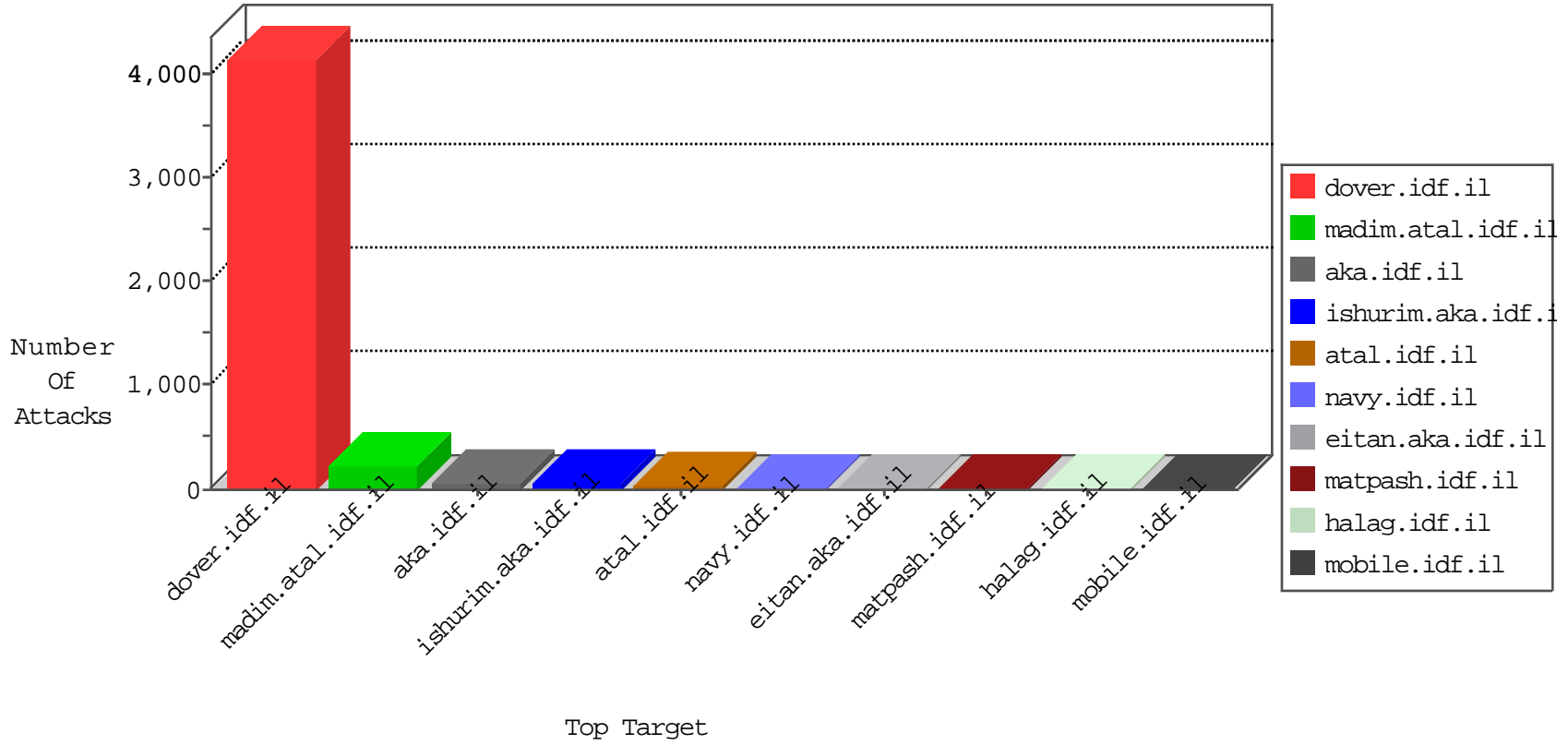


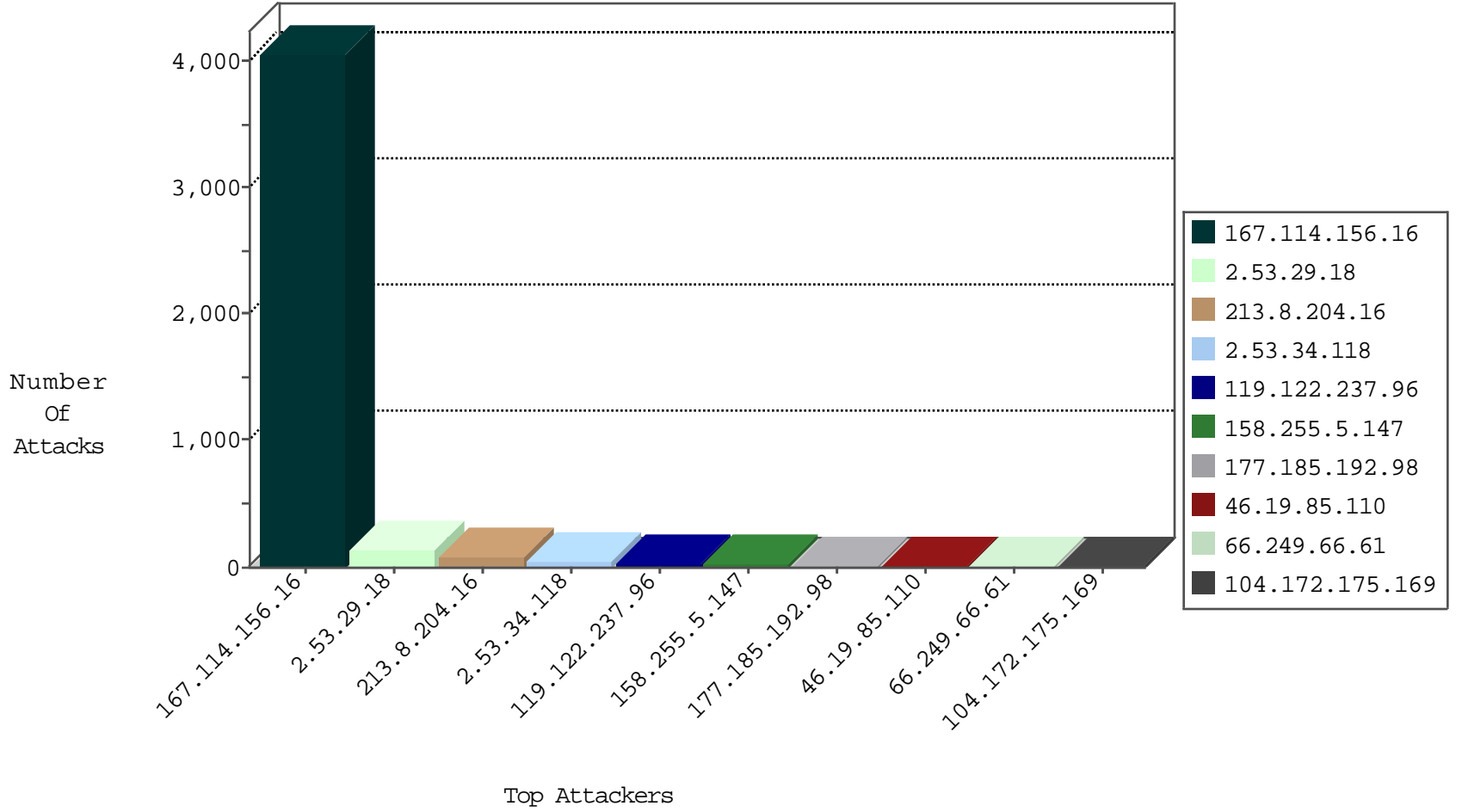
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4049
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
69.197.158.234	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.108	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.8.46	e.chimuch.idf.il	Block_Ntp_All_Net	drop	1
61.219.69.164	Taiwan	147.237.76.148	gcqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.192.98	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.98	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.117	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	147.237.8.28	China	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
158.255.5.147	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.219.69.164	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
189.7.18.35	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.106.92.47	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
158.255.5.147	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.147	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.149.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.219.69.164	147.237.76.201	Taiwan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.219.69.164	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.47	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
104.172.175.169	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.53.34.118	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.53.34.118	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
176.13.20.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.53.34.118	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
2.53.34.118	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
119.122.237.96	China	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
79.180.7.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.29	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.148.104	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
23.91.70.119	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
119.122.237.96	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
119.122.237.96	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.230.19	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
209.173.241.141	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
119.122.237.96	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.29	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.230.19	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
149.78.52.195	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.110	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.101.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.210	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.66.20	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.145.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.34.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.110	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.189.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.142	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
178.154.189.38	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.210	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.53.46.110	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.110	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.210	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.146.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
62.0.116.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.218.66.107	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
158.255.5.147	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.102	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
74.82.47.50	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.255.5.147	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.160.242.40	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.219	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
159.226.95.66	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
213.8.204.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	5
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
91.109.30.91	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 91.109.30.91	Block	4
2.55.148.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.167.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.226.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
2.53.14.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.157.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.199.187.68	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.199.187.68	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
91.109.30.91	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.109.30.91	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3416.jpg	Block	1
17.142.157.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
91.109.30.91	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
80.246.130.94	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
119.122.237.96	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
82.102.136.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
46.19.85.110	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-19004-en/	Block	1
104.128.144.131	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
80.246.133.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
75.72.47.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.20.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	1
109.253.226.135	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
213.8.204.16	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
91.109.30.91	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
79.178.231.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
208.100.26.231	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.253.226.135	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/8/	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollpanebottom.gif	Block	1