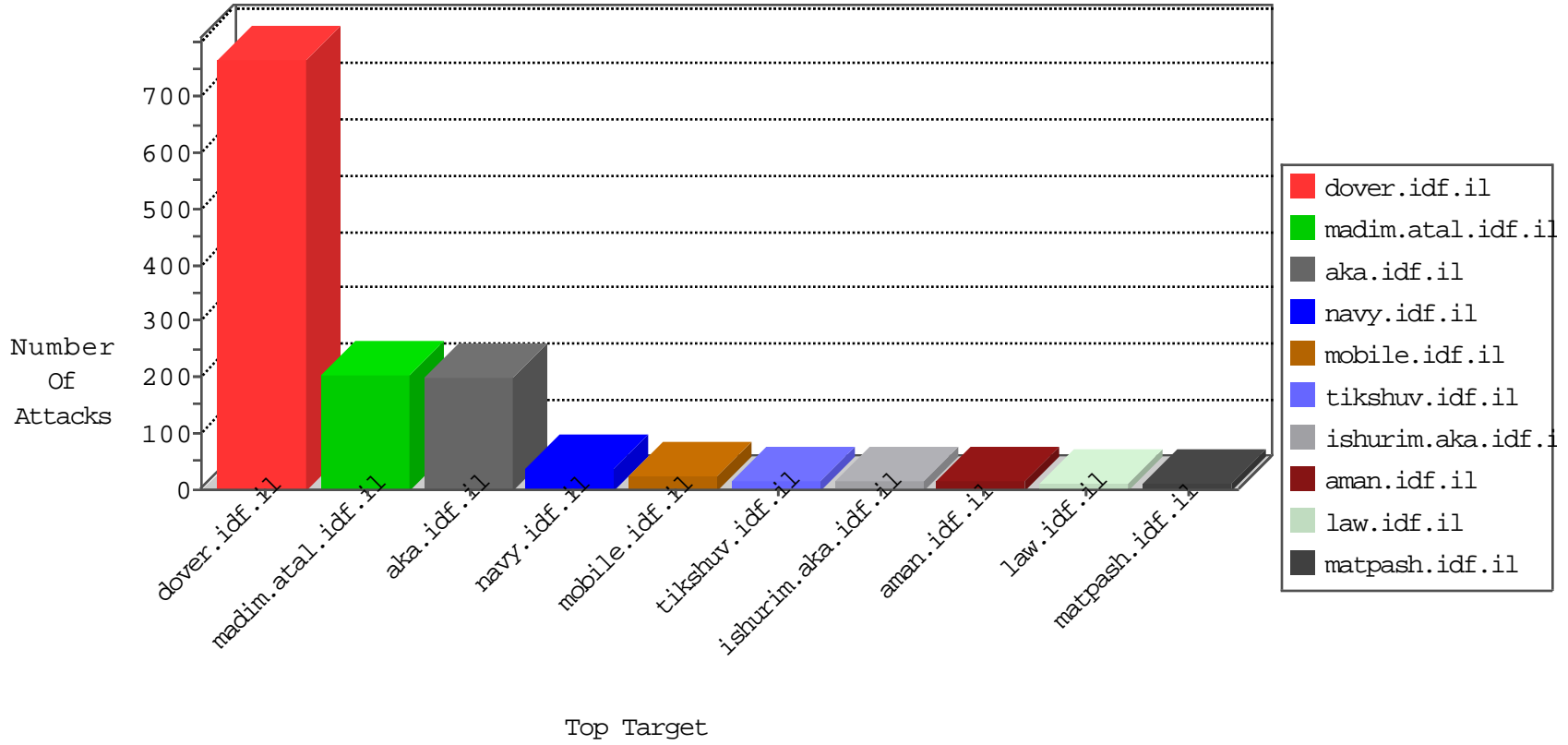


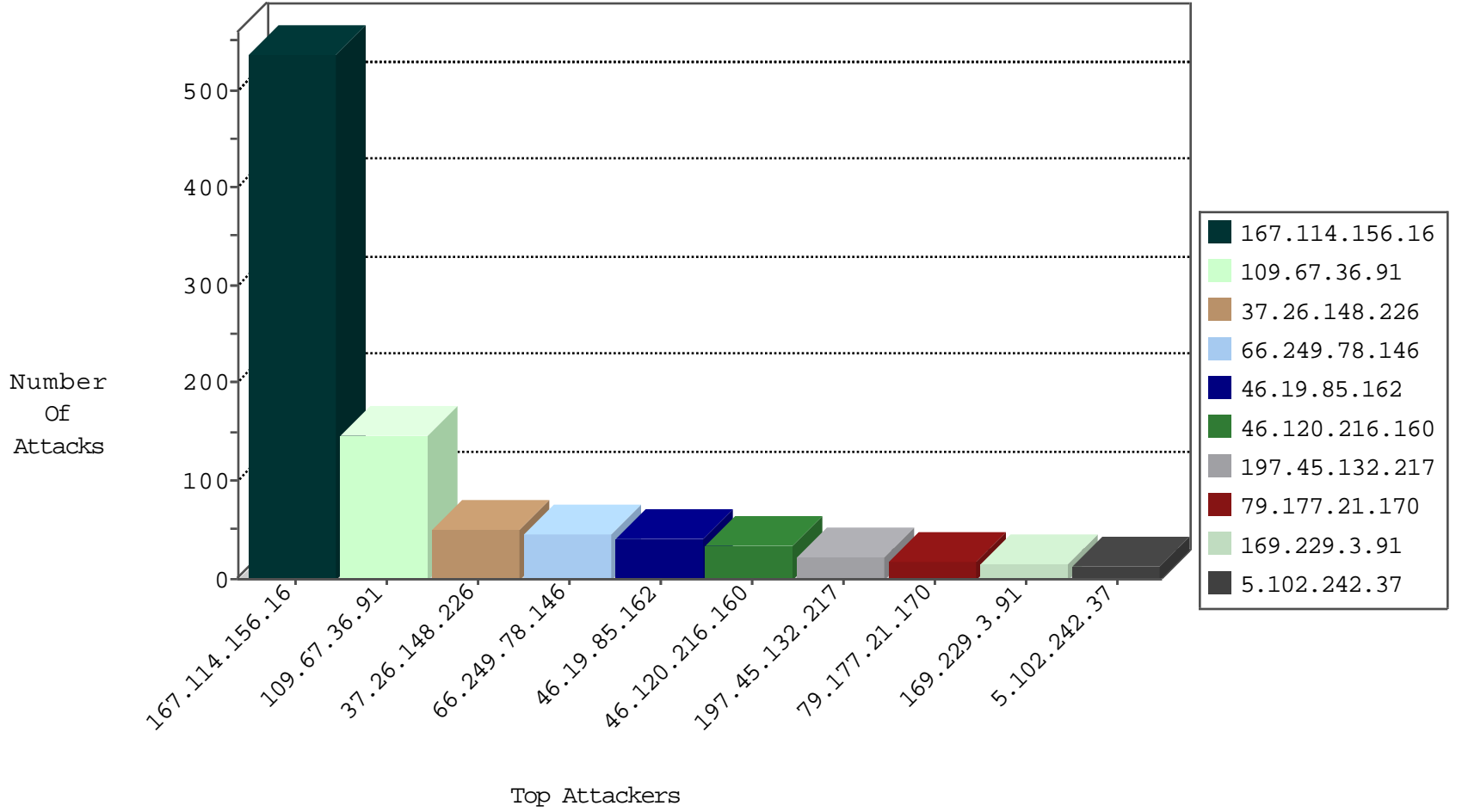
# IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	21831
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1393
5.102.242.37	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	210
149.78.84.13	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	204
73.143.247.211	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
84.254.19.118	Greece	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
38.229.1.13	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
109.64.128.168	Israel	147.237.77.216	dover.idf.il	Invalid I4 Header Length	drop	1
71.6.146.185	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
109.64.128.168	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.220.63.148	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.81.68.2	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
103.246.225.29	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sA (2)	2
67.130.39.67	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
40.76.60.52	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.98	147.237.76.201	United States	e.atal.idf.il	ET DROP Dshield Block Listed Source	1
113.59.33.61	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.238.10	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
67.130.39.67	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
211.220.63.148	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
113.59.33.61	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
67.130.39.67	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.26.148.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.162	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.162	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.9.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.53.40	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
193.43.246.250	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.177.21.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.10.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.21.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.51.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.29.238.10	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.242.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.21.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.53.181.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.253.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.232.163.119	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.64.128.168	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
197.211.53.27	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.186.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
108.30.105.45	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.53.49.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.70.49.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.177.103.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.24.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.249	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.166.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.229.249.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.208.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.117.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.183.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.9.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.190.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.126.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.240.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.53.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.10.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-27-2016-16:04:02 to 04-27-2016-17:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.81.93.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.142.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.36.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
46.120.216.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.53.42.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.7.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.225.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.55.160.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.159.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
207.46.13.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.225.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.125.124.195	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/news/mobile	Block	1
65.55.210.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.134.227	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/mobile	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
80.95.38.249	Russian Federation	147.237.0.19	madim.atal.idf.il	Parameter Type Violation returnUrl in madim.atal.idf.il/login.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3058.jpg	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
37.142.64.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.51.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.238.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.203	United States	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	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2412.jpg	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
2.53.181.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.2.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.224.125	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
65.158.81.132	United States	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
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
109.65.176.23	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
199.30.16.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.210.219.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.12.66	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.105.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
31.168.82.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
52.2.127.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
2.55.19.252	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request method	Block	1
79.182.29.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$ctl155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	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
37.46.41.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
2.53.43.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1