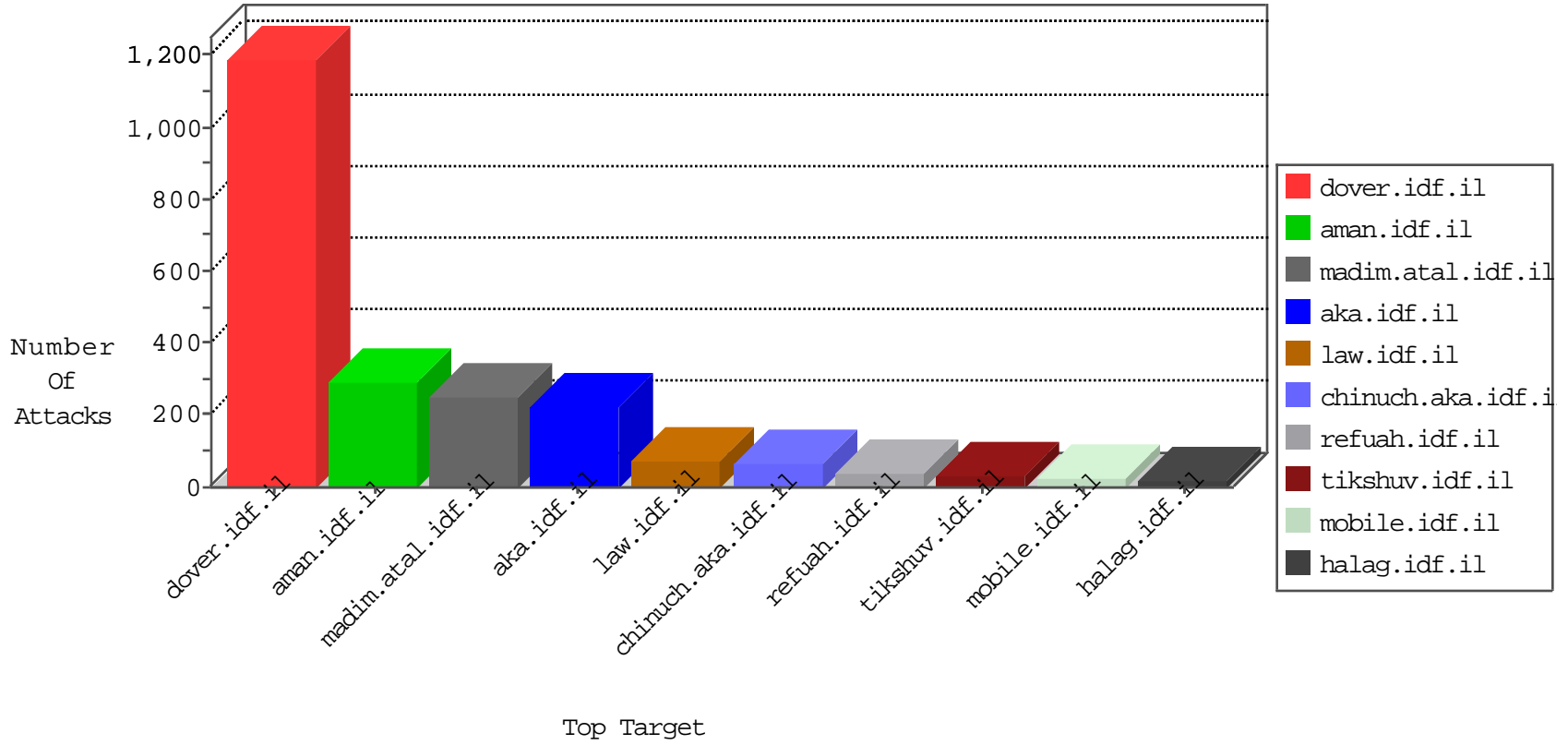


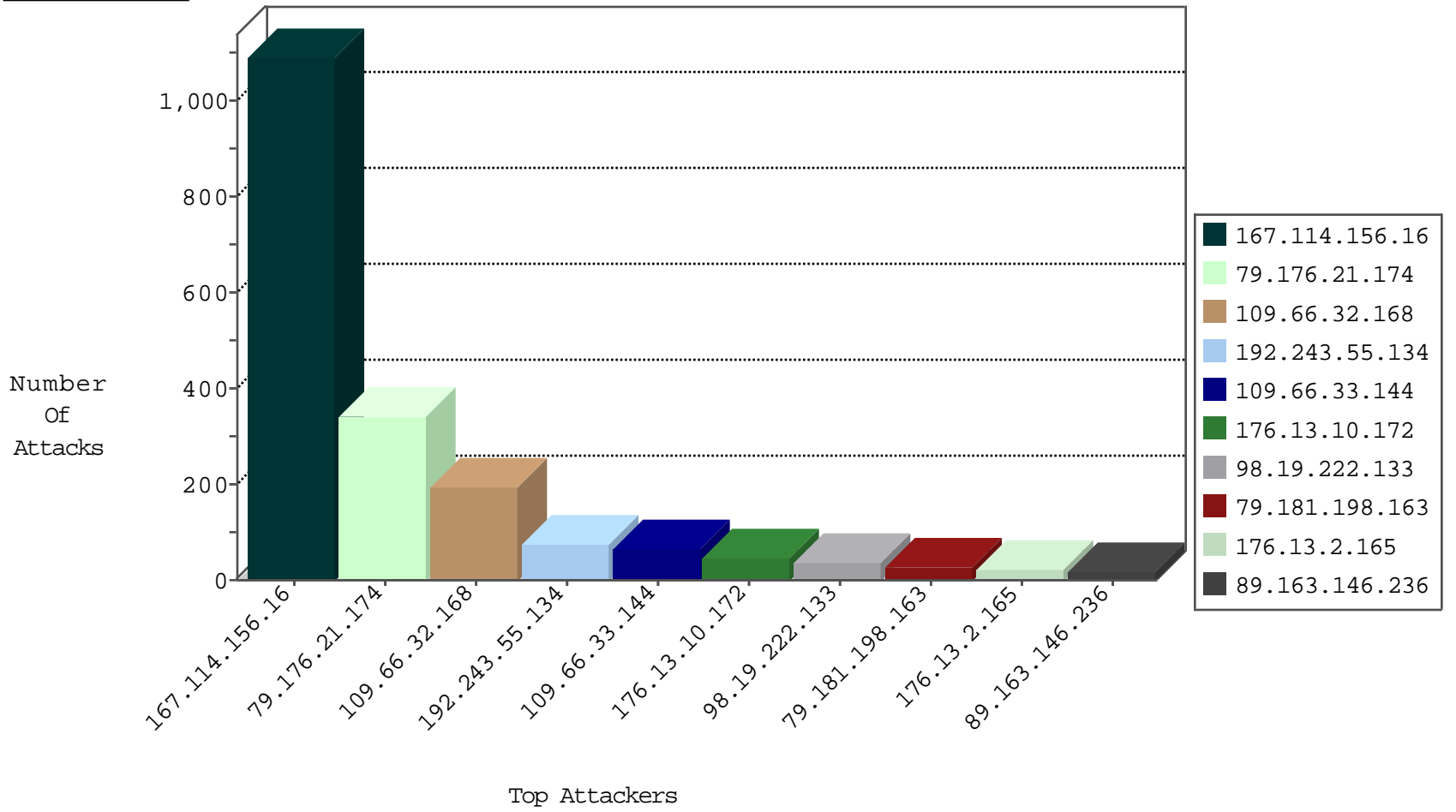
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3989
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.94.111.1		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1		147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.50	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
78.10.114.180	Poland	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
208.77.22.195	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
114.182.98.108	Japan	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.198.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
98.19.222.133	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	10
106.120.173.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
109.64.160.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.216.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
89.163.146.236	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.35	Germany	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
207.225.131.141	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.163.146.236	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.16	Germany	ny-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
52.33.159.204	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.0.16	Canada	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
52.33.159.204	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
89.163.146.236	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.163.146.236	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.8.46	Sweden	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.76.39	Chile	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
142.0.39.178	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
132.248.44.99	147.237.0.19	Mexico	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
52.33.159.204	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.0.16	Canada	ny-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
89.163.146.236	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.163.146.236	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.200.80.26	147.237.76.86	United Kingdom	navy.idf.il	SQL Injection - Select From	1
89.163.146.236	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.178.78	147.237.76.39	Chile	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
142.0.39.178	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
142.0.39.178	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.21.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	134
79.176.21.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	125
109.66.33.144	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
79.176.21.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	40
79.176.21.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
176.13.2.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
169.254.118.167		147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
87.71.114.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.179.170.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
84.229.244.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.43.98.13	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
87.68.244.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
79.178.39.75	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.177.51.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.123.234	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.102.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.71.57.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.183	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.96.98	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
2.54.19.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.1.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.39.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.101.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.33.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.19.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.43.98.13	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.157.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.25		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.11.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.155.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.138.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.71.120.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-11-2016-20:04:07 to 03-11-2016-21:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.205.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.57.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	192
176.13.10.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.185.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.22.131.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.137.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.226		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.84.1.27	Satellite Provider	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.29.41.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.172.229	Block	2
185.89.217.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.28.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
80.84.1.29	Satellite Provider	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.252.90.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.142.252.53	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
128.72.24.220	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter f	Block	1
87.70.28.124	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.71.30.28	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.136.195	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
128.72.24.220	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter l	Block	1
87.70.28.124	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
79.178.57.124	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.96	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
149.88.205.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.43.98.13	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
87.70.28.124	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx	Block	1
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
131.253.25.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.28.124	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
80.84.1.28	Satellite Provider	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.69.133.247	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/12.asp	Block	1
5.189.207.249	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
109.67.152.19	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.70.28.124	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 87.70.28.124	Block	1
66.249.64.175	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
141.101.132.125	Netherlands	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1