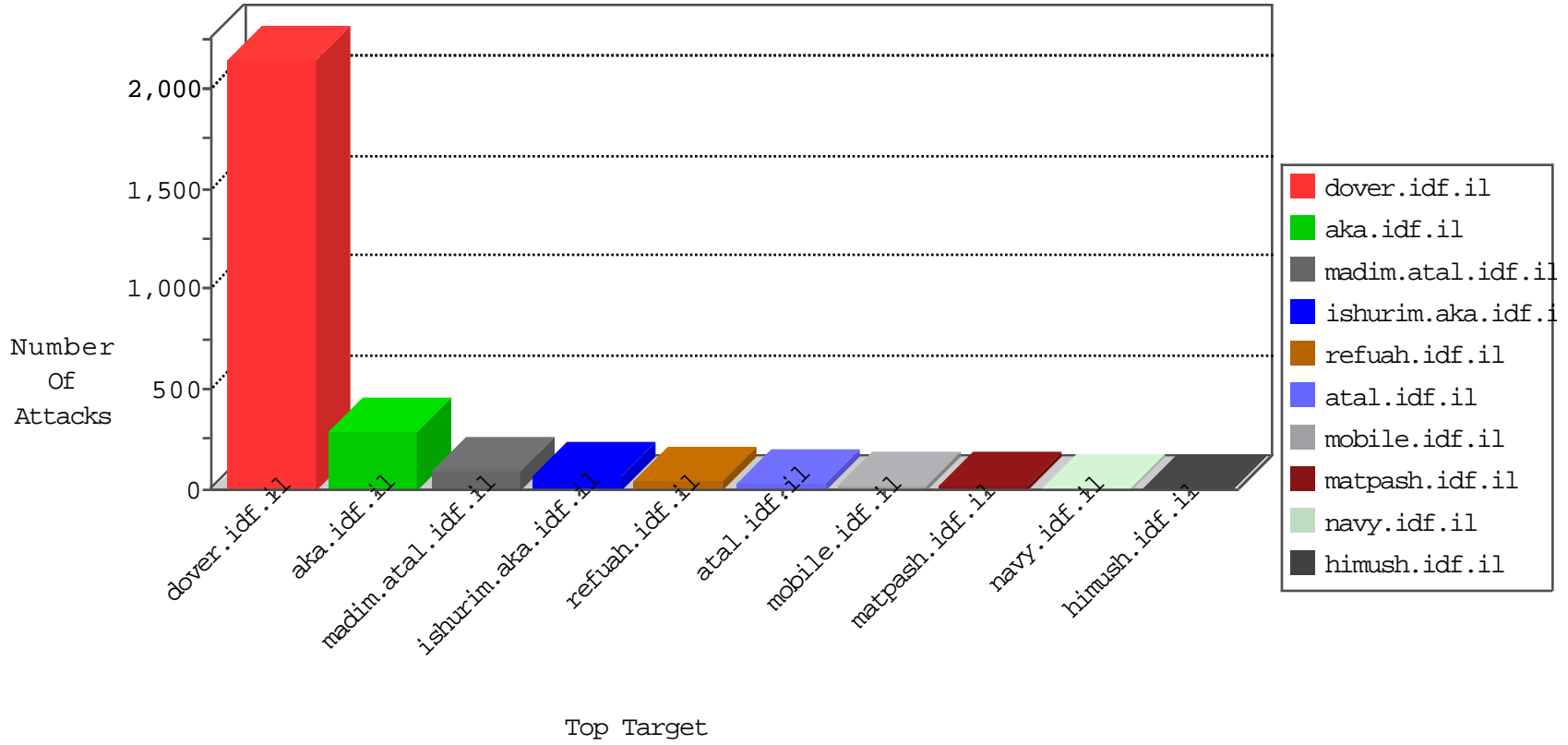


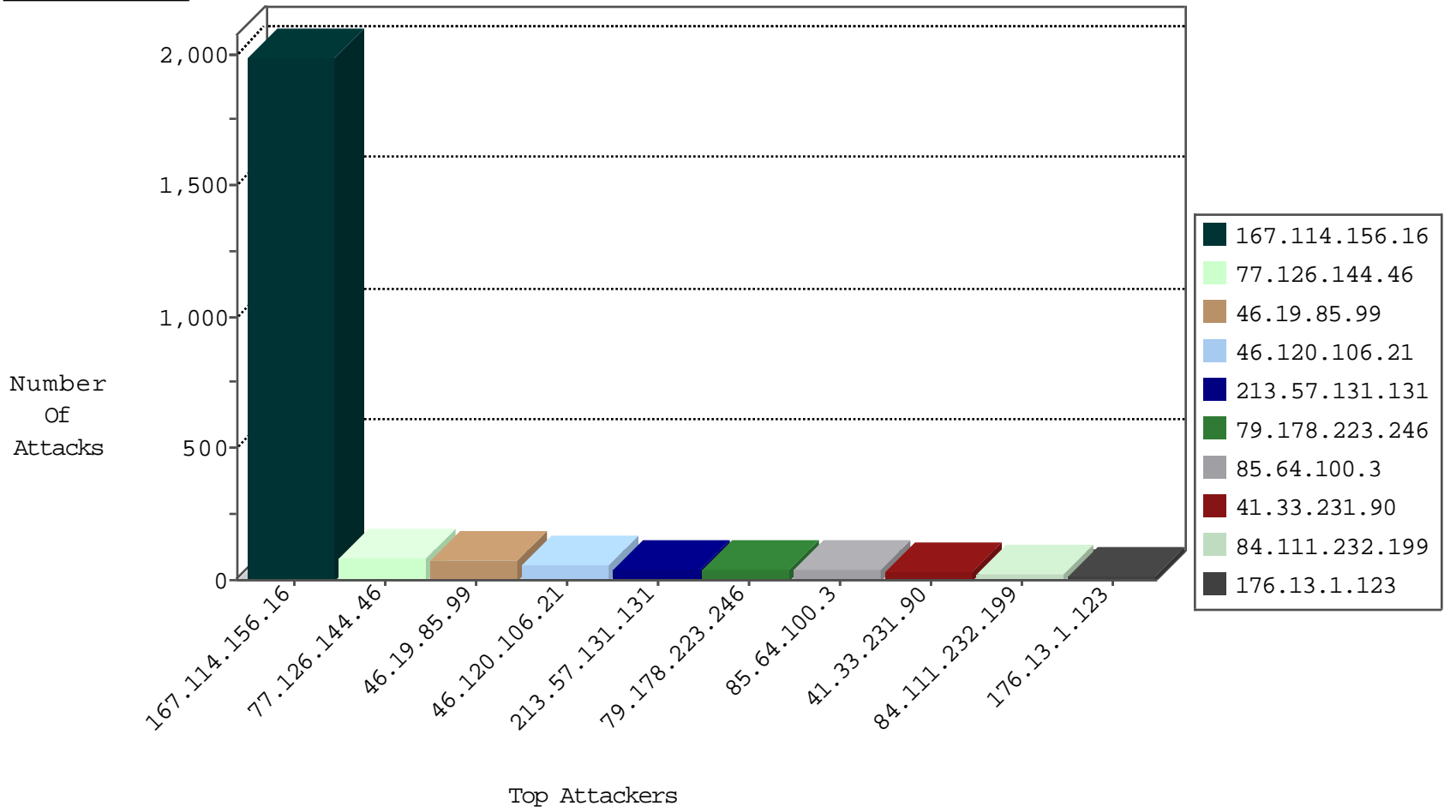
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3069
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	258
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.173.106.6	Netherlands	147.237.76.44	e.refuah.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
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 4096	1
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -f -sS	1
217.16.2.77	147.237.77.227	France	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.77.205	France	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.76.148	France	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.228.33.167	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 2048	1
217.16.2.77	147.237.77.235	France	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.77.216	France	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.76.148	France	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.0.33	France	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -f -sS	1
91.236.213.82	147.237.76.177	Ukraine	ncore.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
46.120.106.21	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
79.178.223.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.131.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
213.57.131.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
213.57.131.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
89.138.40.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.246.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.112	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
185.3.146.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.85.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
176.13.1.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.64.102.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.177.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.223.246	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.1.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.126.91	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.1.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
185.5.223.10	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.246.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
217.132.35.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.52.20.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
199.7.157.45	Canada	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.240.201	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.34.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.154.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.168.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.96		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.166.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.147.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.231.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.183.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.149.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
108.19.36.223	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.144.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
85.64.100.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	35
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
84.111.232.199	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.111.232.199	Block	14
89.138.229.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
80.178.208.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
84.111.232.199	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
84.111.232.199	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
130.193.50.31	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.136.152	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.11.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
195.154.191.97	France	147.237.76.86	navy.idf.il	PHP Attempt	Block	2
77.127.85.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
178.223.66.206		147.237.77.216	dover.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
109.64.185.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.138.68.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.190.134	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.111.224.167	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
195.154.191.97	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-login.php	Block	1
2.54.182.155	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/resources/verisign.php	Block	1
77.127.196.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.44.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
79.182.39.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
2.54.182.155	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
185.32.179.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
109.201.152.22	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.166.190.144	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
195.154.191.97	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.54.182.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
162.243.188.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
79.176.104.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.65.76.149	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.223	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
192.42.116.16	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
54.153.33.152	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.191.97	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1