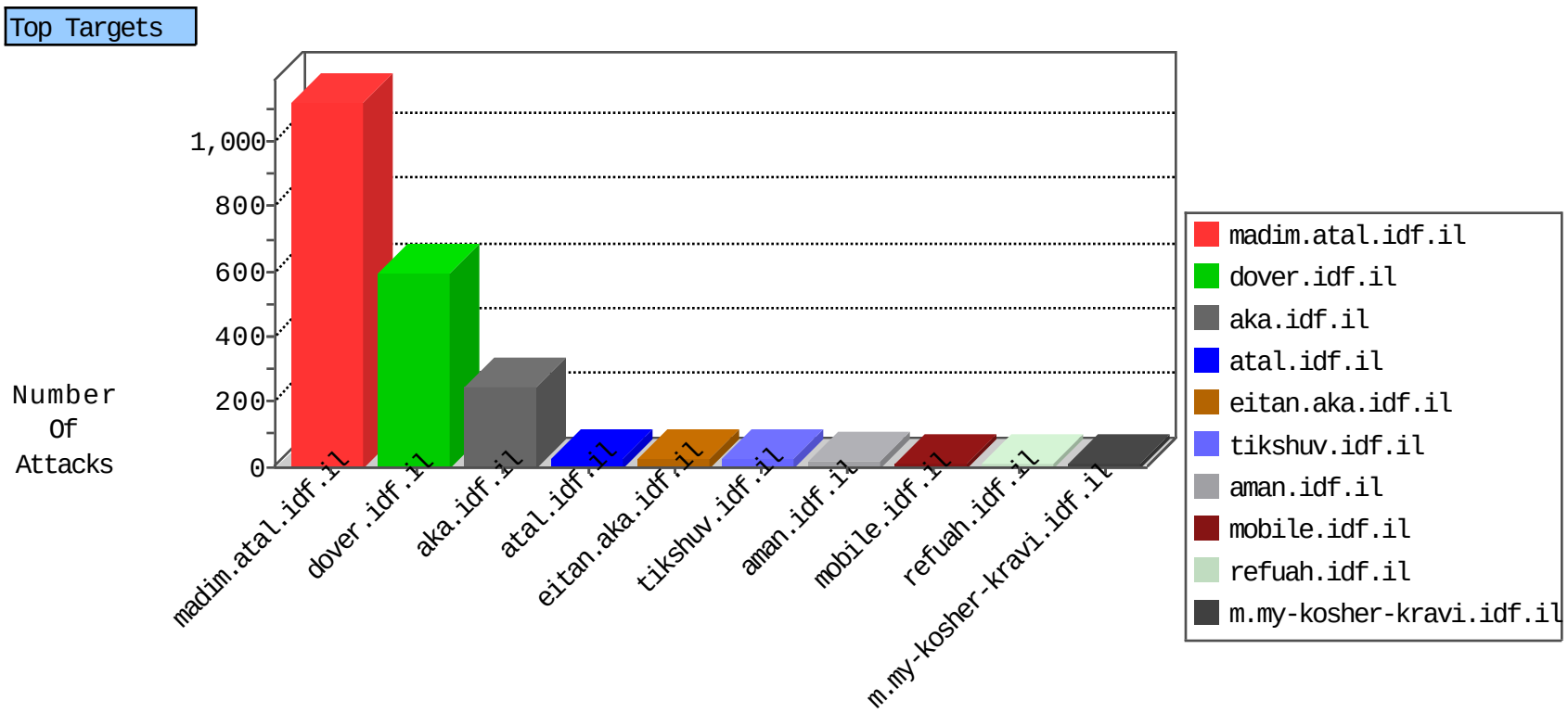
11-21-2015-15:04:01 to 11-21-2015-16:04:01

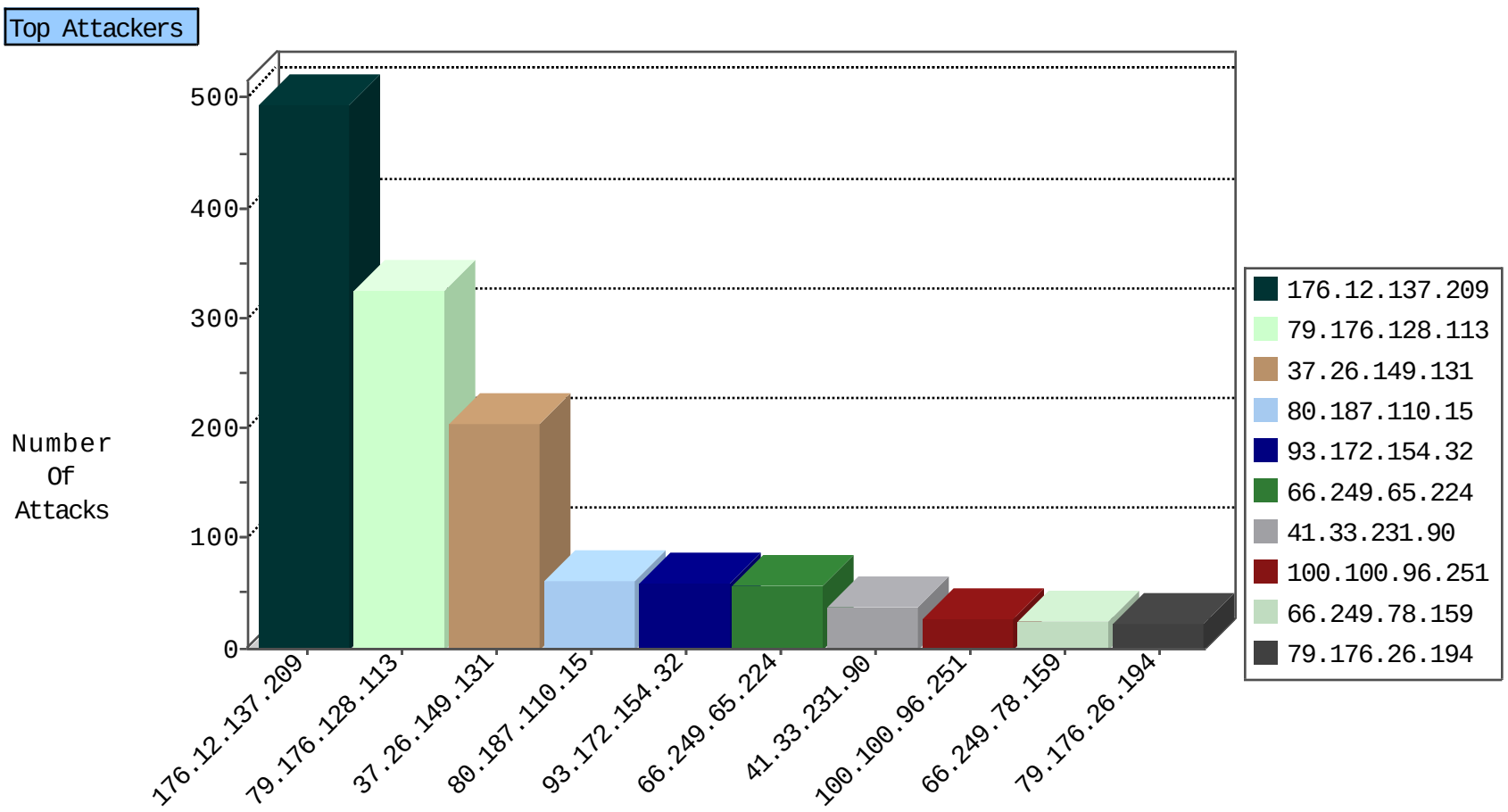
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-21-2015-15:04:01 to 11-21-2015-16:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.78.252.13	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	442
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	67
31.210.187.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.85.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.179.206.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.119.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
218.205.20.41	China	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
37.26.147.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.82.64.198	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-15:04:01 to 11-21-2015-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.176.19	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-21-2015-15:04:01 to 11-21-2015-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.12.137.209	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.26.149.131	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.224	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.219.144.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.77.216	Poland	dover.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
46.166.190.177	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
176.77.80.120	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
125.65.165.215	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
119.73.228.130	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
119.73.228.130	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

11-21-2015-15:04:01 to 11-21-2015-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.187.110.15	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
100.100.96.251		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.57.141.219	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
2.54.35.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
100.100.104.20		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.176.26.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
104.131.197.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.208.180	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.38.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.64.160		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
156.197.101.28		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.176.26.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.26.147.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.64.179.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.59.229		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.201.171.84	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.119.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.48.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.139.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
173.252.89.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.116.172.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.109.235.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.98.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.194.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
85.65.93.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.67.174.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.210.187.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.139.38.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.133.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.139.38.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.119.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.176.48	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.116.172.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.61.221	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
65.55.215.44	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.138.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	290
79.176.128.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	203
79.176.128.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.12.137.209	Block	80
93.172.154.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.54.144.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
31.154.152.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.64.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	3
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.178.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.90.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.76.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.183.32.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.140	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.32.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.111.38.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.48.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.117.242.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.24.76.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/&sa=u&ei=zqsutjfxmn-fopdm-pkb&ved=0cauqfjaa&usg=afqjcnf2apehywz9apusaqdzaz5_jkfq7g	Block	1
173.252.90.246	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
2.54.7.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.86.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.132	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
65.55.215.44	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
109.64.42.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.172.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
173.252.120.123	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
41.143.110.168	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
2.54.26.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.93.136	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
213.57.43.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.98.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1