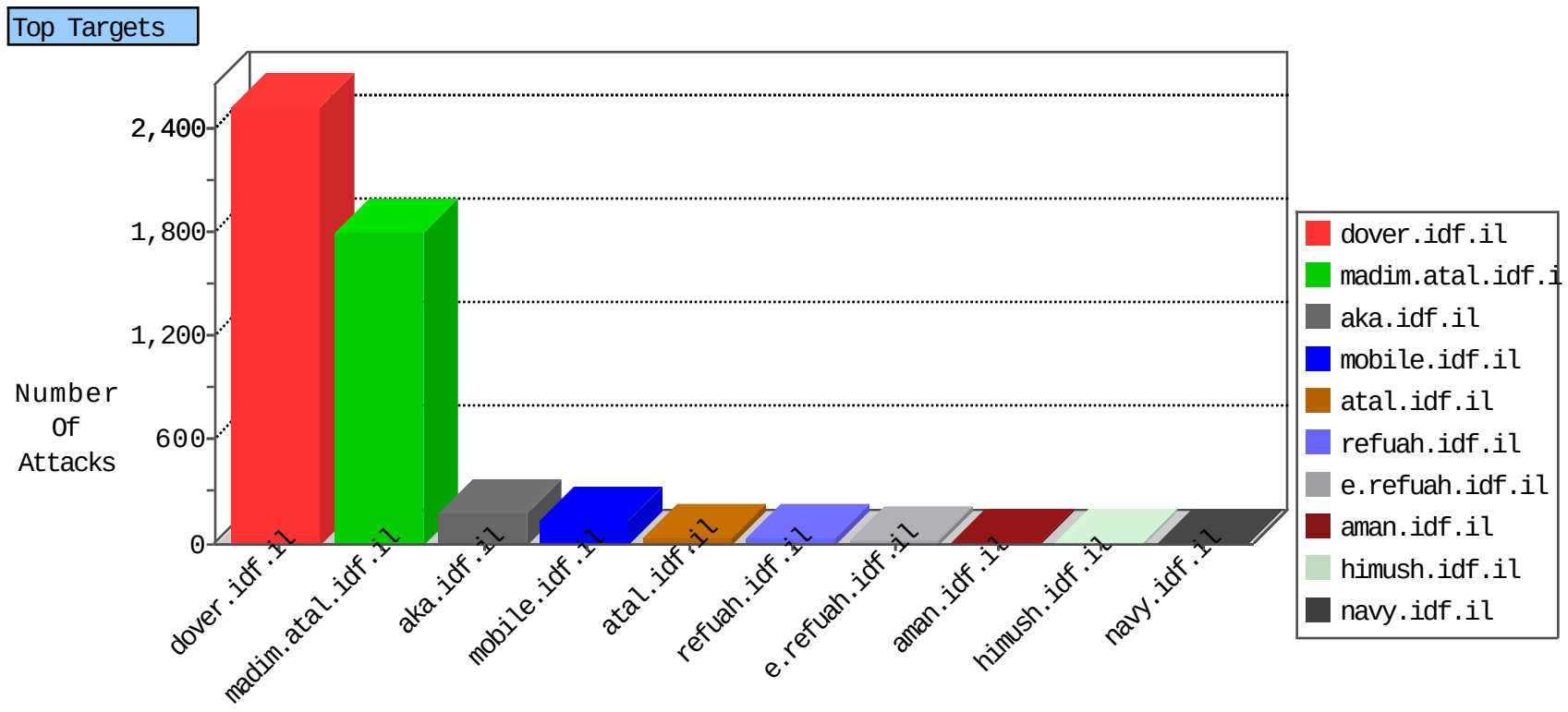
01-23-2016-14:04:02 to 01-23-2016-15:04:02

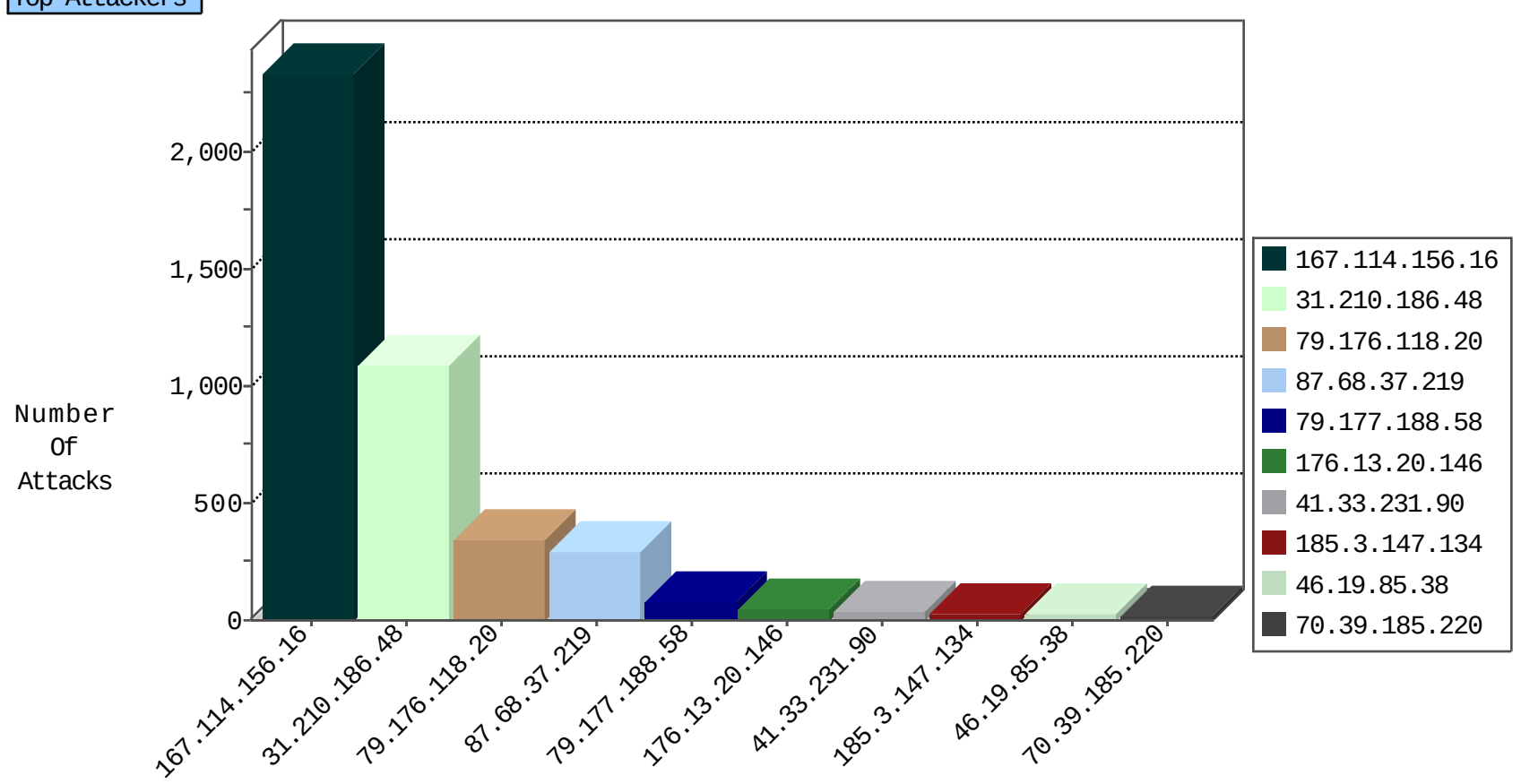
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-23-2016-14:04:02 to 01-23-2016-15:04:02

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	3088
23.95.54.18	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
23.95.54.18	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
80.246.130.157	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
23.95.54.18	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

01-23-2016-14:04:02 to 01-23-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2

01-23-2016-14:04:02 to 01-23-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.210.186.48	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.177.168.107	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
117.21.248.87	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.231.180.23	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.200	Latvia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.65.165.215	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.111.166	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

01-23-2016-14:04:02 to 01-23-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.3.147.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
70.39.185.220	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	15
216.72.40.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
5.29.121.211	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.22.135.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.120.148.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
178.48.247.116	Hungary	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.117.177.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
31.210.187.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.139.172.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.131.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.28.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.93.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.13.151	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
89.139.172.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.144.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.135.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.144.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.128.62.1	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.4.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.106.47.57	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
31.210.187.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
110.168.229.115	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.186.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.184	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.181.195	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.26.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.119.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.152.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.212.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.89.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-23-2016-14:04:02 to 01-23-2016-15:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.253.135.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.184.149	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
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	672
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	264
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	205
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	148
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.177.188.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	55
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 79.176.118.20	Block	28
176.13.20.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
197.118.35.20	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.118.35.20	Block	6
79.177.188.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
2.54.42.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.182.134.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.3.147.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.56.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.170.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.16.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
188.120.148.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.26.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
65.52.240.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	2
185.3.147.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
41.96.201.79	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	2
54.158.73.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
185.32.179.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.62.87.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
5.102.213.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.96.93.58	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/information.aspx	Block	1
197.118.77.247	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
87.69.135.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.160.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.151	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
41.42.179.235	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.28.159.183	Israel	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	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8956-he/refuah.aspx	Block	1
54.201.13.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.15	China	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/994-9736-he/refuah.aspx	Block	1
82.145.208.174	Europe	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
31.168.201.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.130.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.126.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1