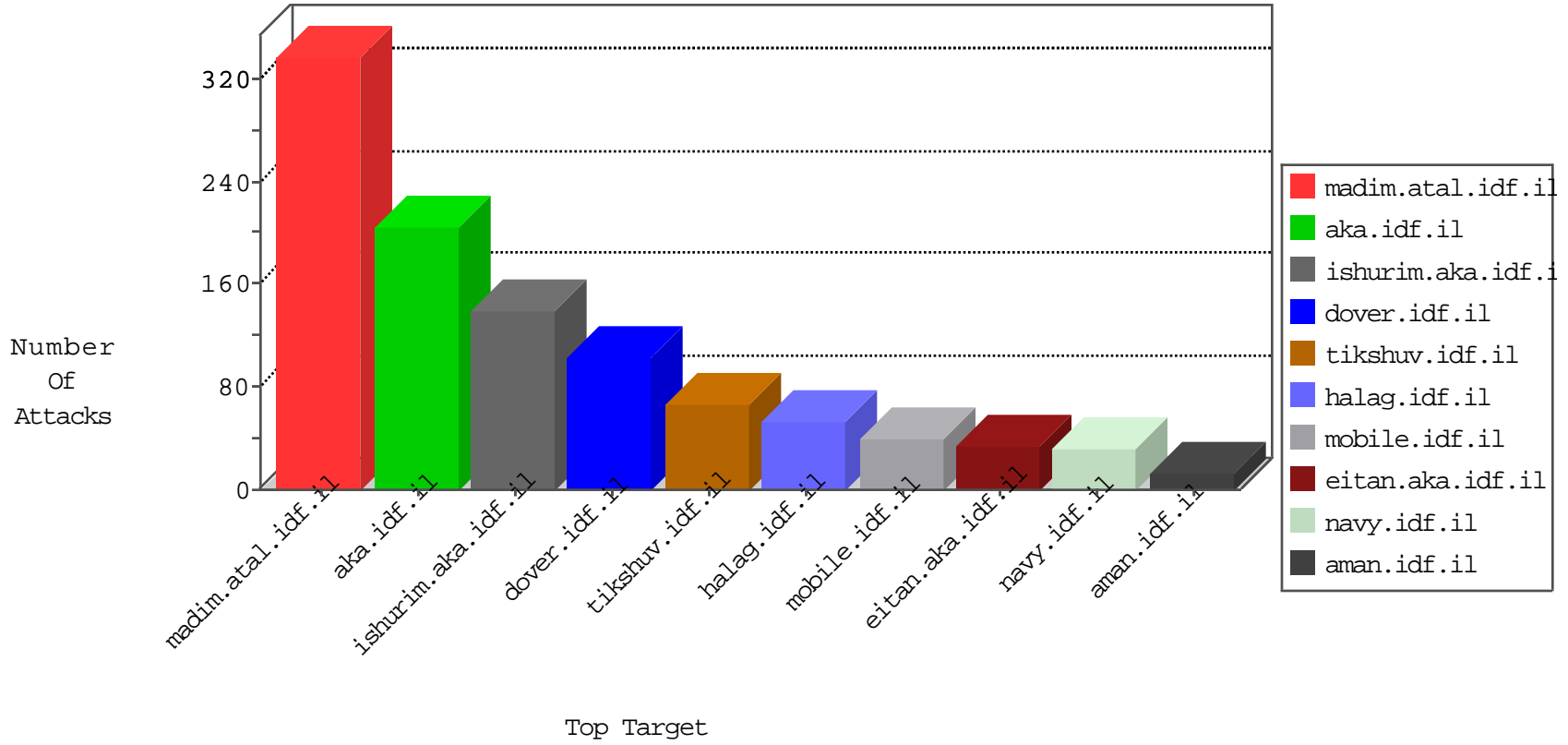


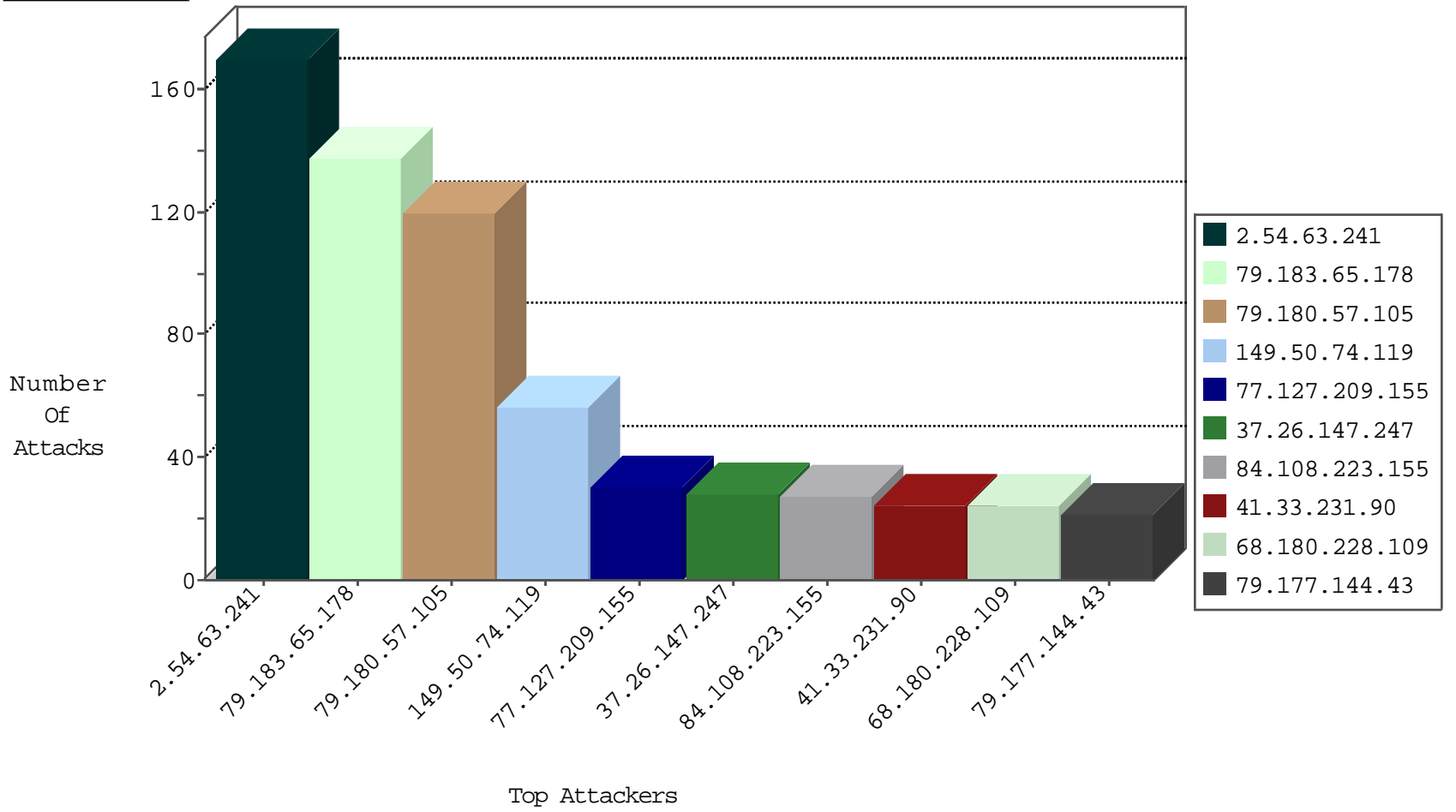
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.211.118	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
82.145.218.95	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
204.42.253.2	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
159.104.163.18	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.19	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.127.239.133	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Invalid TCP Flags	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
149.50.74.119	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
93.173.189.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
95.86.64.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.120.148.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
149.88.25.44	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
85.93.5.66	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
193.36.35.241	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
118.165.7.106	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
83.249.225.177	147.237.76.30	Sweden	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.158	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
14.169.175.191	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.231.195.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
118.165.7.106	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
108.61.228.113	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.65.178	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	138
149.50.74.119	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	24
84.108.223.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.54.40.176	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
79.177.213.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.55.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
84.108.223.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.86.93.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.137	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.196.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
46.19.85.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.180.35.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.250.225.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.194.84.106	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
95.86.114.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.108.223.155	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
85.65.164.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.133	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.99.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.57.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.233.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.118.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.7.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.6.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.154.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.56		147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.67.18.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.50.74.119	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.26.149.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.159.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
85.65.105.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
188.120.148.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
204.15.64.187	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.71.75.102		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
192.116.146.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.117.34.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

02-26-2016-12:04:07 to 02-26-2016-13:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.88.196.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.63.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
79.180.57.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
37.26.147.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
79.177.144.43	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.144.43	Block	13
79.177.144.43	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
46.120.51.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.213.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.66.55.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.153.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.55.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
109.253.131.61	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
80.246.130.162	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.158	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
37.26.148.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.86.96.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
203.133.171.71	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Malformed URL	Block	1
46.19.86.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
131.253.25.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.6.190	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
80.246.130.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.27	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
37.26.148.244	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.168	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.64.3.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
5.29.60.149	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
149.50.74.119	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.149.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
185.120.125.56		147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	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
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Abnormally Long Request method	Block	1
212.34.12.66	Jordan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.1.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
60.251.78.50	Taiwan	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
5.39.222.159	Netherlands	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/rom-0	Block	1
157.55.39.0	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
85.65.105.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.144.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
194.241.30.13	Finland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.136	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.130.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method tK²ly'M"-dÜ[[#12]]"@_0-:•Pmúîš+[[#23]]îRO;'Ă[[#25]]æ•ÝäÿzÜÿ[[#28]]îF[[#29]]·\$°~y[[#3]](gHö@RÖ± in URL	Block	1