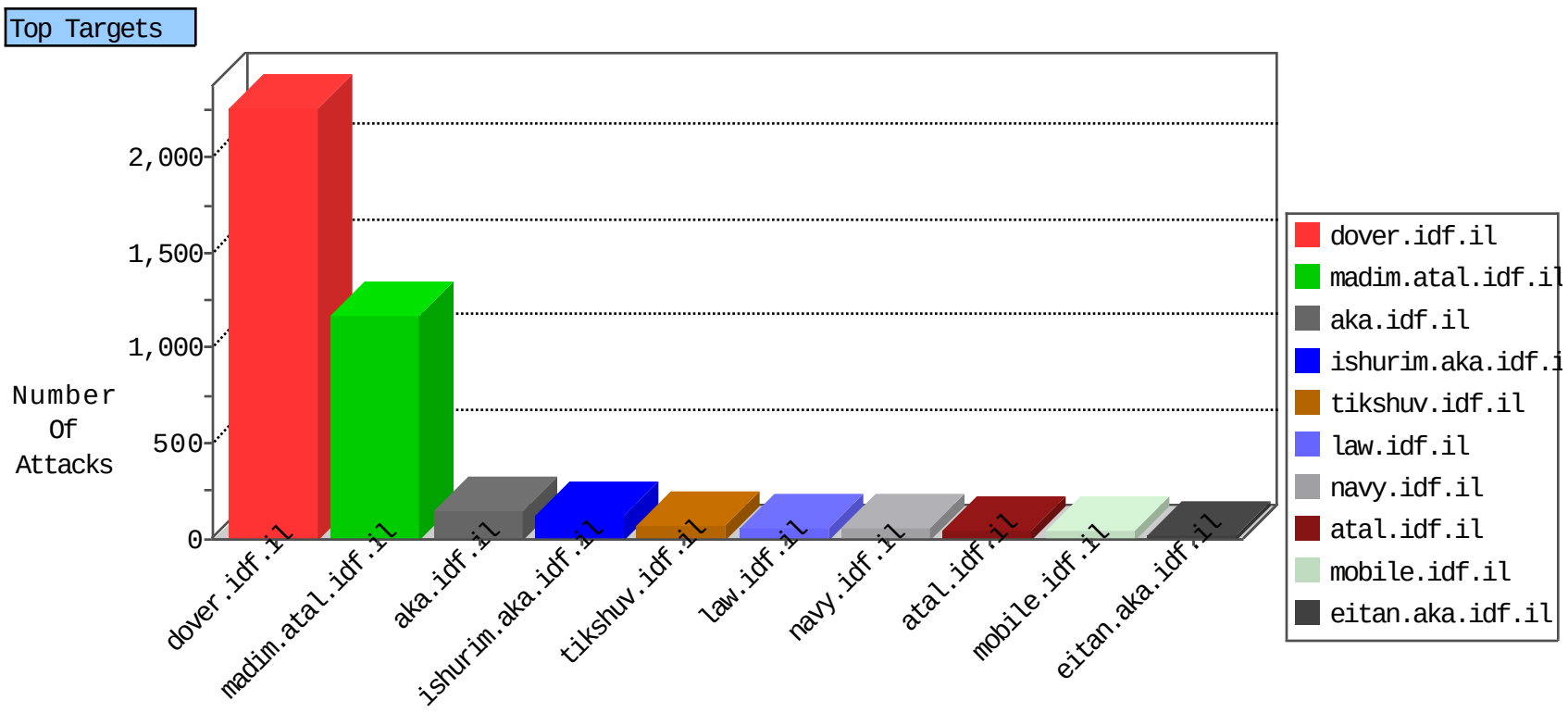
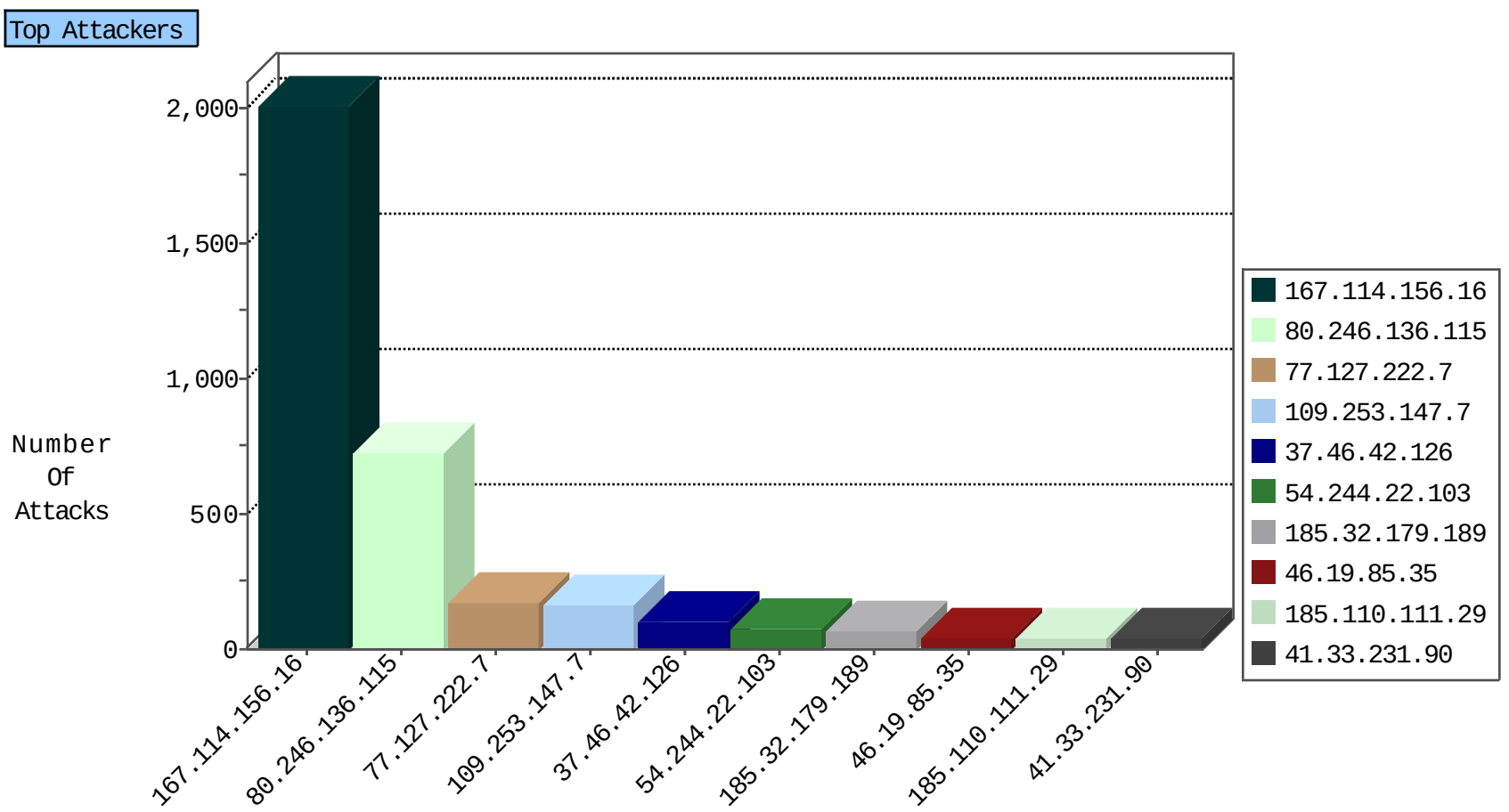
01-12-2016-23:04:04 to 01-13-2016-00:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-12-2016-23:04:04 to 01-13-2016-00:04:04

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	3003
46.120.102.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.160.164.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.158.166	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
91.121.100.46	France	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-23:04:04 to 01-13-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-12-2016-23:04:04 to 01-13-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.115	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	10
213.8.204.59	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.247	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.78.93	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
185.110.111.29	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sA (2)	2
89.248.167.162	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.129.55.113	147.237.72.14	France	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.129.55.113	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
80.246.133.231	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.166.33.184	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.166.33.184	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
61.166.33.184	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
61.166.33.184	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.129.55.113	147.237.77.216	France	dover.idf.il	ET SCAN Potential SSH Scan	1
61.166.33.184	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.129.55.113	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.166.33.184	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.166.33.184	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.166.33.184	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
61.166.33.184	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.166.33.184	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1

01-12-2016-23:04:04 to 01-13-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	65
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
109.66.223.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.35	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	13
2.52.31.143	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.173.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
187.39.234.202	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
93.173.142.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.8.204.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
213.8.204.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.35	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.116.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.59.139.45	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
173.208.136.170	United States	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.130.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.68.44.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
89.139.171.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.92.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.35	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.186.65	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.168.32	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.35	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
87.68.61.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	4
109.67.41.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.19.116.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.96.181	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.253.28	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.133.231	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.203.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.210.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.163.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.69.165.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
188.120.148.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.130.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.219.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-12-2016-23:04:04 to 01-13-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	331
80.246.136.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	286
37.46.42.126	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 37.46.42.126	Block	101
109.253.147.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
77.127.222.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
80.246.136.115	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.115	Block	92
77.127.222.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
109.253.147.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
185.32.179.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
185.110.111.29		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.16	Block	20
2.52.31.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.54.27.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.3.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.66.183	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.108.66.183	Block	2
37.26.147.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.66.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
79.183.64.163	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.111.14.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.51.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.139.136.35	Israel	147.237.77.233	atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	1
83.130.115.195	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
37.46.42.126	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many 404: Response Code per Session	Block	1
149.88.97.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.101.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter answerid in www.aka.idf.il/sachar/login/	None	1
109.64.52.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1
46.148.18.74	Lithuania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.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
84.228.141.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.238.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
89.139.136.35	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1121-he/atal.aspx	Block	1
66.249.64.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
84.19.190.106	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
186.56.4.3	Argentina	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.54.48.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	1
79.177.188.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.11.212	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
77.126.29.111	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
46.166.186.204	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.64.28.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.196.72.199	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.116.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.176.12.245	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.73.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

01-12-2016-23:04:04 to 01-13-2016-00:04:04