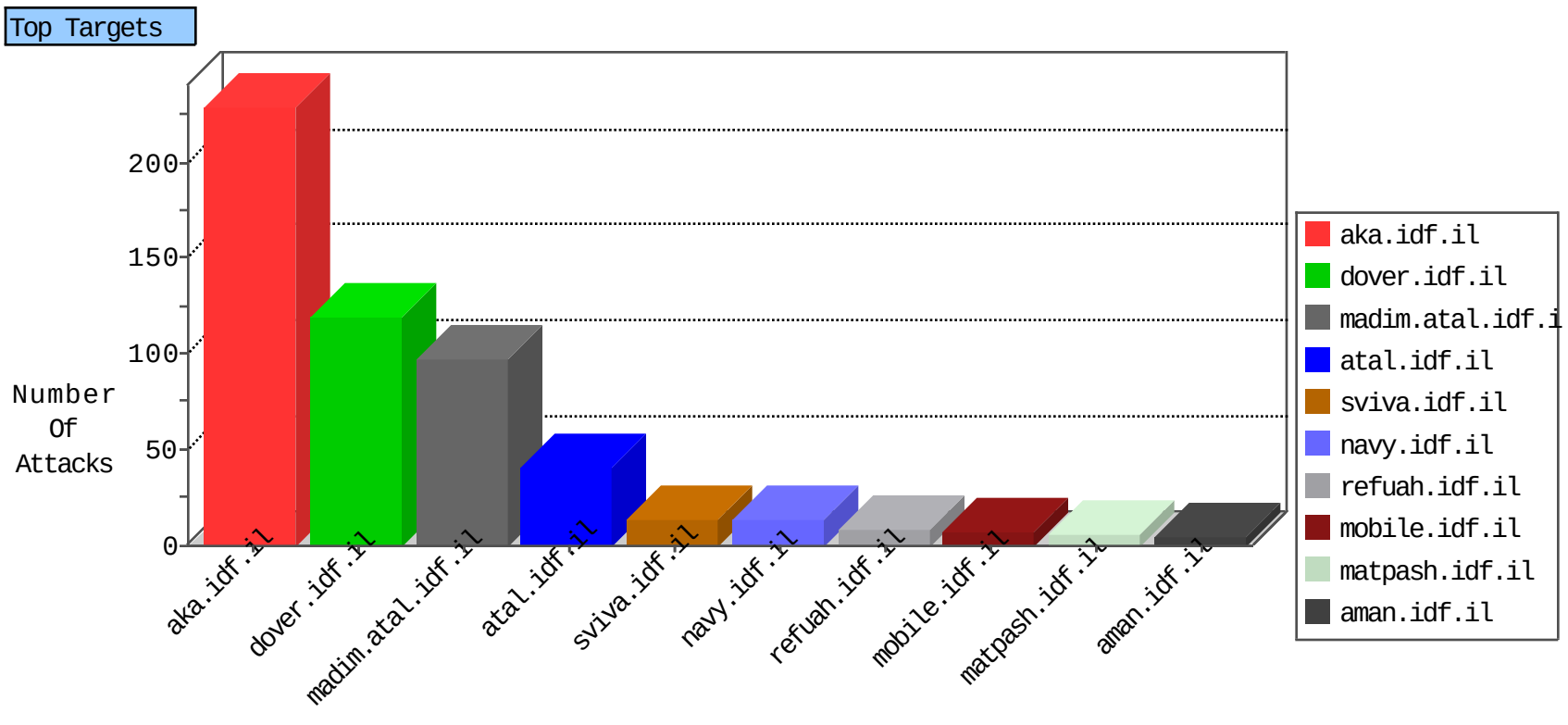
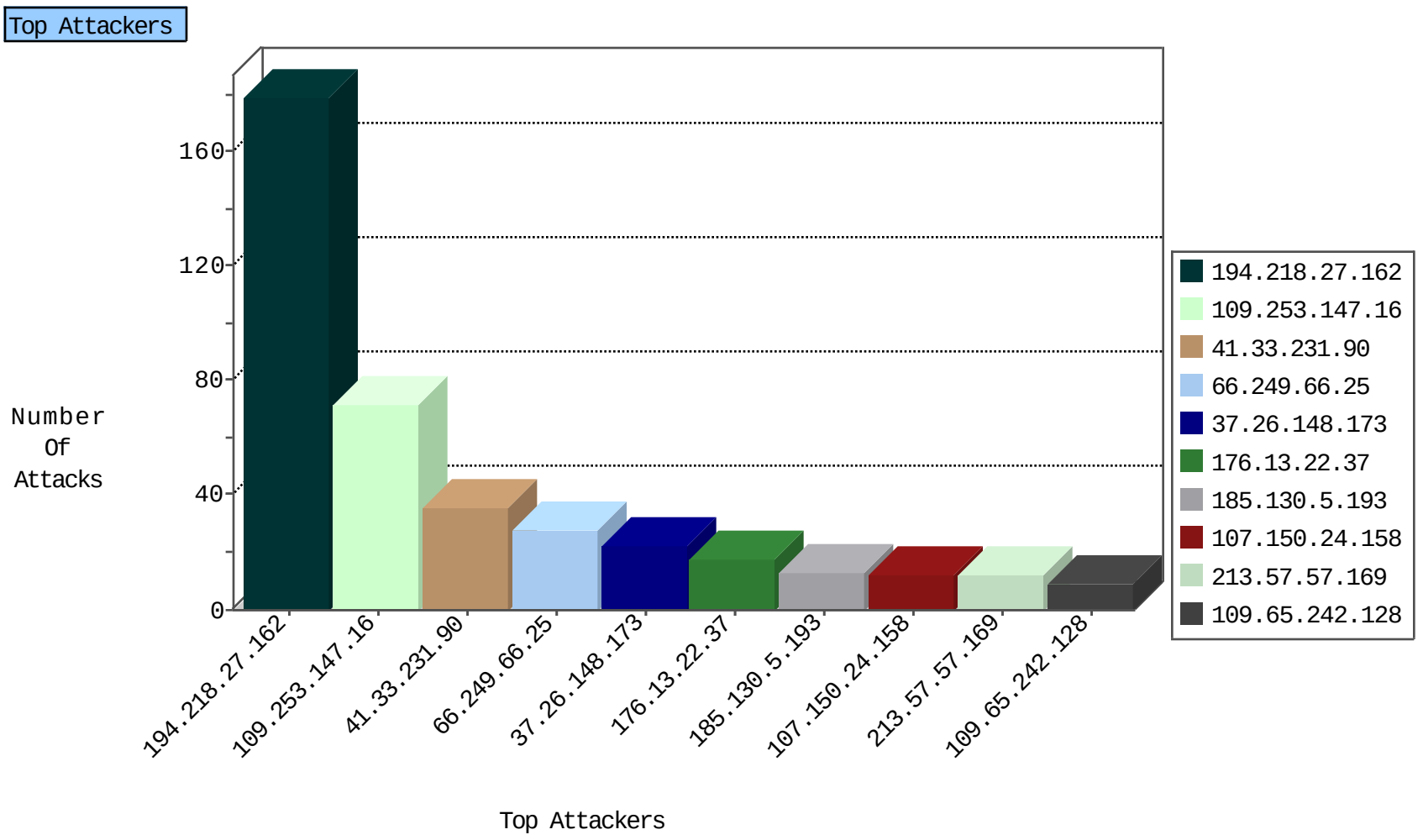
03-02-2016-06:04:09 to 03-02-2016-07:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016-06:04:09 to 03-02-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.96	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.14	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
184.105.139.116	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.26	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
184.105.139.116	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
176.102.202.32	Ukraine	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

03-02-2016-06:04:09 to 03-02-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
69.30.215.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-02-2016-06:04:09 to 03-02-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.22.37	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
110.77.230.216	147.237.8.27	Thailand	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.215.89.20	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.122.144.162	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
189.202.241.84	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -f -sS	1
189.202.241.84	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
185.72.179.221	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
93.122.144.162	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.122.144.162	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
58.253.96.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
189.202.241.84	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
185.72.179.221	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

03-02-2016-06:04:09 to 03-02-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	119
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.130.5.193		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
107.150.24.158	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.65.242.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.22.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.22.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.57.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.57.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.22.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.103	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.112.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.148.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.203	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.253.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.235.135.234	Lebanon	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
2.54.168.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.207.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
131.253.25.233	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
188.120.148.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
45.102.139.146		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
123.125.71.72	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.112	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.177.55.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
47.88.103.153	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.110	United States	147.237.0.33	idf.il	drop		drop	1
45.120.188.105		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
163.44.164.72	Japan	147.237.0.33	idf.il	drop		drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
99.237.151.207	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.22	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.0.35	akaws.idf.il	drop		drop	1
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
62.84.73.242	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.110	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.120.188.105		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.240.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.95	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.198.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	28
37.26.148.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	4
188.120.154.180	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	2
217.132.2.53	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 217.132.2.53	Block	1
46.193.65.65	France	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.104	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oproles/	Block	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
69.156.25.30	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
194.158.199.28	Belarus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
131.253.36.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
217.132.2.53	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.9.59.182	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
31.154.253.217	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
199.104.126.60	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
79.181.173.28	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/sitemap/sitemap.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2003/november/mmmmmmm=d507a9eemmmmmmm_d507a9ee	Block	1
99.237.151.207	Canada	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
31.154.253.217	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 31.154.253.217	Block	1
205.186.184.15	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
188.40.89.95	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.46	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1