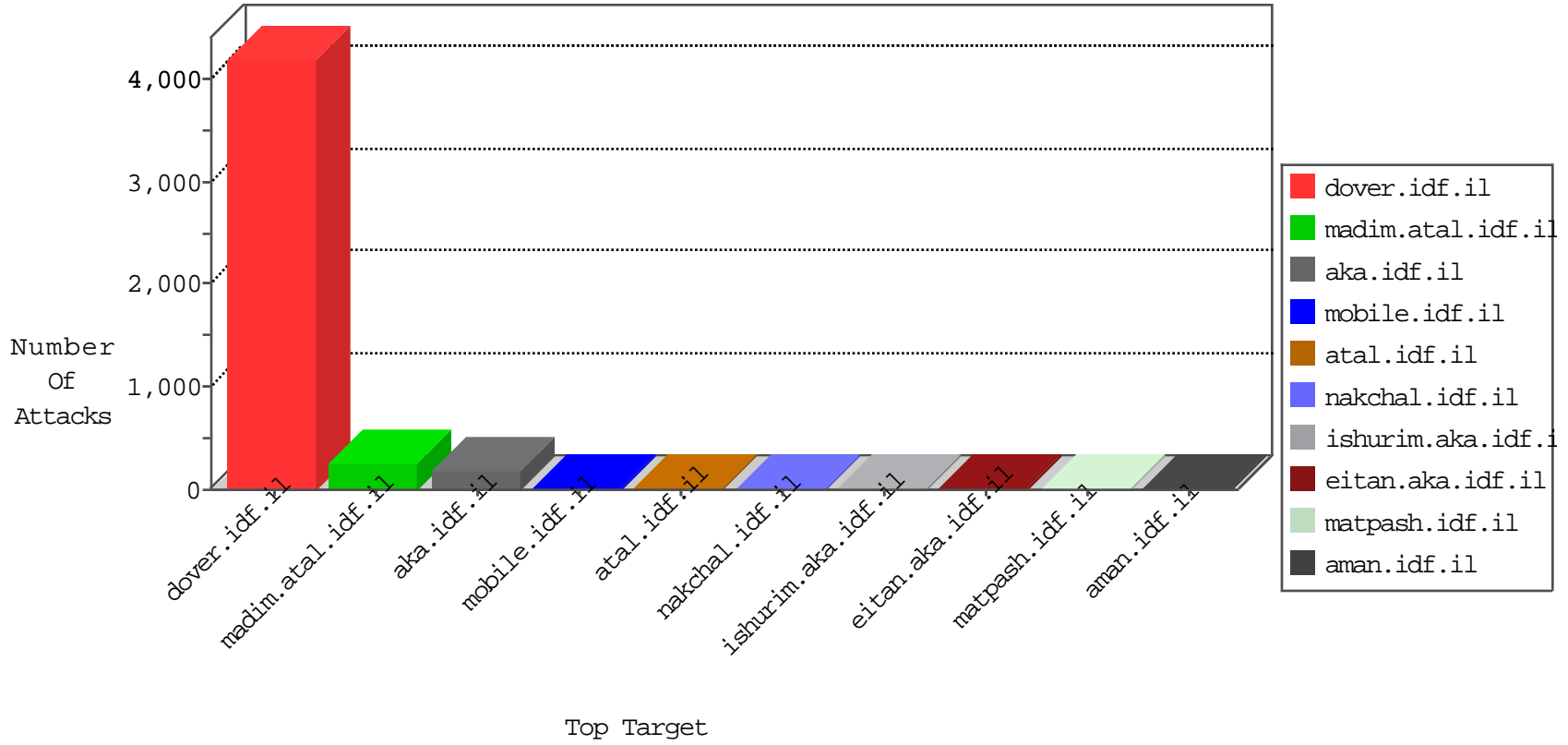


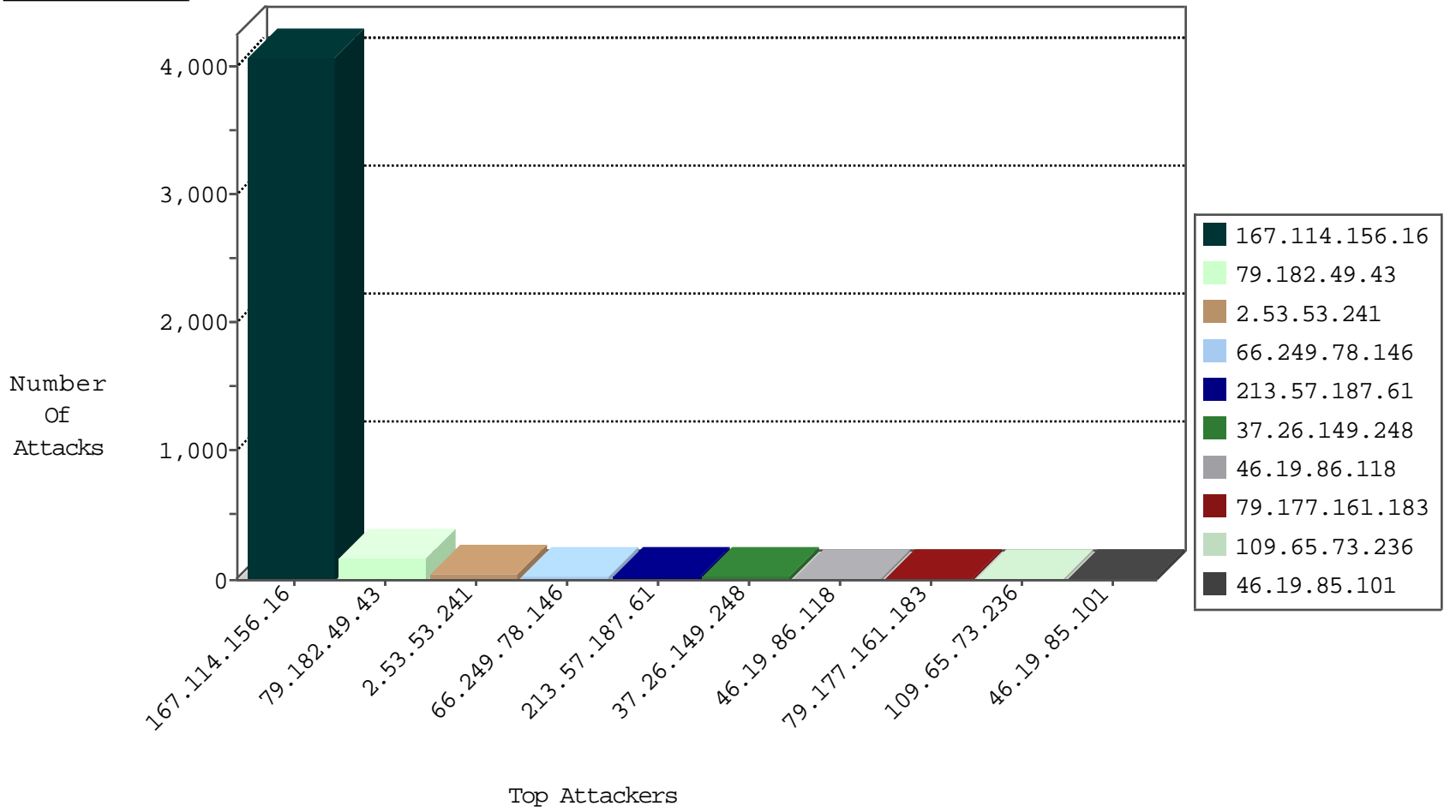
IDF Under Attack Daily Report



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	4070
181.112.143.242	Ecuador	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
198.62.219.5	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
198.20.87.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
65.220.102.4	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.116.160.1	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	3
185.103.252.72	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	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
13.92.245.177	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.245.177	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
213.251.182.106	147.237.77.176	France	matpash.idf.il	SERVER-WEBAPP admin.php access	1
185.103.252.72	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.114.116.55	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.245.177	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
220.134.99.167	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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	27
213.57.187.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.86.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.149.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
109.65.73.236	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.144	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.136	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
207.232.37.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.15.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.161.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.3.147.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.161.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.33.169	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.184.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.144.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.6.230.87	Brunei Darussalam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.70.38.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.100	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.200.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.40.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.246.165.150	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
176.13.2.108	Israel	147.237.76.147	chimuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.187.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.207.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.157.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.56.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.33.169	Israel	147.237.77.243	mobile.idf.il	SYN Attack		reject	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.159.207	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
95.86.93.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.64.234.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.49.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
2.53.53.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.53.53.241	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	17
109.65.131.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
84.111.70.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.146.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.187.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	4
89.139.159.84	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.212.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.133.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.163.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
95.86.93.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.23.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.163.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.163.253	Block	2
109.64.163.253	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
109.253.221.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.166.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.210.187.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.251.182.106	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
87.69.104.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
52.23.231.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	2
213.251.182.106	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 213.251.182.106	Block	2
2.53.155.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.159.84	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 89.139.159.84	Block	2
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.67	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.law.idf.il/644-he/patzar.aspx	Block	1
109.65.241.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
213.57.187.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.126.176	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.176	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.142.64.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
217.194.195.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
204.79.180.170	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	147.237.76.86	navy.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.139.159.84	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/8/	Block	1
5.22.131.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
213.251.182.106	France	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/license.php	Block	1
149.78.192.135	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
41.107.66.244	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15127-ar/	Block	1
204.79.180.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.228.161.242	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.15.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1