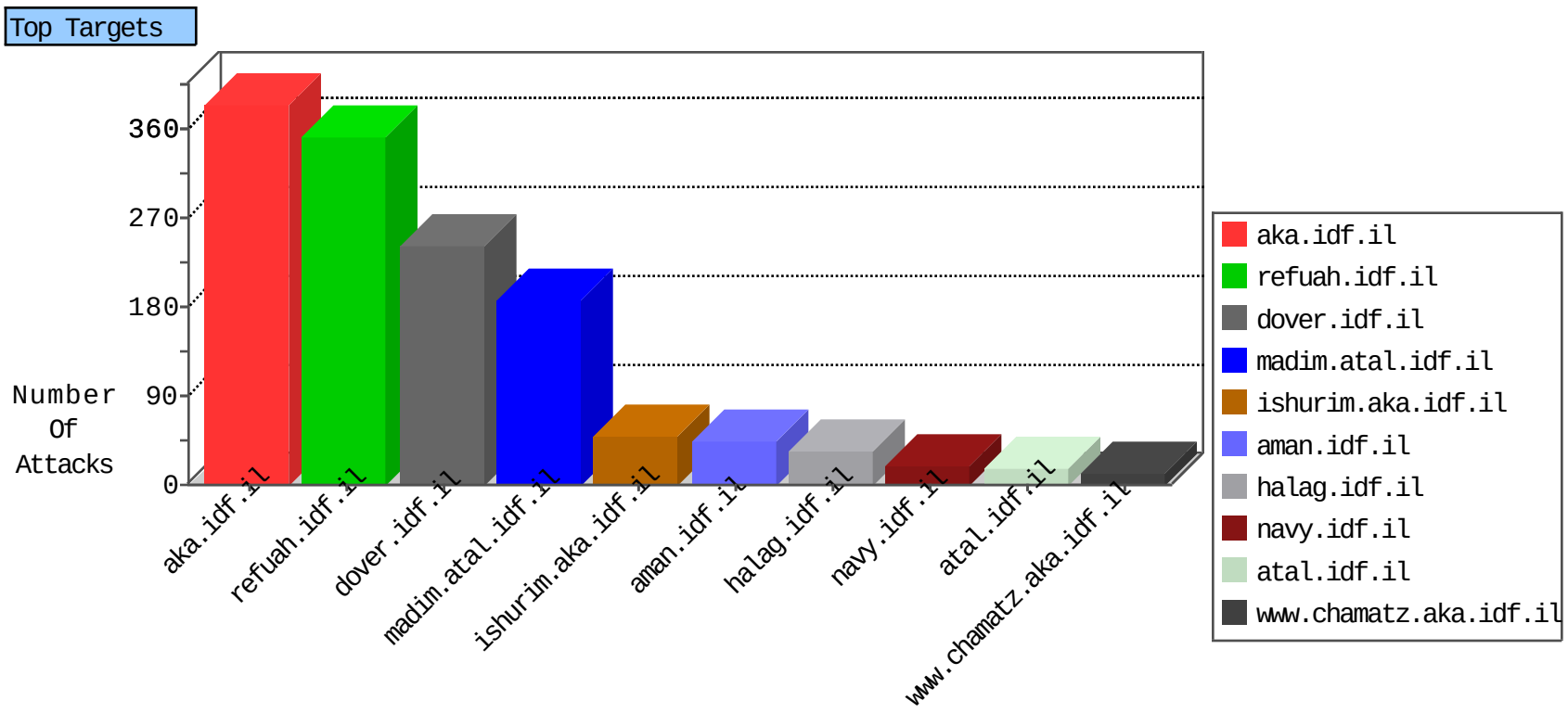
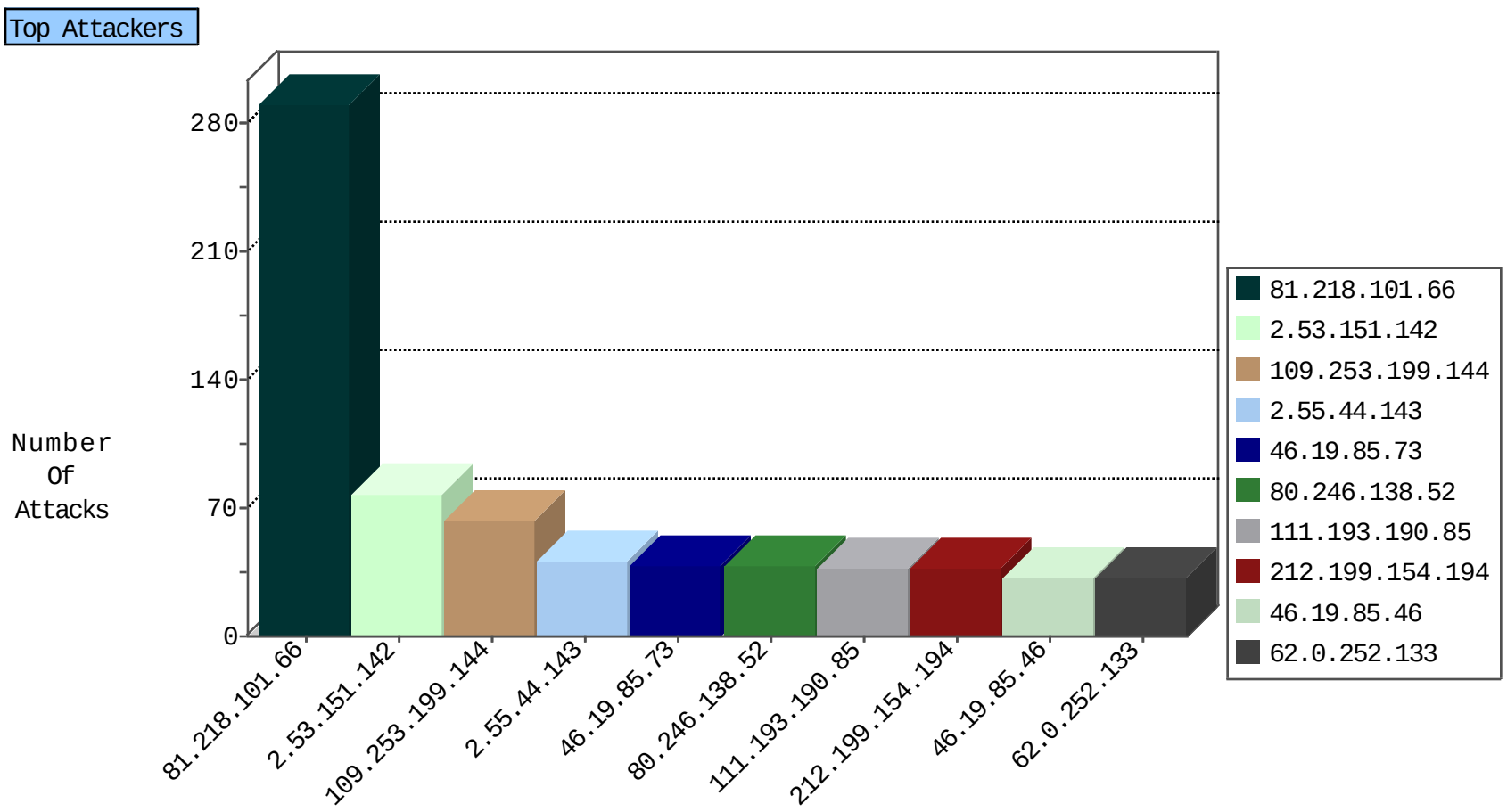
09-14-2016-09:04:07 to 09-14-2016-10:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

09-14-2016-09:04:07 to 09-14-2016-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
111.193.190.85	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
109.64.184.4	Israel	147.237.72.166	aka.idf.il	Black List	drop	6
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
2.53.146.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
46.19.85.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.198.151.36	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
153.90.1.35	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
82.166.199.245	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.117.174.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
46.19.85.73	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	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

09-14-2016-09:04:07 to 09-14-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	31
123.126.68.98	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-14-2016-09:04:07 to 09-14-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
106.79.131.190	147.237.76.39	India	mobile.meitav.idf.il	GPL SCAN nmap TCP	3
46.227.67.158	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
207.232.27.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.163.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.19.115.4	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	1
123.232.26.132	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
8.37.237.44	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.52.71	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.110.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.219.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.128.45.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.56.98.132	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
213.151.36.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.69.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.232.26.132	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.90.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.23.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.225.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.31.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.56.98.132	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1

09-14-2016-09:04:07 to 09-14-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	291
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	36
62.0.252.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
111.193.190.85	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.253.199.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
141.0.12.212	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
62.0.227.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
192.117.162.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
109.253.199.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.46	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.46	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
109.253.241.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
178.134.63.55	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.253.199.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
141.228.106.148	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.147.229	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
80.246.136.179	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	7
109.253.199.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.241.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.130.92	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.120.126.52	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.177.199.8	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.138.82	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.241.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.181.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
80.246.136.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.20.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.228	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.149.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
80.246.136.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.253.198.94	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.118	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.22	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

09-14-2016-09:04:07 to 09-14-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.151.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
2.55.44.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.138.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.148.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.16.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.25.102.63	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	6
108.171.129.164	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	4
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.109.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/	Block	2
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	2
77.138.195.96	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	2
185.120.124.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized HTTP Method	Block	2
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.181.168	France	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
62.90.181.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
195.154.181.168	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/wp-admin/user/wp-reader.php	Block	1
176.13.15.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.148.184	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	1
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
195.154.181.168	France	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
72.131.28.44	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.19.85.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.117.175.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sachar/login	Block	1
10.152.70.20		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
217.194.194.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.197.43	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
195.154.181.168	France	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 195.154.181.168	Block	1
195.154.181.168	France	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
2.53.32.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.179.28.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/klali.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.181.168	France	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
77.124.49.247	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.19.85.241	Block	1
132.74.208.161	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
37.19.115.4	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
219.92.228.34	Malaysia	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
195.154.181.168	France	147.237.77.243	mobile.idf.il	PHP Attempt	Block	1
195.154.181.168	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-admin/user/wp-reader.php	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
176.228.141.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
37.142.40.152	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
212.199.57.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.181.168	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/wp-admin/user/wp-reader.php	Block	1
46.19.86.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1

09-14-2016-09:04:07 to 09-14-2016-10:04:07