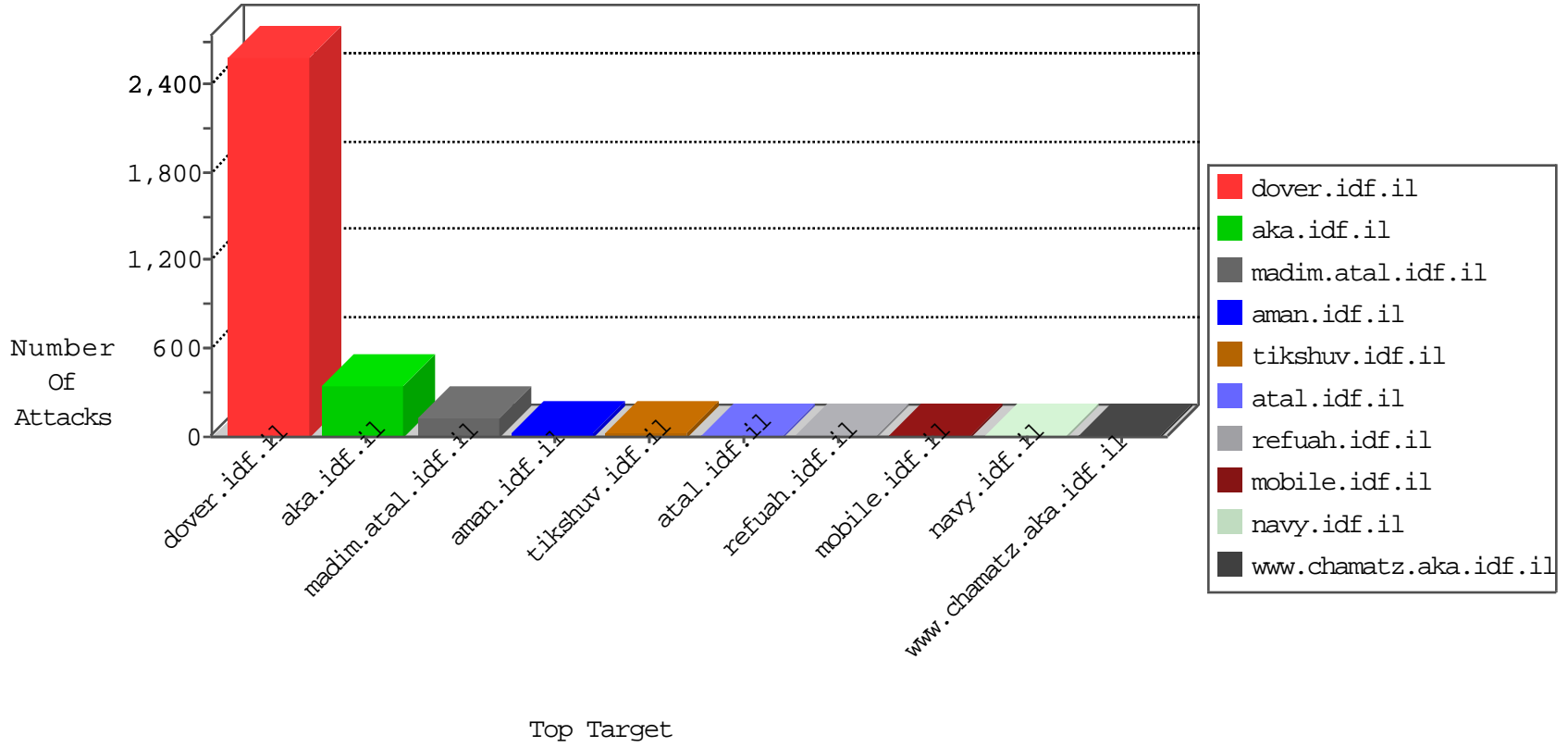


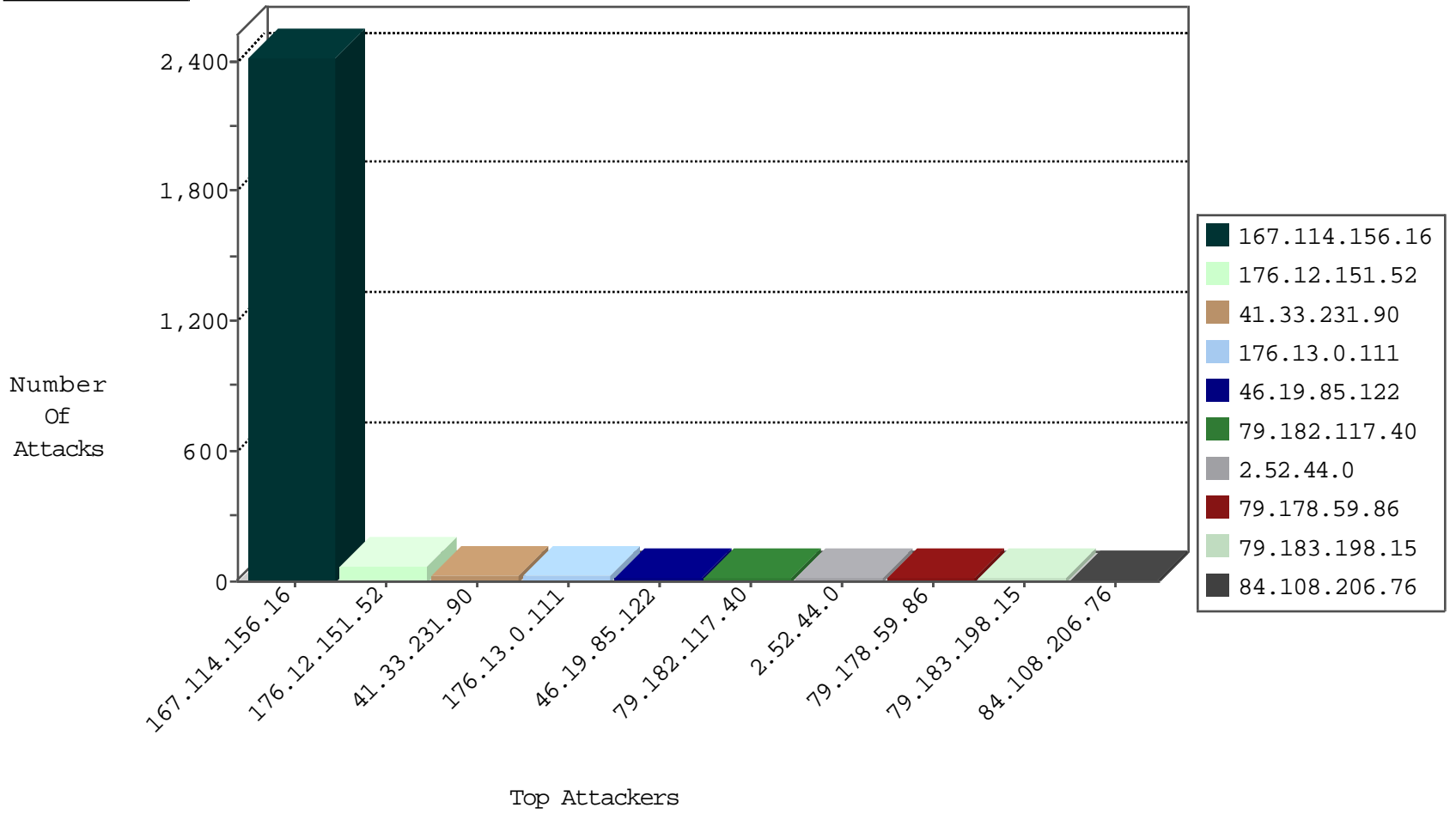
IDF Under Attack Daily Report



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	3383
192.168.1.207		147.237.0.34	tikshuv.idf.il	Anomaly-TCP-shortheadr	dest-reset	2
208.67.1.66	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
151.100.17.112	Italy	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
208.67.1.66	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.187.221.12	Lebanon	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
2.54.169.221	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
89.187.221.12	147.237.77.216	Lebanon	dover.idf.il	SQL Injection - Select From	1
79.181.225.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.120.16.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
182.75.6.126	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.170.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.187.221.12	147.237.77.216	Lebanon	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
79.177.205.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.211.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.146.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	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	30
79.178.59.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.198.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
84.108.206.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.182.117.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.85.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
188.120.148.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.10.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.74.150.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.25.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.211	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.8.234	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.250.26.212	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.125.105.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.1.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.63.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.19.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.59.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.27.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.194.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.117.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.55	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.146.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.117.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.57.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.204	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.160.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.60.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.251.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.31	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.207.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.44.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.57.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.190.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.37.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.100.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

12-22-2015-17:04:03 to 12-22-2015-18:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.35.33	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
176.12.151.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.13.0.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.52.44.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
79.176.112.129	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.112.129	Block	6
176.13.21.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.114.23.208	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nosuchpage123	Block	2
84.94.103.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	2
193.17.1.25	Slovenia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	2
93.172.154.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
50.56.176.183	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	2
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.190.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
185.32.179.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
141.212.122.80	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 141.212.122.80	Block	1
84.109.192.142	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
37.142.68.28	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.66.194.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.215.251	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	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
2.54.45.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.187.221.12	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/~nosuchpage123	Block	1
54.235.159.206	United States	147.237.72.166	aka.idf.il	Cross-site scripting on url in aka.idf.il/main/giyus/	Block	1
85.250.95.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.169.206.107	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.74.150.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.13.102.104	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.112.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
213.57.49.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
2.52.160.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.139.33.237	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.139.33.237	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
190.206.16.65	Venezuela	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
149.78.139.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.212.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.187.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
109.67.122.113	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1
79.179.130.77	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
212.116.166.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.144.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.187.221.13	Block	1
86.104.177.146	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1