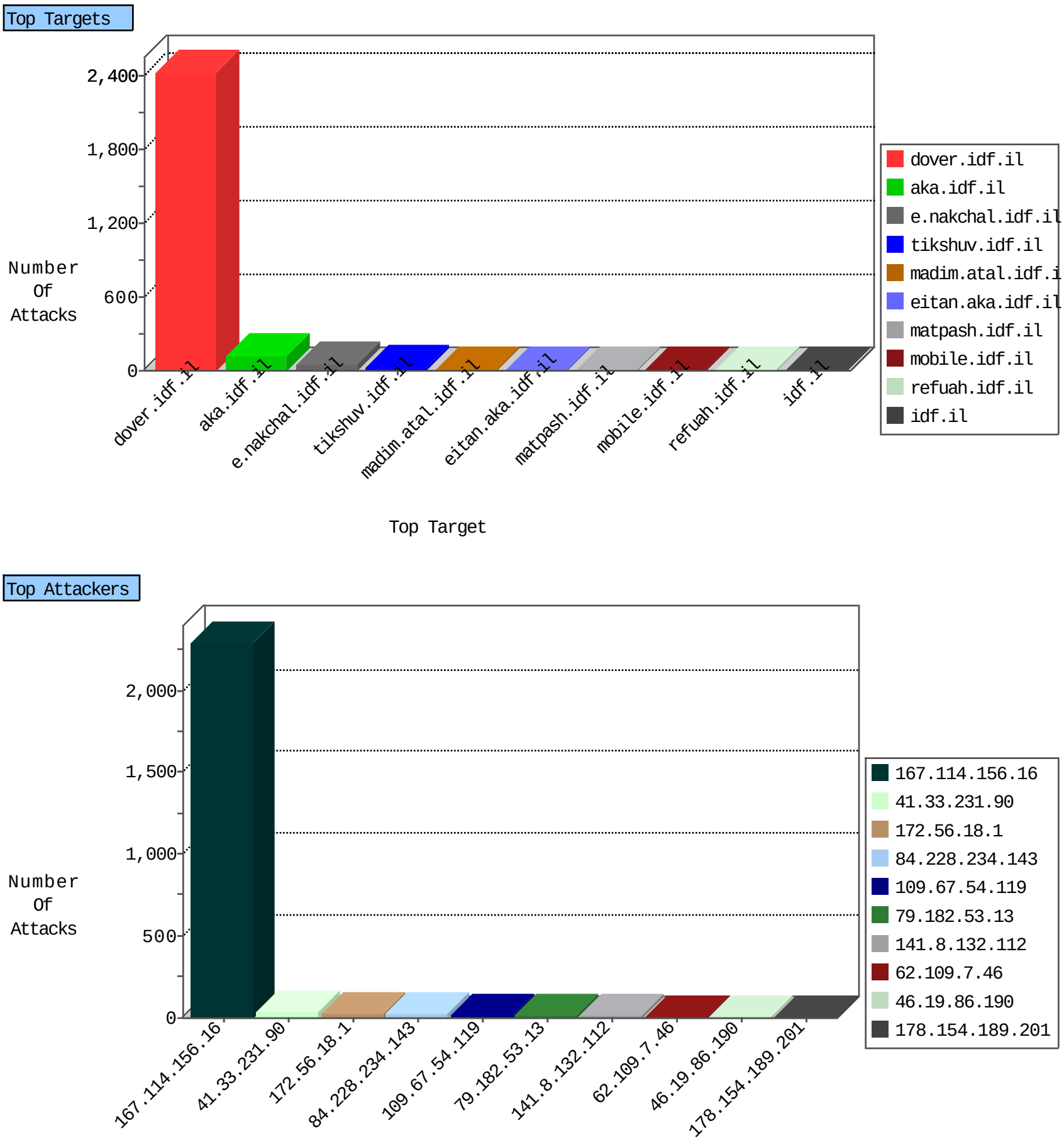
01-26-2016-01:07:54 to 01-26-2016-02:07:54

IDF Under Attack Daily Report



01-26-2016-01:07:54 to 01-26-2016-02:07:54

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	3037
49.80.254.226	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	6
14.209.240.45	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	5
101.228.246.121	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	5
58.58.183.2	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	5
180.118.31.168	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
183.142.131.166	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
120.39.148.218	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
60.181.28.172	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
58.45.121.27	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
221.126.136.45	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
112.156.90.103	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
60.180.2.126	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
118.248.41.23	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
218.2.244.94	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
185.56.28.67	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
119.127.42.126	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.38.12.22	Netherlands	147.237.76.198	e.yohalan.idf.il	L4 Source or Dest Port Zero	drop	1

01-26-2016-01:07:54 to 01-26-2016-02:07:54

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
42.101.154.233	China	147.237.77.216	dover.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	1
62.109.7.46	Russian Federation	147.237.77.216	dover.idf.il	C196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
188.165.15.49	France	147.237.72.167	ishurim.aka.idf.i	C228: HTTP: AhrefBot crawler	Block	1

01-26-2016-01:07:54 to 01-26-2016-02:07:54

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.143.82.50	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
37.143.82.50	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
101.2.168.215	147.237.0.33	Australia	idf.il	ET SCAN NMAP -sS window 2048	1
101.2.168.215	147.237.0.33	Australia	idf.il	ET SCAN NMAP -f -sS	1
82.145.33.11	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
62.109.7.46	147.237.77.216	Russian Federation	dover.idf.il	SERVER-WEBAPP admin.php access	1
37.143.82.50	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.72.167	Latvia	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.115	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
101.2.168.215	147.237.0.33	Australia	idf.il	ET SCAN NMAP -sS window 1024	1
89.163.148.90	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-01:07:54 to 01-26-2016-02:07:54

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
109.67.54.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.228.234.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
172.56.18.1	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.189.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.234.143	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
103.231.94.76	Myanmar	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
172.56.18.1	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
172.56.18.1	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
172.56.18.1	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.176.24.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.73.248.230	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.197.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.198.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.12.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.164.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.195.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.215.0.164	Sierra Leone	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.22	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.0	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
191.240.136.5	Brazil	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.187	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
54.196.208.206	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
172.56.18.1	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.29.194.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
191.240.136.5	Brazil	147.237.76.196	e.sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.187	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

01-26-2016-01:07:54 to 01-26-2016-02:07:54

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.212.122.176	United States	147.237.0.200	m4u.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
79.182.53.13	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.53.13	Block	11
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	4
62.109.7.46	Russian Federation	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 62.109.7.46	Block	3
62.109.7.46	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.109.7.46	Block	3
109.66.123.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
62.109.7.46	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
109.253.196.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.147.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
79.182.53.13	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/transportation.asp	Block	1
42.101.154.233	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.12.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
104.238.93.79		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	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
192.157.245.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
42.101.154.233	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/90sec.php	Block	1
180.76.15.33	China	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	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
79.176.9.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.49.104.44	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
149.78.163.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
184.168.193.47	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
197.49.104.44	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.209	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
85.214.11.209	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
217.199.187.68	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
185.110.109.191		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.34.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
65.132.59.34	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.164.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.236.224.114	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
94.102.51.30	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/plugins/content/plugin_googlemap2_proxy.php	Block	1
67.212.175.138	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
46.105.220.179	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1