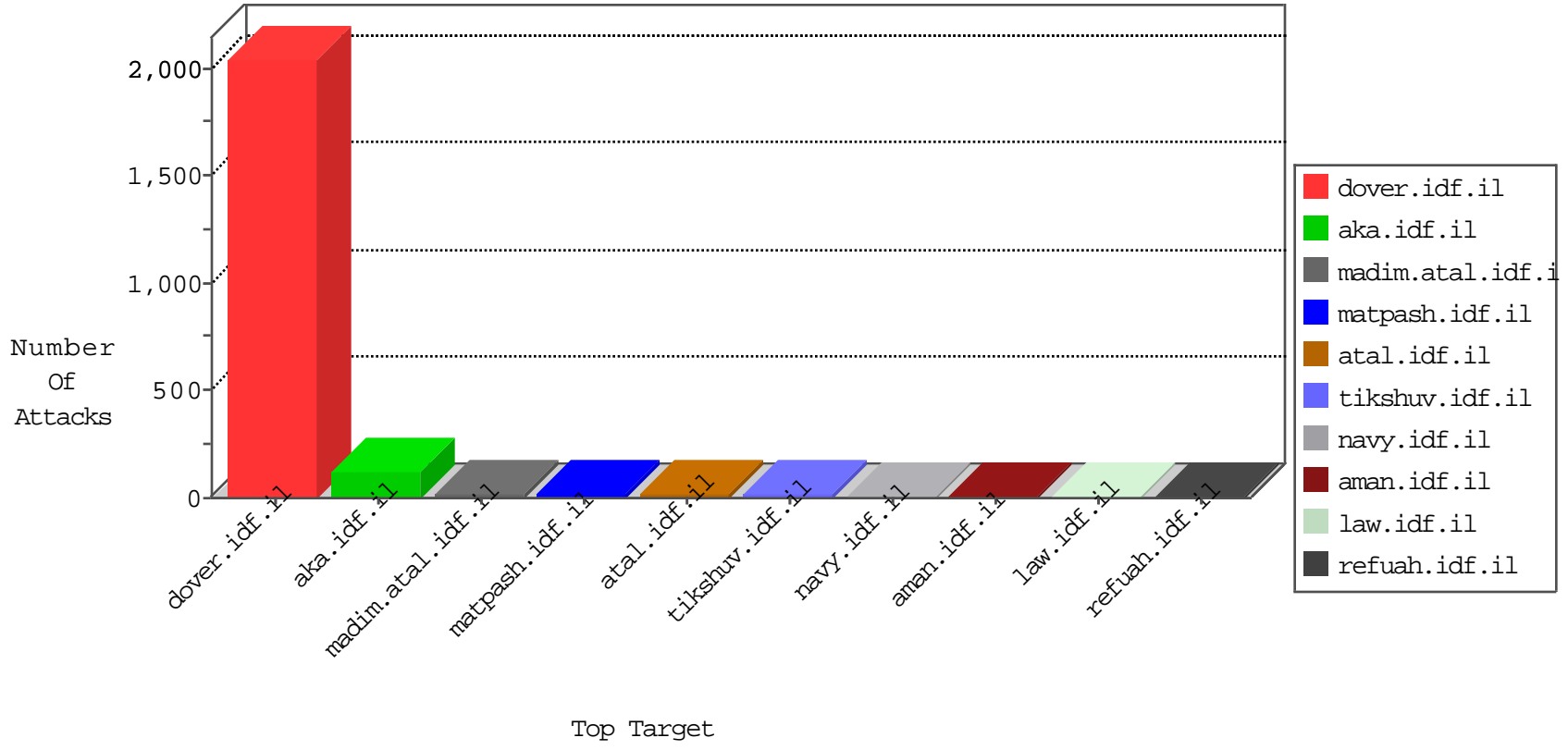


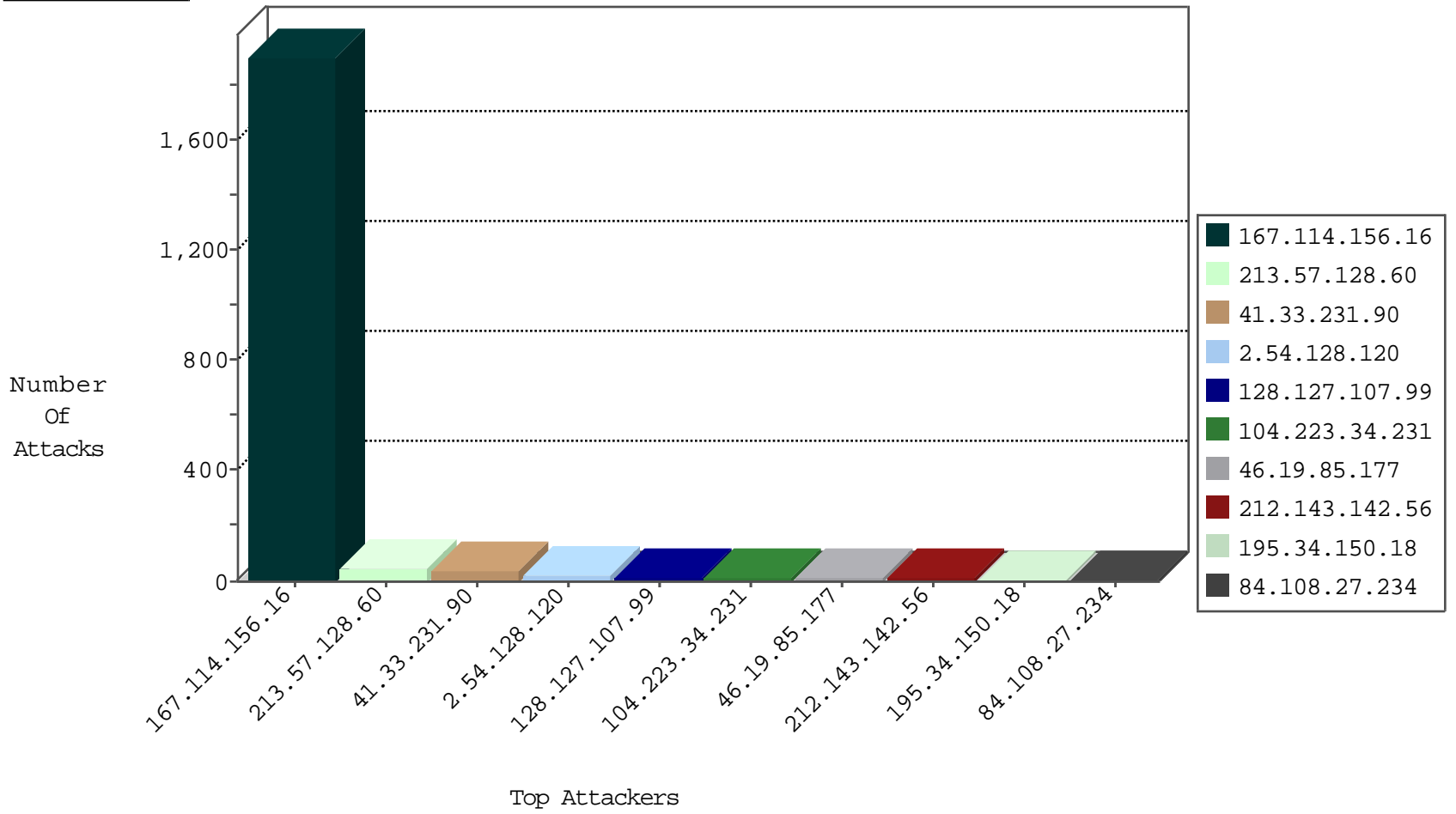
# IDF Under Attack Daily Report



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	3141
198.50.250.4	Canada	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
198.50.250.4	Canada	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
186.213.6.138	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.117.208.243	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.76.201	Hong Kong	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.223	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	1
58.56.98.132	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.231	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.244.78	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
123.232.26.132	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
87.197.159.157	147.237.76.198	Slovakia	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.104.49.211	147.237.72.14	China	dover.idf.il(ol	ET SCAN Potential SSH Scan	1
58.56.98.132	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
201.172.76.60	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.231	147.237.77.61		e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.244.82	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
123.232.26.132	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.128.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
213.57.128.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
213.57.128.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.108.27.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.1.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.178.215.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
104.223.34.231	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.254.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.47.79.216	Romania	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
149.78.27.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.90	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.141.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.127.107.99	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.186.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.132.8	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.128.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.127.107.99	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
81.218.132.8	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.149.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.140.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
128.127.107.99	Netherlands	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
80.178.157.105	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.148	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.39.191.63	Switzerland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.148	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
217.132.103.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.22.129.116	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.127.107.99	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
104.223.34.231	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
178.39.191.63	Switzerland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.141.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.223.34.231	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.104.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.253.205.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.86.66.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
104.223.34.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.219.106.162	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.163	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.18.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.128.120	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	15
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	6
93.118.79.249	Romania	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	4
128.127.107.99	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.52.145.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.125.113.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.37	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
69.163.152.114	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
208.113.160.8	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
37.26.147.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.77.216	dover.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
195.154.227.118	France	147.237.77.176	matpash.idf.il	Illegal HTTP Version HTTP/	Block	1
41.101.133.26	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.65.190.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.230.110.17	Turkey	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
149.78.78.178	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
97.100.147.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
195.154.227.118	France	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 195.154.227.118	Block	1
46.117.10.112	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.92.17.220		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.108.27.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
212.179.61.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
184.168.193.218	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
40.77.167.20	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
107.155.87.163	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
198.50.200.135	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.166.190.174	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.163.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.92.17.220		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.108.207.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.144.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.20	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.20	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1117-he/nakchal.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
61.6.1.112	Malaysia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/2/4912.png	Block	1
5.29.79.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.113.42.100	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzyz	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1