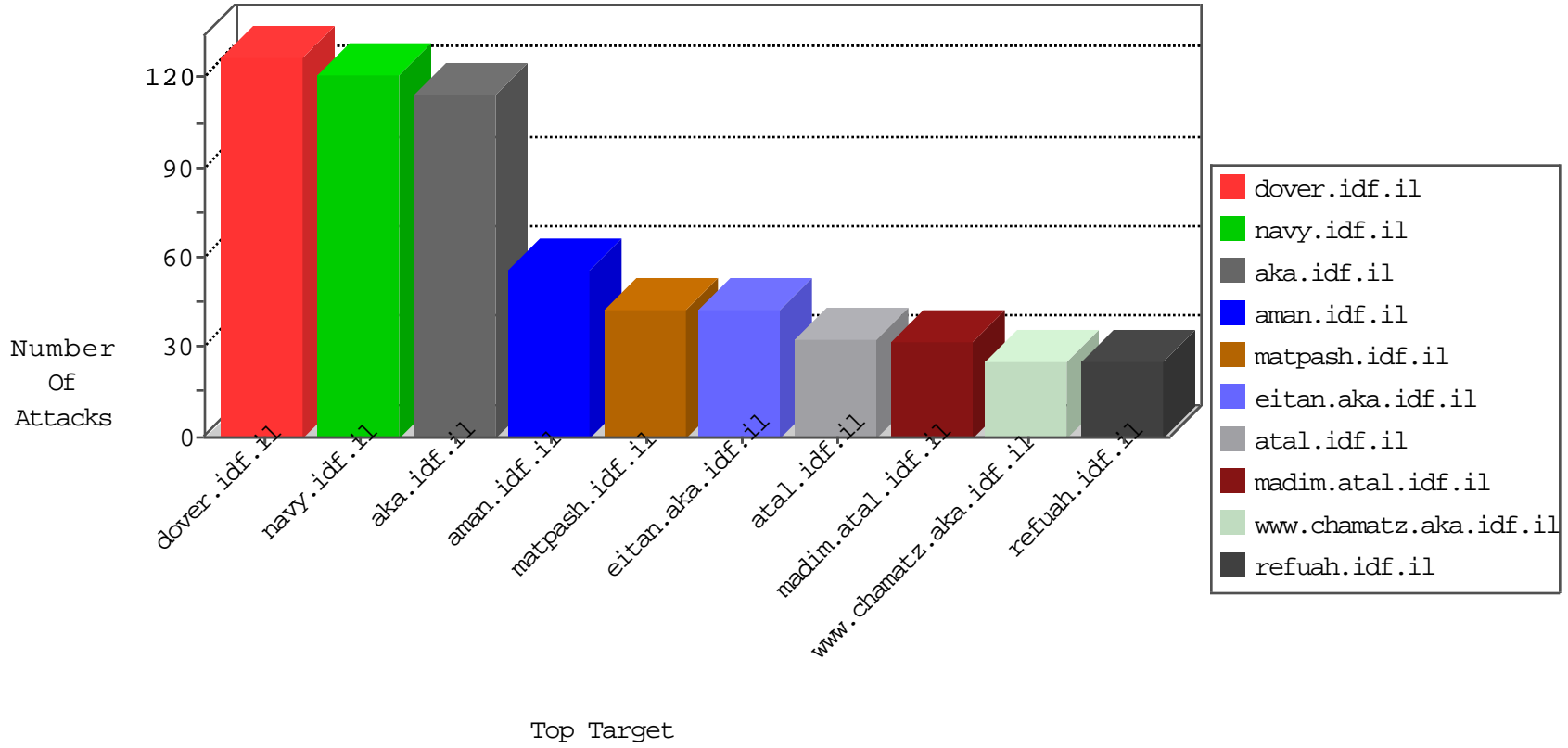


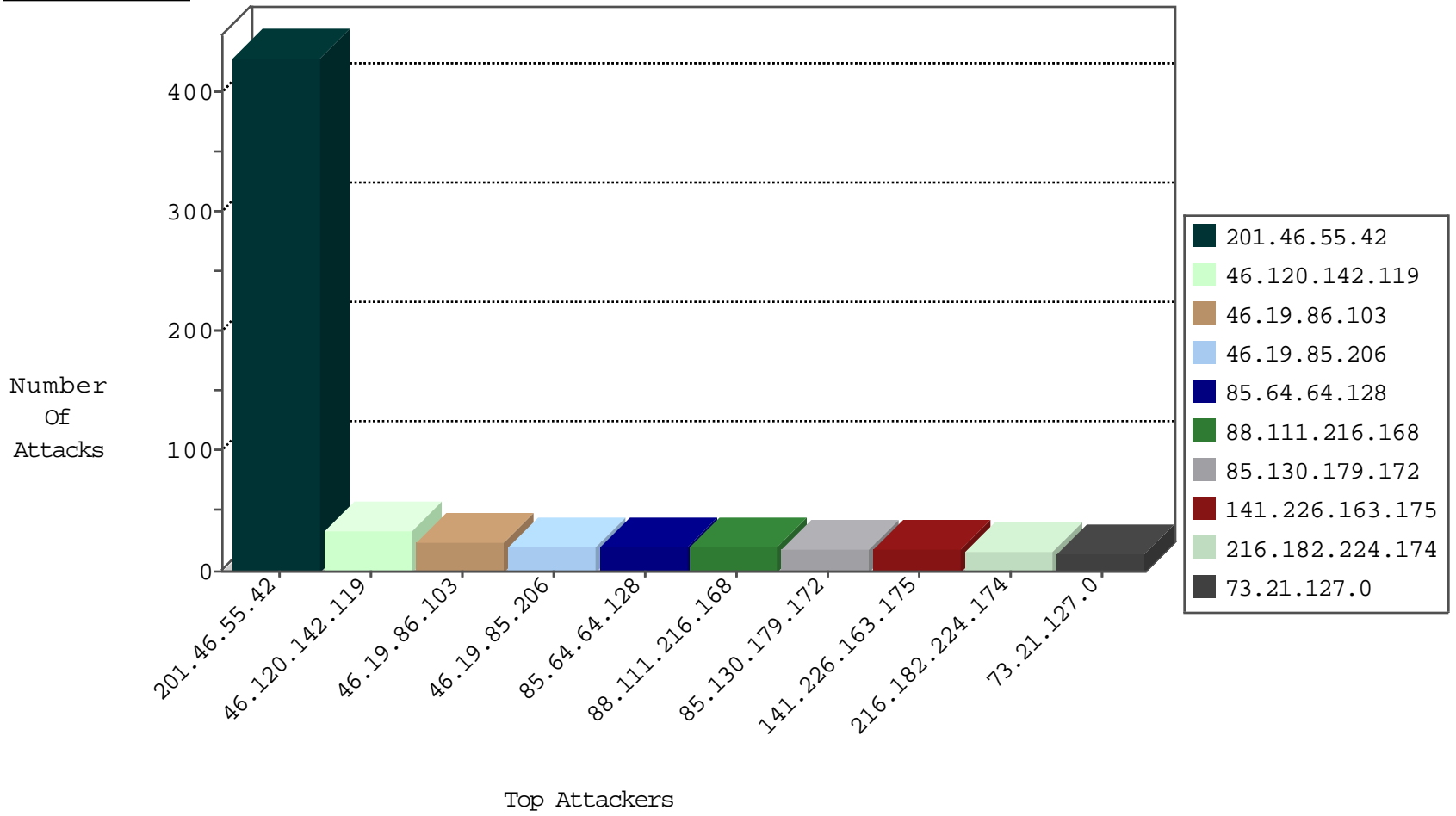
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.28.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-00:04:04 to 09-11-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.161.40.17	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.33.116.208	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.150.38.110	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
201.38.68.132	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
69.24.208.162	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
46.161.40.17	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
23.92.20.154	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.150.38.110	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.160.132	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.38.241.105	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.249.66.240	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
46.161.40.17	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
85.64.64.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
73.21.127.0	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.103	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
46.19.86.103	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.120.142.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
84.94.155.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.120.142.119	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
85.130.179.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.226.163.175	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
85.130.179.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.226.163.175	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.130.179.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
141.226.163.175	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.64.150.94	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.120.142.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.120.142.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.142.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
88.111.216.168	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.23	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
88.111.216.168	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
88.111.216.168	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
88.111.216.168	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
88.111.216.168	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
72.186.196.8	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
69.178.112.197	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
69.178.112.197	United States	147.237.76.86	navy.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
85.65.109.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.146.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.27.106.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.27.106.72	Block	3
2.53.2.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.98.181	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
77.139.79.242	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	2
85.64.88.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
106.38.241.105	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.146.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
85.65.109.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.66.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.180.129.206	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/	Block	1
37.26.149.133	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
87.71.242.166	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
79.180.218.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
46.116.14.218	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
89.237.89.196	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1
93.158.152.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.139.241.14	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
5.28.136.99	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1