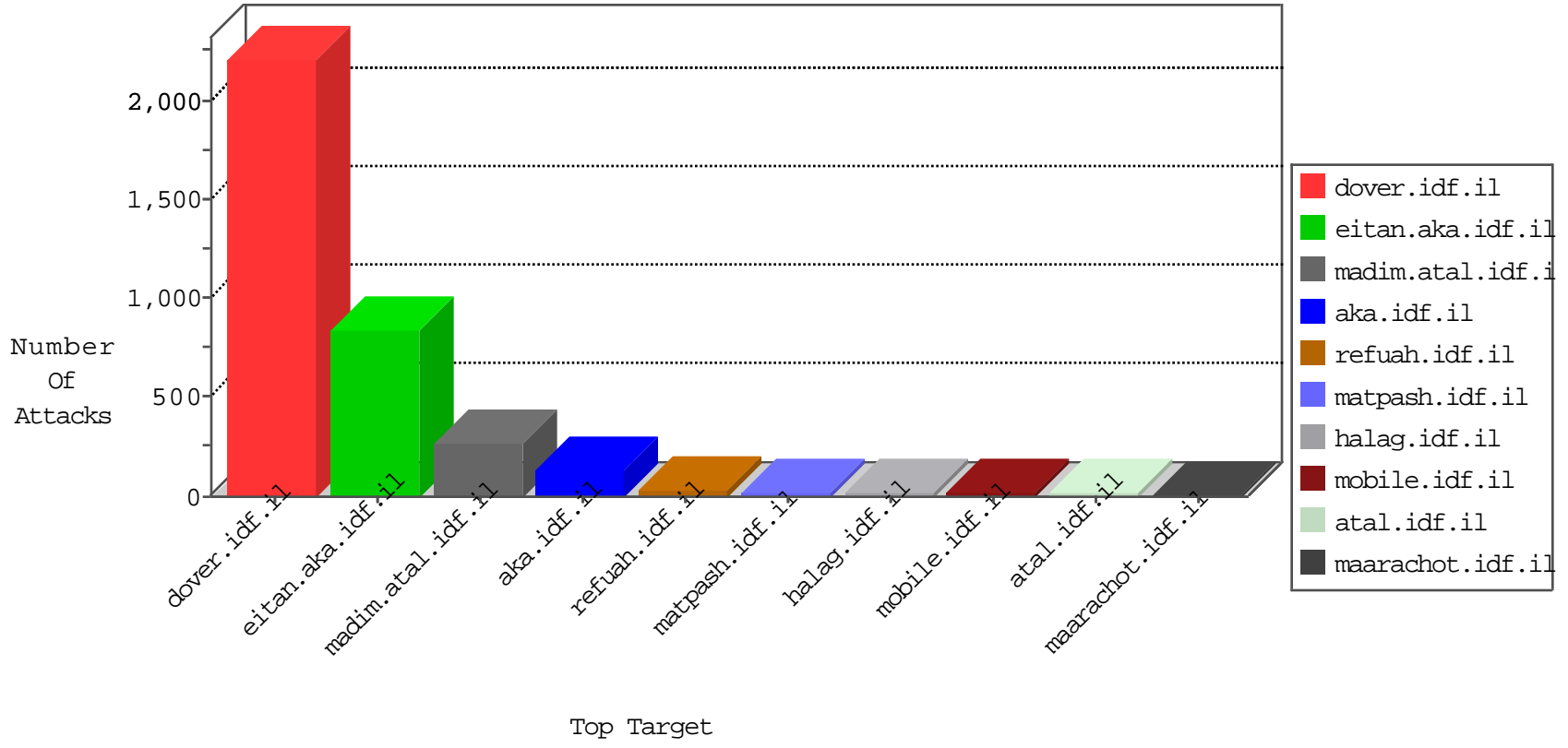


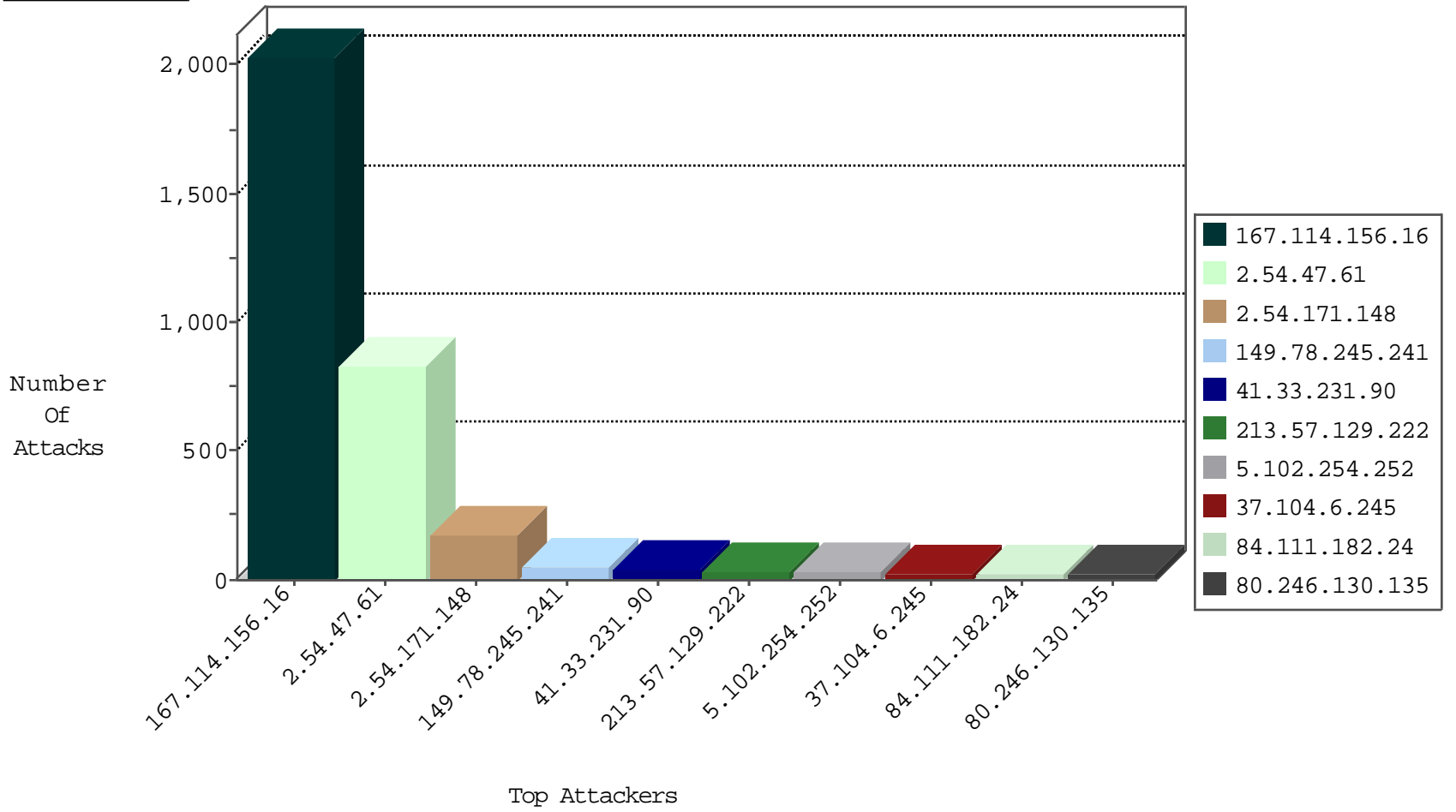
IDF Under Attack Daily Report



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	3493
216.4.56.168	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.166.188.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
106.75.199.220	China	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

12-25-2015-21:04:09 to 12-25-2015-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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	3
66.249.69.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.76.115.186	147.237.72.217	China	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
113.236.9.112	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.192.174.251	147.237.0.35	Morocco	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.99.203.248	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.80.155.223	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.130.5.207	147.237.8.46		e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.47.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	717
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.104.6.245	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
80.246.130.135	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.111.182.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
213.57.129.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.116.166.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.213.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.253.141.155	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.182.216.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
81.168.45.148	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.66.157.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.210.223	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.66.192.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.4.252.172	Lebanon	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
80.246.136.97	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
217.132.56.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.134.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.3.146.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.11.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.232.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
216.4.56.168	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
80.230.16.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.51.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.17.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.60.34.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
216.4.56.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.146.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
216.4.56.168	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.111.182.24	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.116.166.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.121.251.35	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.4.252.172	Lebanon	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.162.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.146.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.89.217.232		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.104.6.245	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.57.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.47.61	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.171.148	Block	53
149.78.245.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
5.102.254.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.171.148	Block	14
149.78.245.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
31.154.90.124	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
79.183.203.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.230.240	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	3
31.154.90.124	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 31.154.90.124	Block	3
5.28.135.217	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
2.54.12.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.255.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
109.253.146.183	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.120.236.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.56.247	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 217.132.56.247	Block	2
176.228.136.200	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.228.136.200	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
50.31.26.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
89.31.140.31	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
84.111.182.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
40.77.167.20	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/contactus.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.126.69.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
103.23.20.117	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
89.31.140.10	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
31.154.90.124	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=1c5cf4b1kkkkkkk_1c5cf4b1	Block	1
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
109.64.68.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.87.161.155	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
89.31.140.40	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp/wp-admin/	Block	1
85.65.168.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
46.166.186.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.31.140.11	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wordpress/wp-admin/	Block	1
37.19.120.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.88.25.143		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/	Block	1
80.246.136.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1