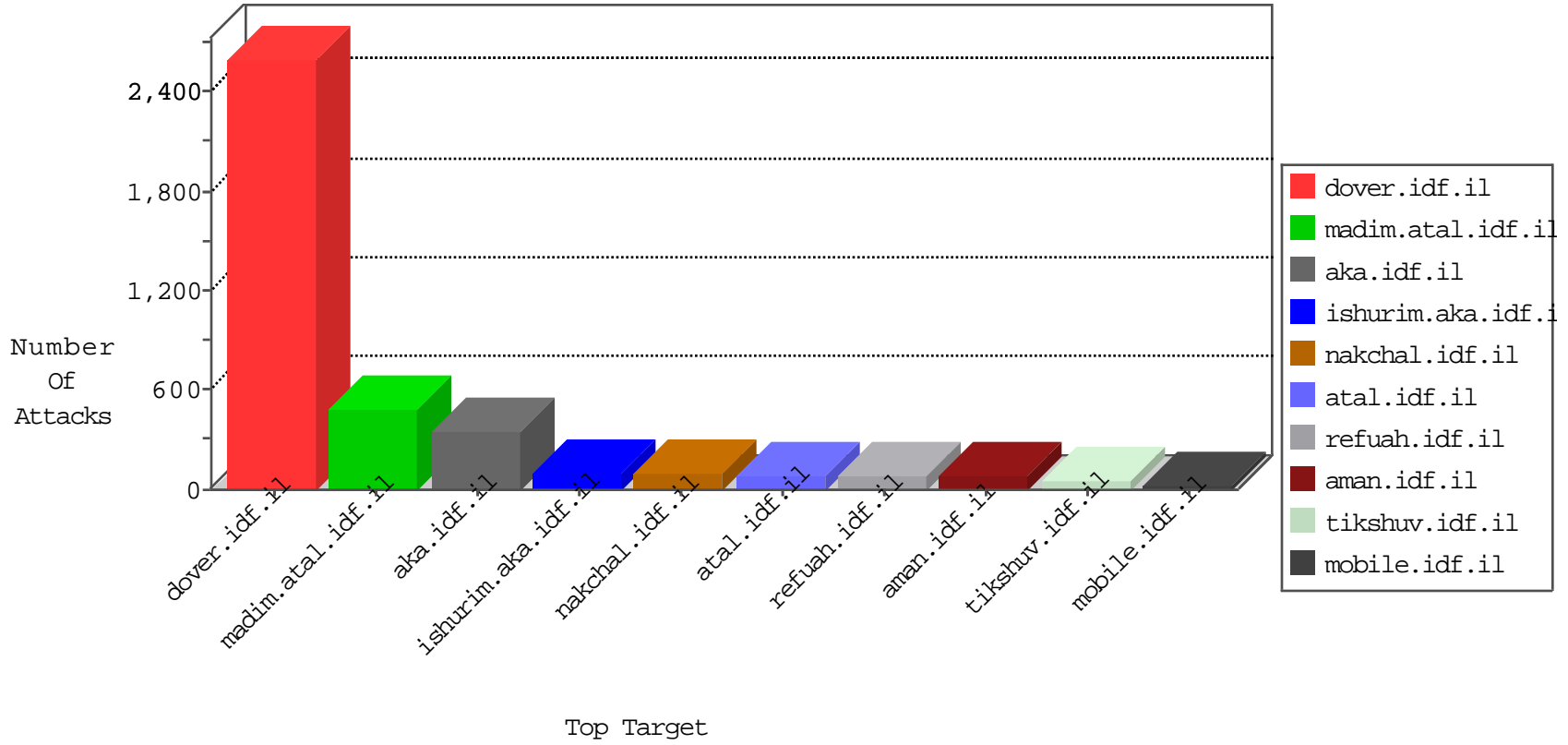


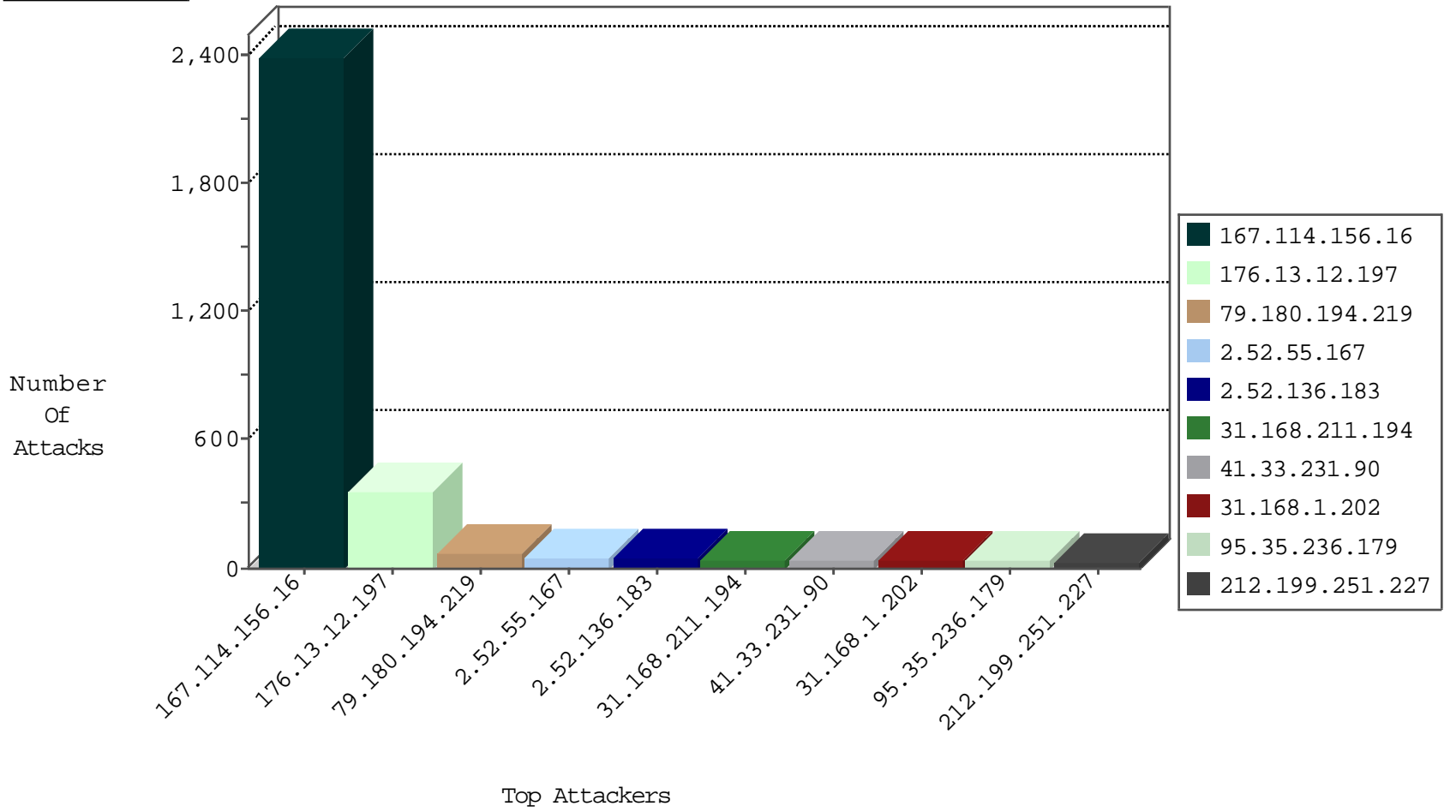
# IDF Under Attack Daily Report



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	3323
146.185.239.100	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

12-08-2015-10:04:00 to 12-08-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.106.94.91		147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.112.102.211	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.142.192.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.56.82.14	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
132.74.214.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.245.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.12.154.117	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 2048	1
79.180.155.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.116.161.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
40.115.58.160	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.112.102.211	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.153.151.102	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.138.210.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.120.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.12.154.117	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
212.179.19.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.194.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
95.35.236.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
31.168.211.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.85.186	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.232	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
37.142.192.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.19.85.5	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
31.168.211.194	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.85.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.214	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.29.164.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.52.55.167	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
79.181.231.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.151	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.19.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.173.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.202	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.78	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.39.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.151	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.104.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.154	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.23	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.106.94.2		147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	6
87.68.58.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.228.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.57.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.194.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.202	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.117.78.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
138.134.192.10	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.118.27.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.52.55.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.55.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	170
176.13.12.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
176.13.12.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	47
2.52.136.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.52.54.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
31.168.11.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.13.13.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.168.1.202	Block	6
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
168.159.213.214	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 168.159.213.214	Block	3
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.28.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.120.151.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.120.151.22	Block	3
176.12.149.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.0.73.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.18.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.2		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.90.2.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
37.142.181.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	2
109.67.105.97	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
89.139.42.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.101.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ain/home/default.aspx	Block	1
176.12.150.246	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
2.54.172.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.65.249.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.24.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.95.29.116	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.95.29.116	Block	1
176.13.19.136	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	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
176.13.10.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.123.78	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.123.78	Block	1
79.181.123.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/894-he	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
5.29.164.106	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.142.232.7	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
185.120.126.25		147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
93.172.19.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.13.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
176.12.150.246	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
2.89.234.189	Saudi Arabia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
134.0.11.76	Spain	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1