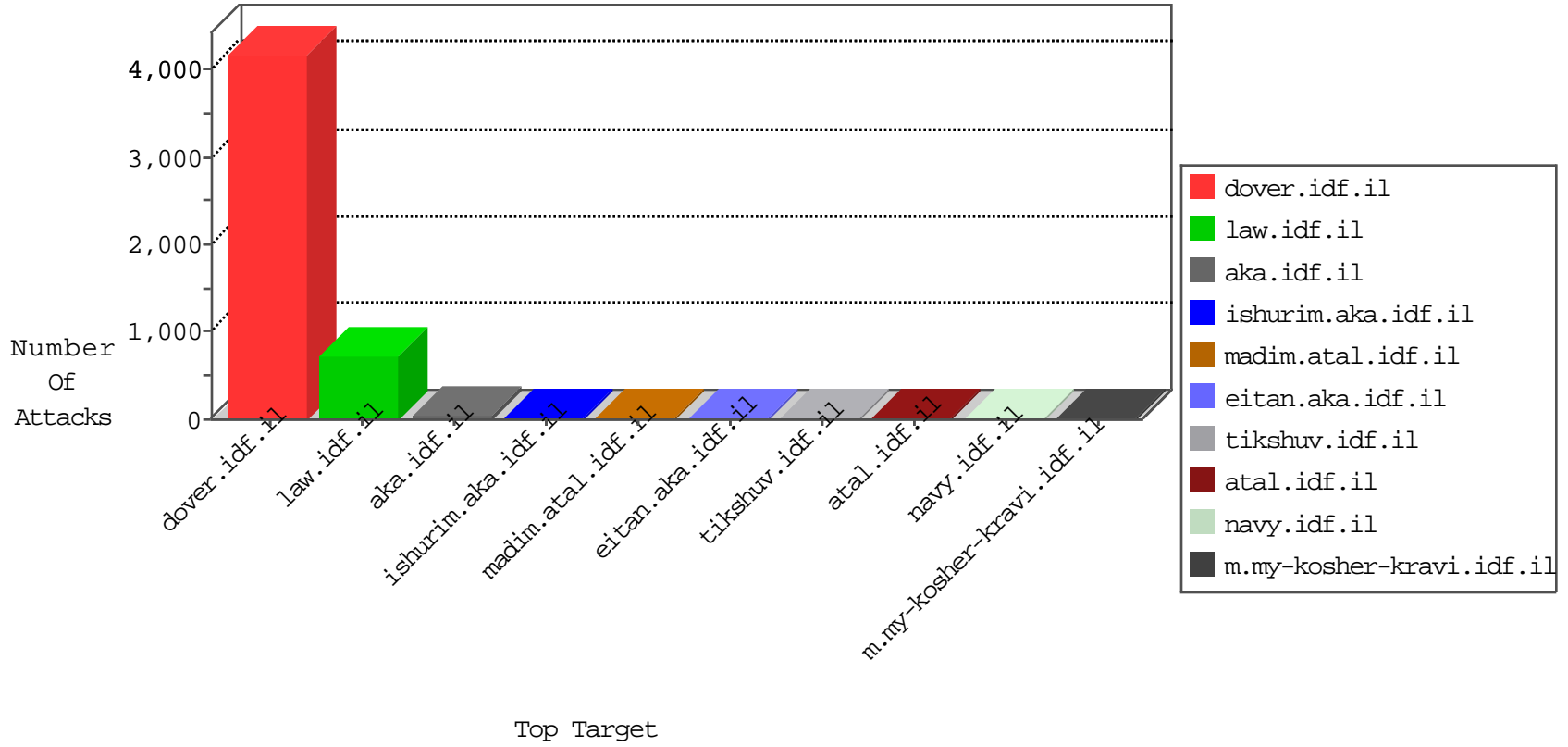


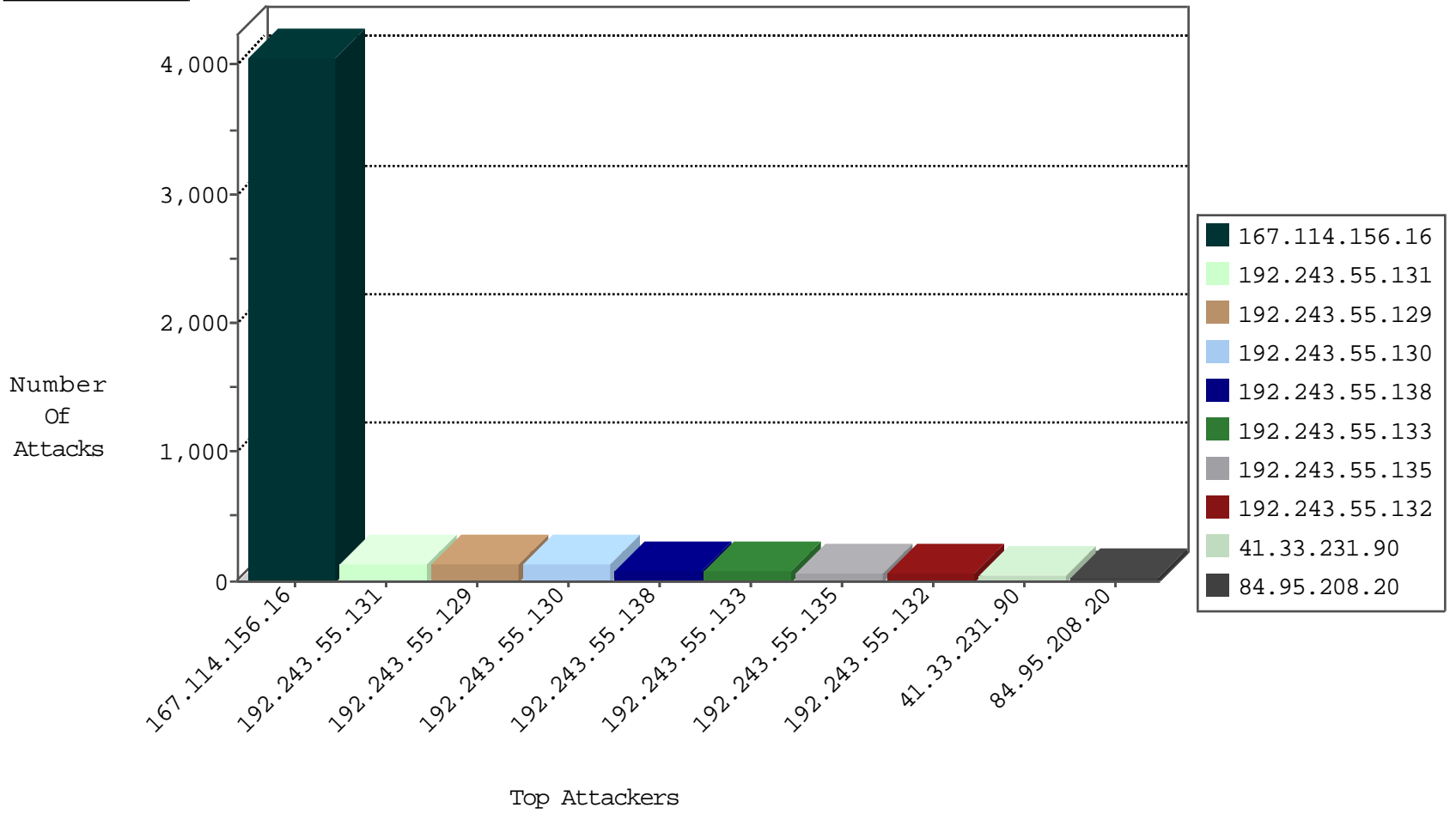
# IDF Under Attack Daily Report



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	4065
0.0.0.0		147.237.77.216	dover.idf.il	HTTP_Page_Flood_Attack	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
107.150.32.60	United States	147.237.77.170	maarachot.idf.il	block-sp-trafl	forward	2
204.12.196.236	United States	147.237.77.74	law.idf.il	block-sp-trafl	forward	2
204.12.196.237	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	forward	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
204.12.196.235	United States	147.237.72.156	aman.idf.il	block-sp-trafl	forward	2
93.201.74.250	Germany	147.237.0.16	ny-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
93.201.74.250	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
192.96.201.142	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
158.130.6.191	United States	147.237.0.16	ny-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
93.201.74.250	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
192.96.201.142	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
93.201.74.250	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
213.246.49.97	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
92.156.250.251	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
207.46.13.135	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	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
84.245.33.104	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	4
5.189.167.216	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.148	Latvia	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
181.222.28.45	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.3.117.72	147.237.8.46	Philippines	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.189.167.216	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.72.167	Latvia	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.125.216.100	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	21
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	19
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	16
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
46.19.85.75	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.43.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
73.171.202.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.201.46.68	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.84	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	12
162.243.25.240	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.25.240	Block	3
199.30.25.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.121.26.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.118.27.14	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.121.83.118	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
77.75.76.165	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
46.19.86.59	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
204.12.196.236	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.66.161	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
185.118.27.9	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.39.222.159	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
94.181.164.109	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
204.12.196.237	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
87.69.87.7	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
23.29.125.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
94.181.164.109	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
46.121.30.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/logi	Block	1
157.55.2.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
87.69.87.7	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authentication-service.aspx/getauthuser	Block	1
185.118.27.15	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.150.32.60	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
89.163.140.26	Germany	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.93.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1440-he/refuah.aspx	Block	1
162.243.25.240	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1