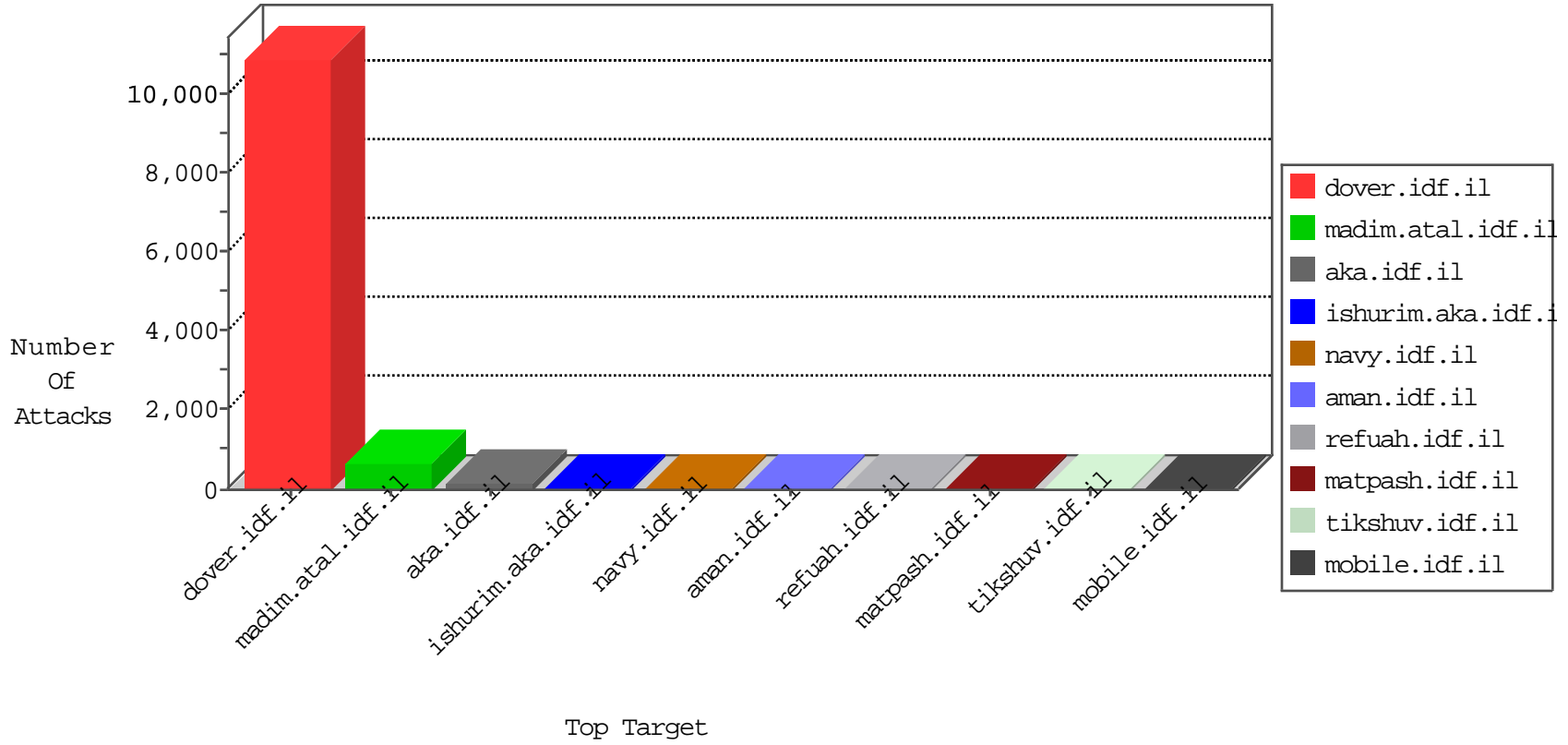


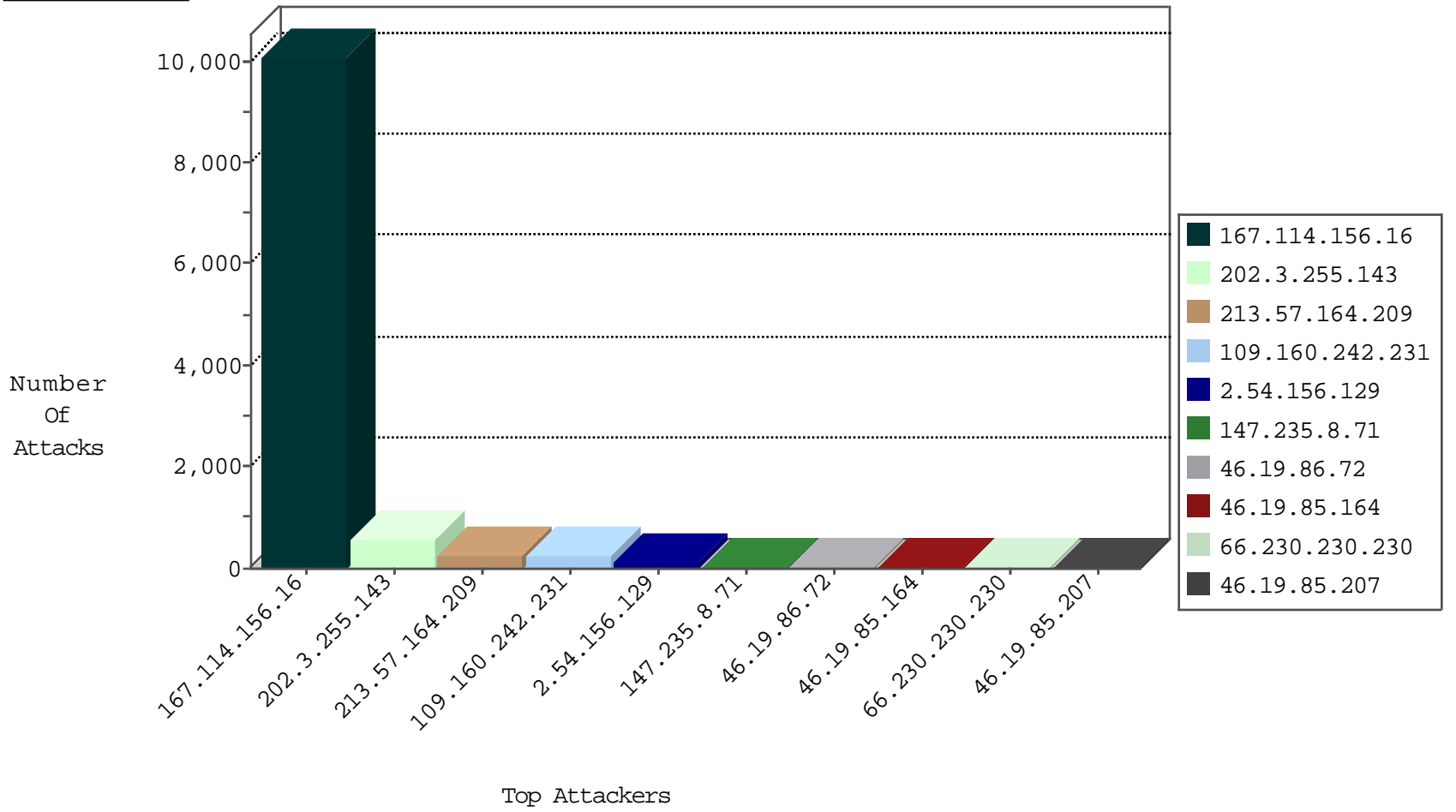
# IDF Under Attack Daily Report



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	1425
37.26.147.235	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
180.97.106.37	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.143	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	514
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.39.222.253	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.163.60.211	147.237.77.176	Taiwan	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.25.155.164	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
71.6.165.200	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.216.2.15	147.237.77.121	Taiwan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
216.178.244.30	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
194.187.249.70	147.237.76.202	Europe	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
117.25.155.164	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 3072	1
82.166.184.187	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
82.166.184.187	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
67.231.20.97	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.56.241.103	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.253.96.122	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
216.178.244.30	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
5.39.222.253	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8433
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	970
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	617
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.72	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
79.178.170.220	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.235.8.71	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
147.235.8.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
37.26.147.176	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	11
84.228.62.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.230.230.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
95.140.160.2	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
58.62.253.51	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.178.254.4	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
79.182.100.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.245.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.72.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.55.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
147.235.8.71	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.164	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.164	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.184.128	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.132	Israel	147.237.76.42	refuah.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
147.235.8.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.203	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.184.128	Israel	147.237.76.42	refuah.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
46.19.85.182	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.210.162.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.172.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.215.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.55	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.97.63	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
147.235.8.71	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.242.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
213.57.164.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.160.242.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
213.57.164.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	101
2.54.156.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
213.57.164.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	35
2.54.156.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
109.160.242.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	19
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.12.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.140.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.143.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.147.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
204.13.200.200	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/doover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/doover.aspx.	Block	2
109.253.133.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.82.65.82	Netherlands	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/page.asp	Block	1
109.253.192.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.207	Israel	147.237.77.216	doover.idf.il	Abnormally Long Request method	Block	1
2.54.15.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.62.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
107.178.194.79	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/doover.aspx.	Block	1
79.176.216.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/doover.aspx.	Block	1
130.193.50.31	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.69.78	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
46.19.85.207	Israel	147.237.77.216	doover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
217.194.206.108	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	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/doover.aspx.	Block	1
212.199.107.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.116	Israel	147.237.77.216	doover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.177	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
23.229.8.247	United States	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
84.110.53.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.207	Israel	147.237.77.216	doover.idf.il	Malformed URL _pk_id.20.8afc=687ec3d5c85db473.1452843944.1.1452843944.1452843944.;	Block	1
109.253.206.55	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
2.54.140.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.162.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.19	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	1
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.216	Israel	147.237.77.216	doover.idf.il	SSL Untraceable Connection - Open Mode	None	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/	Block	1