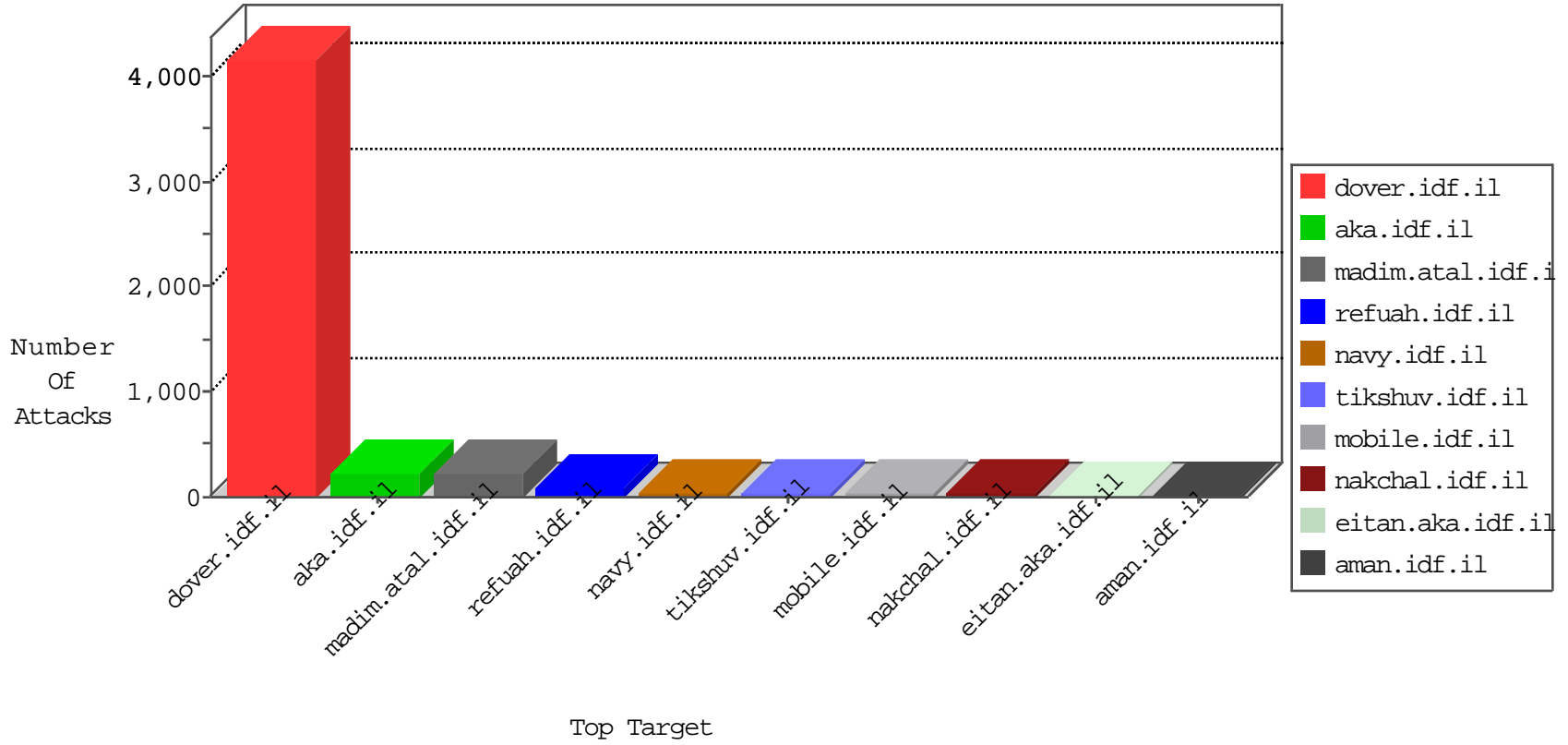


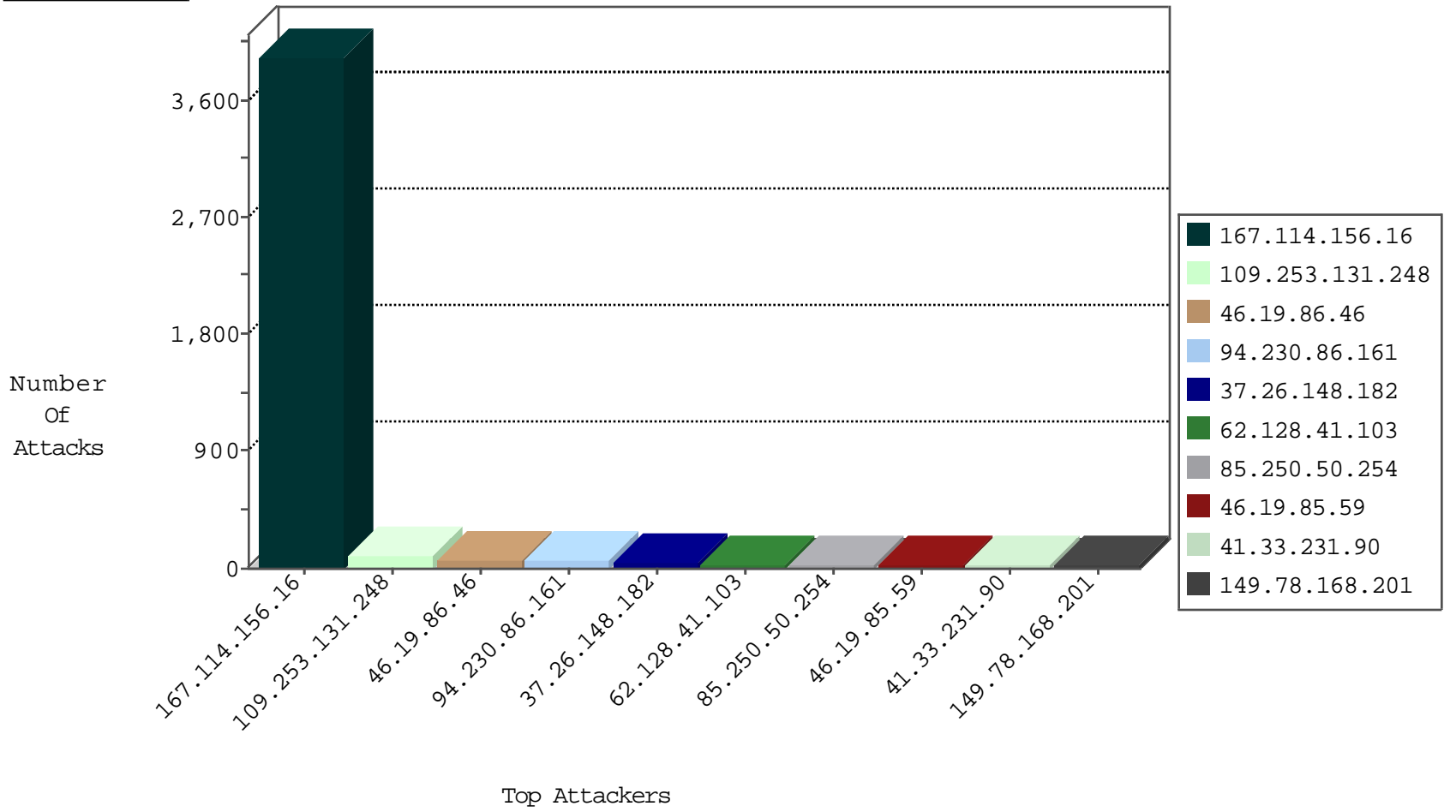
# IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	3918
79.183.224.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
80.178.251.210	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
209.126.120.23	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
71.6.146.185	United States	147.237.76.198	e.yohanan.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
188.40.95.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
188.40.95.70	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
149.78.215.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.64.135.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.109	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
84.94.149.23	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.200.15.174	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
79.181.149.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.113.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.182.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.250.75.148	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.71.81.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.200.15.174	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
79.181.2.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.175.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.177.79.199	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.23.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
84.200.15.174	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.230.86.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
85.250.50.254	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
197.214.99.15	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.16.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.109.50.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
81.83.5.137	Belgium	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
62.128.41.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.64.146.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.166.253.165	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.128.41.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.137.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
185.32.179.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.227.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.12.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.30	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.50.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.215	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.59	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.59	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.17.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.128.41.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.128.41.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.230.86.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
132.254.81.4	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.128.41.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.65.1.28	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.16.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.167.97.151	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.70.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.64.94.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.130.77	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.22.130.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.174.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.203.204	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.53.21.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.131.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	3
109.253.200.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.80.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
5.102.218.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.25.102.63	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	2
176.10.99.208	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
94.230.86.161	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.235.20.125	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus/asp/gyus.asp	Block	1
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.55.233.182	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/894-he/nakchal.aspxshared/usercontrols/headerupper/	Block	1
80.178.251.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.253.93.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.17.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
103.237.74.198	Hong Kong	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
213.8.204.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/gyus/leshakot/	None	1
46.19.85.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
87.70.27.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
204.79.180.203	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.159	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8916-he/refuah.aspx	Block	1
14.203.108.115	Australia	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
213.8.204.65	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.19.85.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
149.50.123.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	1
89.139.148.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
204.122.110.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
182.186.254.184	Pakistan	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
109.253.195.152	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.178.218.194	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
188.163.78.47	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 188.163.78.47	Block	1
157.55.39.95	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
91.200.12.76	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11540-en/dover.aspx/trackback/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15490-he/dover.aspx	Block	1
182.186.254.184	Pakistan	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/wp-login.php	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.180.2.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyud	Block	1
188.163.78.47	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1