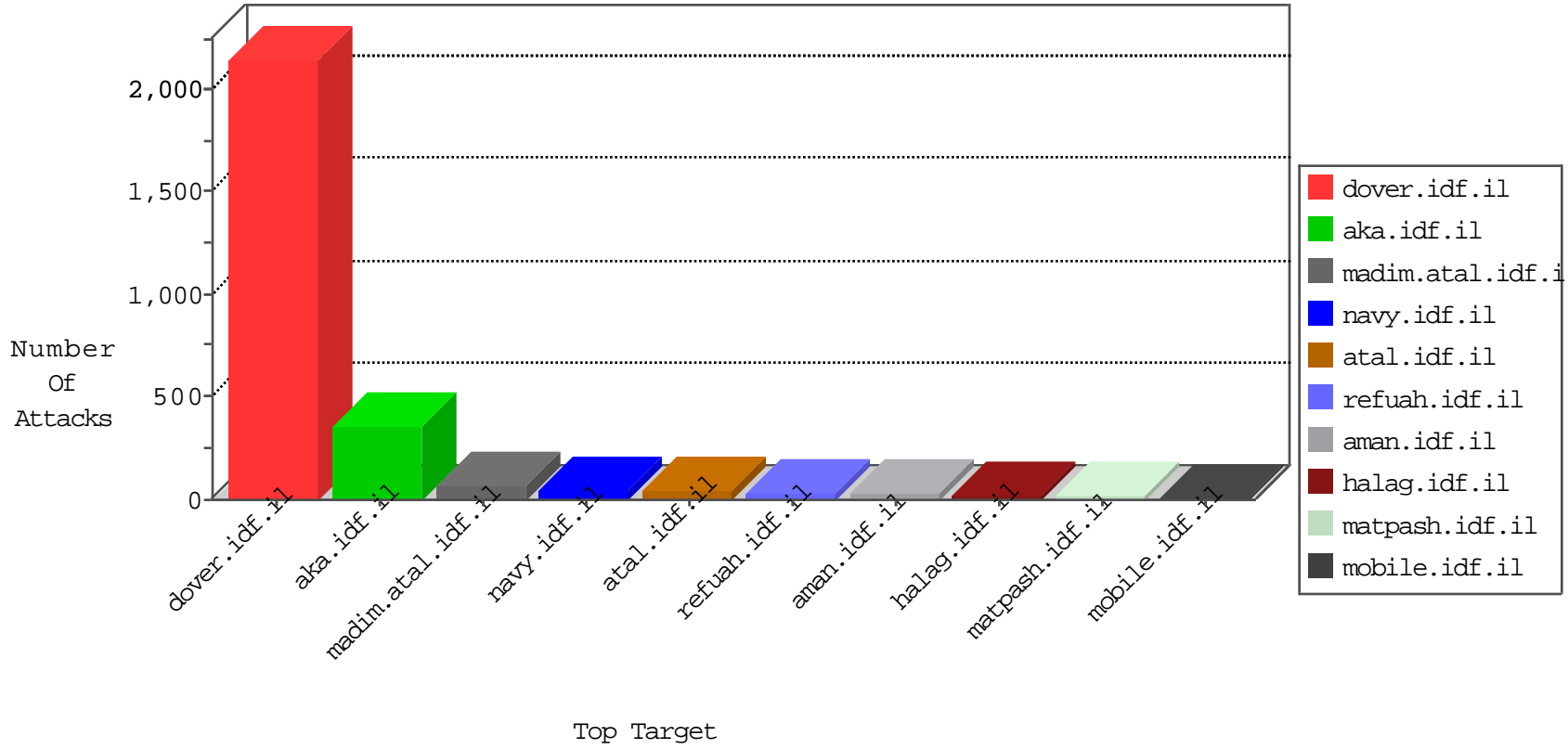


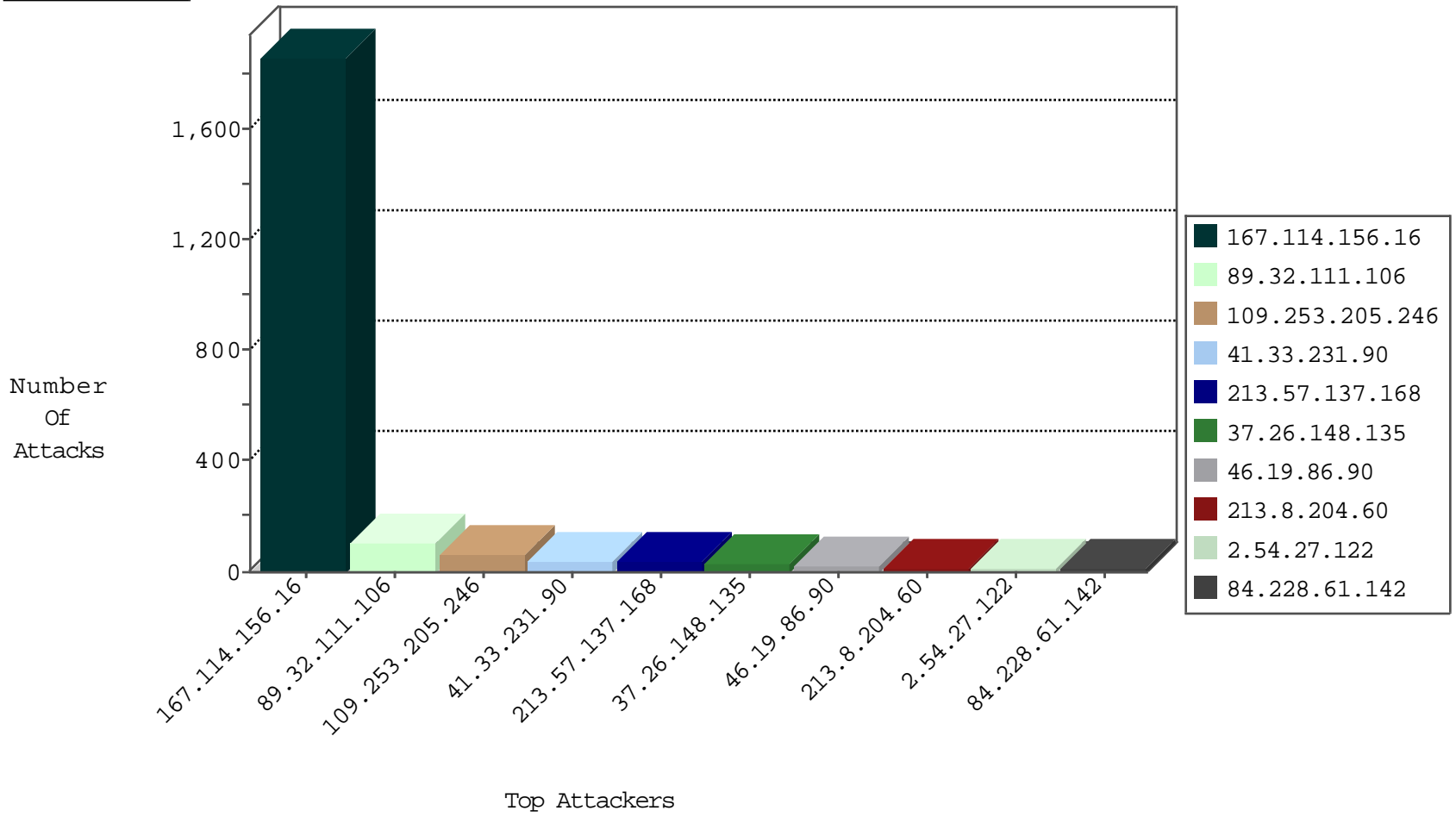
# IDF Under Attack Daily Report



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	3107
178.250.35.60	Lithuania	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
77.247.178.132	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-24-2015-20:04:06 to 12-24-2015-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
190.208.55.250	147.237.8.50	Chile	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
77.125.10.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
46.151.52.16	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
37.143.82.50	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
162.222.185.165	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
5.230.134.108	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.76.197	Cote D'Ivoire	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
190.208.55.250	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
190.208.55.250	147.237.72.167	Chile	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.59.33.61	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
190.208.55.250	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.208.55.250	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.164.250.73	147.237.8.28	Croatia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
189.198.118.62	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.52.16	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
37.143.82.50	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
182.18.170.77	147.237.0.34	India	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -f -sS	1
162.222.185.165	147.237.76.147	United States	chinuch.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
190.208.55.250	147.237.76.197	Chile	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.59.33.61	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
190.208.55.250	147.237.0.35	Chile	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.122.188.184	147.237.77.243	Romania	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.198.118.62	147.237.77.234	Mexico	halag.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
89.32.111.106	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
89.32.111.106	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
89.32.111.106	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
213.57.137.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
213.57.137.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
66.249.69.122	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.135	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	12
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.90	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
94.230.86.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.177.158.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
188.120.148.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.43	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
149.78.173.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.110.35.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.61.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.29.113.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.35.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.173.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.61.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.35.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.130.106.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.148.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.148.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.113.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.64.25.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.64.25.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.78.236.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.230	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.252.113.116	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.54.27.122	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.227	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.228.172.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
109.64.176.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.63.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.171	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (403) in Session from 213.8.204.60	Block	13
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	2
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	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
79.177.182.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.207.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.46.13.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
85.64.230.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
84.109.17.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.13.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.116.140.62	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationsservice.asmx/getauthuser	Block	1
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.142.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: returnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
79.183.216.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.254.246	Israel	147.237.76.30	himush.idf.il	PHP Attempt	Block	1
89.139.42.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
79.177.49.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
84.228.64.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.11.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.95.208.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.202.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.63.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.230.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.85.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.109.216.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/images/2001/may/22may01_1dotjpg	Block	1
195.154.194.111	France	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
80.246.137.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.254.246	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/xmlrpc.php	Block	1
94.230.86.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.158.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/www.idf.il	Block	1
212.116.177.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.172.130	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.108.70.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.72.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.5.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.64.176.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.175.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.230.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.34.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1