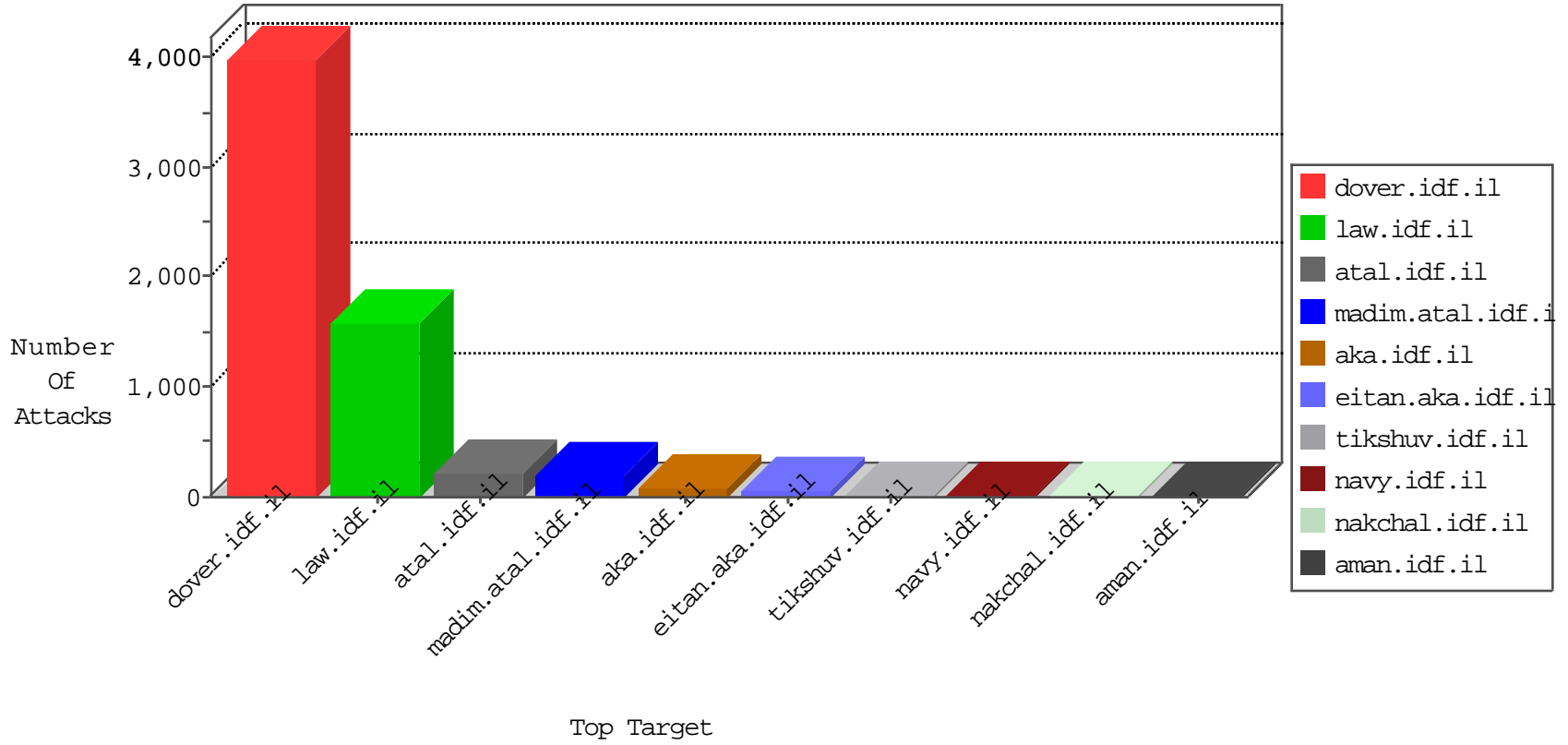


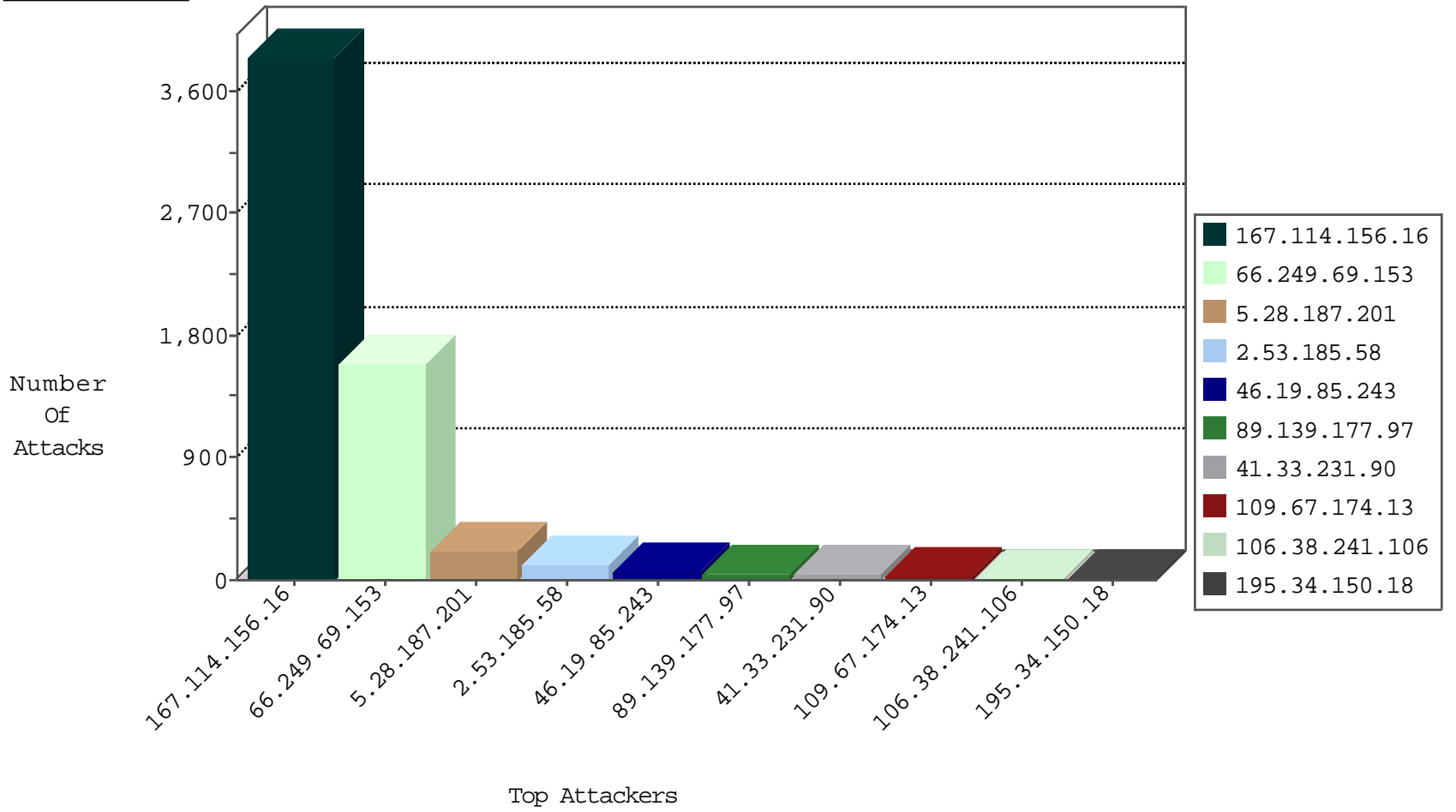
# IDF Under Attack Daily Report



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	3857
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
113.248.166.23	China	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
94.102.52.10	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.210.48	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
109.65.0.156	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
192.168.0.15		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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	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
66.249.69.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1590
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
177.207.143.25	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
106.184.2.29	147.237.0.19	Japan	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
36.84.76.230	147.237.8.14	Indonesia	e.orchot.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
5.28.187.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	203
89.139.177.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.67.174.13	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.228.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.163.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.148.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
97.77.25.226	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.128.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.203.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.34.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.202.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.155.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.1.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.8.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.129.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.3.46	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
207.46.13.120	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.230.97	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.219.146	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
207.241.225.235	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.170.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.219.146	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.241.226.216	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
92.237.187.34	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
92.237.187.34	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.66.58.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.121.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.153.234.58	Sweden	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.135.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
108.61.228.87	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.44.103.160	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.245.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.144.41.122	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.185.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
109.253.142.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
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	5
79.178.197.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.183.35.134	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
188.143.232.123	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.123	Block	4
2.55.155.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.35.134	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	3
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
217.78.4.232	Ireland	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
207.46.13.19	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/7/1557.jpg	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
217.78.4.232	Ireland	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
66.249.65.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/grid.css	Block	1
207.46.13.172	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
217.78.4.232	Ireland	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-en/cogat.aspx	Block	1
5.28.187.201	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
157.55.39.205	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
74.95.149.205	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
217.78.4.232	Ireland	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
66.249.65.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
207.46.13.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.81.3.151	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.aspx/getauthuser	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/69054.pdf	Block	1
217.78.4.232	Ireland	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/1558.jpg	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
87.70.29.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$cb14641127 in aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
217.78.4.232	Ireland	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/901-en/cogat.aspx	Block	1
37.187.114.171	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /irj/portal	Block	1
199.47.81.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-	Block	1
79.183.35.134	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.183.35.134	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
2.53.185.58	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1